

Establishing the Legal Framework of Telehealth in the Philippines

Ivy D. Patdu and Allan S. Tenorio

National Telehealth Center, National Institutes of Health, University of the Philippines Manila

ABSTRACT

The National Telehealth Service Program aims to address the inequity in health, and to utilize the advancements in information and communication technology to improve health outcomes in the country, primarily through telemedicine. There are no laws that directly govern the practice of telemedicine but the implementation of the National Telehealth Service Program has legal implications. The Round Table discussions were effective in identifying key issues such as the nature of the practice of telemedicine, liability issues for stakeholders, and the privacy concerns in Telehealth. Based on an analysis of these issues in the context of relevant laws and jurisprudence, it is established that those who practice telemedicine will have a duty to exercise diligence in managing patients or providing specialty advice. The standard of care for physicians practicing telemedicine should take into consideration the limitations of technology and the inherent differences between telemedicine and face-to-face doctor-patient consultations.

The National Telehealth Center has a responsibility to put in place internal policies and procedures that would improve the delivery of health services through telemedicine while safeguarding the patient's right to privacy. Current laws, particularly the Data Privacy Act of 2012, puts emphasis on obtaining patient's consent and requires putting in place organizational, physical and technical security measures in the collection and processing of personal and sensitive information.

Key Words: Telemedicine, Telehealth, eHealth

Introduction

Health for all remains to be an elusive dream. In the Philippines, where more than 20% of Filipinos fall below the poverty line, the inequity in health care delivery is a palpable problem.¹ In 2010, it was reported that six out of ten Filipinos die without receiving medical attention.² There continues to be geographically isolated and disadvantaged areas with severely limited access to health care. Most hospitals are concentrated in the National Capital Region, and on the average, travel time to a health facility is 39

minutes with relatively longer travel time in rural areas as compared to urban areas.^{3,4}

Low doctor to patient ratio is observed across the country. The Doctor to the Barrios Program was launched by then Secretary of Health Juan Flavio Velasco in 1998 after the Department of Health discovered that some "271 towns in the country has had no municipal physician for 10 years or more."⁵ The problem of "brain drain" is still prevalent in the health sector, with health professionals leaving the country to seek greener pastures abroad.^{6,7} It is with these realities that the National Telehealth Center, National Institutes of Health, based in the University of the Philippines Manila, established the practice of Telemedicine. Telemedicine is defined by the World Medical Association as:

"the practice of medicine over a distance, in which interventions, diagnostic and treatment decisions and recommendations are based on data, documents and other information transmitted through telecommunication systems."⁸

Telehealth has often been used interchangeably with Telemedicine. Telehealth is, however, a more encompassing term, that goes beyond curative medicine. It is understood to mean "the integration of telecommunication systems into the practice of protecting and promoting health."⁹ eHealth on the other hand refers to "Internet-based health care delivery" and refers to "all forms of electronic healthcare delivered over the Internet."^{9,10}

Dr. Portia Fernandez-Marcelo, Director of the National Telehealth Center, reports that the University of the Philippines Manila - National Telehealth Center (NTHC) embarked on telemedicine in 2004-2006 through the support of the Commission of ICT.¹¹ From its inception, the National Telehealth Center was envisioned to be a means for improving health outcomes in the Philippines. Since 2008, the NTHC has been supporting the Department of Health Doctors to the Barrios (DOH DTTB) through telemedicine.¹¹

Telemedicine utilizes Information and Communication Technology (ICT) to allow a physician, usually a general practitioner in a distant community, to consult with specialists, called domain experts, in the Philippine General Hospital. The general physicians, including the DOH Doctor to the Barrios or the Municipal Health Officer in a rural or disadvantaged community, referred to as the remote physicians, are able to consult with specialists in the Philippine General Hospital through SMS (short messaging system using cellular phones) or electronic mail.

Corresponding author: Ivy D. Patdu, MD, JD
National Telehealth Center
National Institutes of Health
University of the Philippines Manila
3rd Floor IT Complex, Philippine General Hospital
Taft Ave., Ermita, Manila 1000 Philippines
Telephone: +632 5091003
Email: ivypatdu@yahoo.com

Radiographs and other diagnostics are transmitted electronically and interpreted by specialists based in other regions. In geographically isolated and disadvantaged areas, where physical access to health facilities may be a problem, or where there is lack of qualified practitioners to attend to patients, availability of Telemedicine services improves access to healthcare of disadvantaged communities.

Materials and Methods

This paper is based on the roundtable discussions held on October 15, 2011 and December 17, 2013 on the "Legal framework of Telehealth and eHealth in the Philippines." The participants of the roundtable discussions belonged to different sectors and included stakeholders in Telehealth, legal consultants, members of the Academe, Physicians, Nurses, representatives from the Department of Health, and information technology experts. The roundtable discussions identified key issues such as the nature of the practice of telemedicine, liability issues for stakeholders, and the privacy concerns in Telehealth.

In other countries, Telemedicine is a practice already governed by rules and regulations. In the Philippines, there is no law that specifically regulates Telehealth or eHealth. There are existing laws, however, that will have an impact on Telemedicine and eHealth initiatives. The effectiveness of the full implementation of the National Telehealth Service Program (NTSP) will be guaranteed only if these laws are considered in all policy and program development. Given the realities in the healthcare delivery system in the Philippines, law and policy should be geared towards development of Telehealth or eHealth rather than becoming legal stumbling blocks to achieving the greater purpose of addressing the inequity in health.

In evaluating the issues threshed out in the roundtable discussions, the paper considers the emerging practice in Telemedicine in the context of relevant laws and jurisprudence. It proceeds from the premise that even in the absence of local laws that specifically address the current practice of Telemedicine, the implementation of the NTSP is not without legal implications, particularly on issues of liability and data privacy and security. Recommendations on legal safeguards in the implementation of the NTSP were outlined based on the results and discussion.

Results and Discussion

The National Telehealth Service Program, in its full implementation, envisions to maximize the use of information and communications technology to improve the delivery of health care. The delivery of health services over a distance, involving medical specialist referral services and patient consultations, raises questions on the extent of the physician-patient relationship established, the liability of the participants and the NTHC, and legal implications of the acknowledged inherent limitations of the practice of

telemedicine. The processes in the NTSP involves data collection and processing of personal and sensitive health information, and inevitably, the issues of data privacy, confidentiality and security become paramount.

Accountability and Liability

1. Practice of Medicine

In the roundtable discussions, one constant issue was whether the practice of telemedicine is to be considered practice of medicine. Under the Medical Act of 1959, the practice of medicine has been defined:

Section 10. *Acts constituting practice of medicine.* A person shall be considered as engaged in the practice of medicine (a) who shall, for compensation, fee, salary or reward in any form, paid to him directly or through another, or even without the same, physically examine any person, and diagnose, treat, operate or prescribe any remedy for any human disease, injury, deformity, physical, mental or physical condition or any ailment, real or imaginary, regardless of the nature of the remedy or treatment administered, prescribed or recommended; or (b) who shall, by means of signs, cards, advertisements, written or printed matter, or through the radio, television or any other means of communication, either offer or undertake by any means or method to diagnose, treat, operate or prescribe any remedy for any human disease, injury, deformity, physical, mental or physical condition; or (c) who shall falsely use the title M.D. after his name.¹²

Under Section 10(a), physical examination of a person is a pre-requisite to be considered practicing medicine.¹³ Under this definition, the practice of telemedicine, particularly the domain expert, who provides advice to the DTTB or other remote physicians from a distance, should not be considered practice of medicine because of the absence of the requirement of physical examination. This interpretation according to the letter of law was challenged. First, some of the domain experts participating in the round table discussion felt that they were practicing medicine even if merely giving advice. Second, it was also raised that it would be more prudent to assume that physicians providing telemedicine service are considered practicing medicine. This issue, being a novel question, would be resolved with finality when challenged before the courts or when legislature chooses to define it under a new law.

It is submitted, however, that the point of contention on whether telemedicine is practice of medicine has limited practical relevance with regard to establishing liability for those practicing telemedicine. The provision in the Medical Act defining what acts constitute the practice of medicine

finds application when a person without a license to practice is being made liable for *illegal practice of medicine*.¹⁴ Under the Medical Act, no person shall engage in the practice of medicine without a valid medical license.¹⁵ The consequence is that if a person is practicing medicine without a license then the person will be liable for *illegal practice of medicine*.¹⁴

In telemedicine, the remote physicians and domain experts, being physicians, are presumed to have the license to practice medicine. There is no law or rule in this jurisdiction that lays down additional requirements for the physician to practice telemedicine that could serve as basis for charging *illegal practice of telemedicine*. This does not mean, however, that the person or physician practicing telemedicine will never incur liability, or will be free to do as he or she pleases without responsibility or accountability. In determining liability, whether a physician practicing telemedicine has a duty of care to the patient becomes a more important question than whether a physician practicing telemedicine is to be considered practicing medicine under the Medical Act.

2. Physician-Patient relationship and Duty of Care

In order for liability to attach to a physician as a consequence of the management of a patient, the physician-patient relationship must first be established. The physician-patient relationship establishes a duty of care on the part of the physician for the benefit of the patient.

If there is no duty of care between a physician and a patient, there can be no liability. The Supreme Court had occasion to define when a physician-patient relationship is generated. Thus—

When a patient engages the services of a physician, a physician-patient relationship is generated. And in accepting a case, the physician, for all intents and purposes, represents that he has the needed training and skill possessed by physicians and surgeons practicing in the same field; and that he will employ such training, care, and skill in the treatment of the patient.¹⁶

There is no question that there is a physician-patient relationship between the remote physician and the patient who consults with him or her. This relationship is, however, not clearly established in relation to the domain expert. Under the NTSP, consent is obtained from the patient to transmit health data for medical specialist consultation. There is generally no communication between the patient and the domain expert. Personal identifiers are removed from the health data before it reaches the medical specialist or domain expert. Given this process, it falls under grey area whether a physician-patient relationship is established between the patient who provides consent for transmission of health data to the domain expert, and the latter who provides advice only to the remote physician based on de-identified data.

In other jurisdictions, the Court inquires into the facts of the case, particularly the extent by which the remote physician exercised independent control on the treatment of the patient, and whether a reasonable expectation of care on the part of the patient has been created.¹⁷ If the element of control is looked into, the domain expert does not exercise control over the management of the patient. Domain experts given de-identified information are strictly giving only advice and the final management plan of the patient is left to the discretion of the remote physician. Under this framework, the primary relationship that is established remains to be a doctor-patient relationship between the patient and remote physician. The existing relationship between the remote physician and the domain expert has been likened to informal consultations between colleagues. Features that suggest an informal consult include the following:

1. The consulting physician has not examined the patient.
2. The consulting physician has no direct communication with the patient.
3. The consulting physician does not review the patient's records.
4. The consulting physician has no obligation for formal consultation.
5. The consulting physician receives no payment for services.
6. The consulting physician gives opinion and advice solely to the treating physician.
7. The treating physician remains in control of the patient's care and treatment.¹⁷

The general rule, based on a review of court decisions in the United States is that "a physician contacted by a treating physician to discuss medical concerns or options related to a patient does not form a legal relationship with the patient whose care is being discussed."¹⁷ Informal consultations between colleagues are generally viewed as a service to a medical colleague.

In response to this, it was raised in the Round Table Discussion that the practice of telemedicine is more than an informal consultation, but utilizes a system within an institution, with participants agreeing beforehand on the service that they will provide. The fact that the provision of telemedicine services is institutionalized have raised concerns that the domain expert can no longer be shielded from liability by claiming that the advice given is merely recommendatory, advisory or a service to a colleague.

In cases where there is a pre-existing understanding that a physician has a duty of care to the patient, as for example an on call status, or a supervisory role, or what has been termed invisible specialists like radiologists and pathologists, a duty of care on the part of the physician is established for the benefit of the patient. If the same principle is applied to telemedicine, then when the remote physician consults with the domain expert with the express consent of the patient,

the patient may be viewed as agreeing to receive medical services from the domain expert, with the consulting physician acting as an agent for the patient in contracting the service of the domain expert. This would imply that a physician-patient relationship would exist between the patient and the domain expert.

In terms of practical application, it must be understood that even if the domain expert is to be considered as providing services only in an advisory capacity, the domain expert still has the duty of care with regard to providing his medical advice. The Civil Code contains provisions on the "Abuse of Rights", to the effect that all persons have the duty to observe due care in their relationship with others.¹⁸ Therefore, whether there is a physician-patient relationship between the domain expert and patient or whether only a physician-physician relationship is established (between domain expert and remote doctor), the domain expert must still observe due diligence. The distinction would be important in determining to whom the domain expert owes the duty of care. If a physician-patient relationship is established, the domain expert will be liable to the patient, as the domain expert will be presumed to have a duty of care for the benefit of the patient. If only a physician-physician relationship is established, in case of negligent advice, the domain expert may be liable to the remote physician. In this case, the domain expert still accepts the duty of providing medical advice. The fact that the domain expert does not appear to have a direct relationship with the patient does not mean that the domain expert can provide advice without exercising due care.

3. Breach of Duty and Standard of Care

Based on the preceding discussion, what is evident is that a participant in Telehealth, will have a duty of care, whether domain expert or remote physician, and whatever may be the relationships established. Liability, to be established, requires a showing of breach of this duty that results to patient injury.

Under current laws and jurisprudence, the general rule is that duty of care exists whenever a person attempts to render medical assistance. If the person does not possess the necessary skill or competence to treat a patient, the person may be liable if the patient suffers an injury as a result of the treatment. Whether that person is a licensed physician is not material. The Supreme Court stated—

[T]he accused acted with reckless negligence in diagnosing, prescribing for, and treating the deceased xxx knowing that she did not possess the necessary technical knowledge or skill to do so, thus causing her death xxx [O]rdinary diligence counsels one not to tamper with human life by trying to treat a sick man when he knows that he does not have the special skill, knowledge, and competence to attempt such treatment and cure,

and may consequently reasonably foresee harm or injury to the latter. In a similar case wherein the accused, not being a regular practitioner, undertook to render medical assistance to another, causing physical injuries to the latter, said accused was found guilty and convicted xxx¹⁹

This means that a person may be found liable if injury to a patient results from the commission of an act that the said person is not qualified to perform, and if it can reasonably be foreseen that said injury could occur. For example, a person without training in surgery should not operate, because harm to the patient can reasonably be expected when an unqualified person performs surgery on him or her. In the context of telemedicine, a person who is not qualified to provide medical advice through telemedicine should not do so.

In the medical liability system in our country, the physician may be made administratively, civilly or criminally liable. Administrative grounds that could lead to a reprimand, suspension or revocation of license to practice are provided in the Medical Act of 1959, the Code of Medical Ethics, and special laws. Civil liability is founded on the principle of quasi-delict provided in article 2176 of the Civil Code which makes a person liable for damages, if his negligence is the proximate cause of the injury of another. A physician may also be criminally liable for a negligent act that results to patient injury under article 365 of the Revised Penal Code, providing for criminal negligence. In a criminal medical negligence, the question is whether the physician has exercised an inexcusable lack of precaution which defined as—

Whether or not a physician has committed an "inexcusable lack of precaution" in the treatment of his patient is to be determined according to the standard of care observed by other members of the profession in good standing under similar circumstances bearing in mind the advanced state of the profession at the time of treatment or the present state of medical science.²⁰

In medical negligence under the Civil Code, whether a physician has breached his duty of care requires an inquiry into the standard of care. It has been discussed as—

A doctor's duty to his patient is not required to be extraordinary. The standard contemplated for doctors is simply the reasonable average merit among ordinarily good physicians, reasonable skill and competence.²¹

By implication, there is breach of duty if there is failure to observe the standard of care. The question would be what standard of care would be required for the physicians involve in the practice of telemedicine. There is a duty of care on the part of the remote doctor and domain expert. The remote physician has a duty to manage the condition of the patient consulting him for a medical condition. At the very

least, the domain expert has a duty to provide medical advice with ordinary diligence.

The remote doctor, who is usually a general practitioner, a DTTB or a Municipal Health Officer, has a duty of care which requires that he or she uses at least the same level of care that any other reasonably competent physician would use to treat a patient under similar circumstances. As a general practitioner, the remote expert does not have the obligation to meet the standard of care provided by specialists, but only that standard of care observed by physicians under similar circumstances. In seeking advice from a specialist physician through telemedicine, he is actually doing a service to the patient.

The following ethical principles from the Code of Medical Ethics may find relevance:

Section 3. In cases of emergency, wherein immediate action is necessary, a physician should administer at least first aid treatment and then refer the patient to a more qualified and competent physician if the case does not fall within his particular line.

Section 4. In serious cases which are difficult to diagnose and treat, or when the circumstances of the patient or the family so demand or justify, the attending physician should seek the assistance of his colleagues in consultation.²²

In this framework, the critical point would be for the remote physicians to know when a particular case is beyond their competence. This means stabilizing an emergency patient, making prompt referrals if a case is beyond his competence, and arranging for transfer to another health care facility if required by the patient's condition. If transfer is not possible, the physician would still need to competently manage the patient to the best of his abilities. The telemedicine consult and how it may assist in the management of the patient is just an aspect of patient care for the benefit of the patient.

In the case of the domain expert providing advice to a colleague, he must still exercise that reasonable care and caution which an ordinarily prudent person will use in the same situation. One question raised in the Round Table Discussion is whether the standard of care expected of the domain expert is the same as the standard of care expected from physicians who are providing care with the benefit of a face-to-face consult and physical examination. Under our laws, ordinary diligence requires an inquiry into what a prudent person will do in the same situation. The situation of the domain expert is different in many respects from the traditional physician-patient relationship. Telemedicine is subject to limitations of technology, and requires providing an opinion or advice based on limited information inherent in the nature of the consult. Whether the domain expert has breached his or her duty should be determined based on the standard of care observed by other healthcare providers

providing similar medical services through telemedicine. To require more would be inconsistent with the test of negligence established in jurisprudence and a disservice to the goals of improving health care delivery.

If the duty of care of the domain expert is the same as the duty of the specialist providing medical care in the traditional face-to-face consult, then by implication, the domain expert shall always be providing treatment below the expected standard of care. In the context of the traditional relationship between patient and physician that exists in face-to-face consults, the physician should advise about a patient's management only if he has the benefit of a complete physical examination. Under this line of reasoning, the practice of telemedicine will be inherently negligent and should therefore not be pursued, unless advancements in technology would allow the Telehealth consultations to be closely similar if not the same as traditional face-to-face consults. If this view is accepted, it would imply giving up the potential of what Telehealth contributes to the health system.

The thrust of the government, in order to fulfill its duty under the constitution to protect and promote the right to health of the people, is to develop Telehealth services, promote its use and support its growth and continued improvement to the end that quality health services are made available to all the people at an affordable cost.^{23,24} There is public interest in providing Telehealth services, especially in areas where no medical specialists are available. It will be more consistent with public policy to recognize that the standard of care of the domain expert is not the same as the physician managing a patient under the traditional setting. That standard should be based on what is expected of someone who practices telemedicine by providing an advice to a colleague. The domain expert who provides advice must give reasonable advice, based on his skills and competence, but the duty expected of him should consider the limitations of technology, and the fact that the information upon which the advice is based will not be the same as the information that may be obtained in a face-to-face consult.

4. Institutional Liability

The National Telehealth Center is the primary institution providing telemedicine services to the underserved. In fulfilling its functions within the context of a national program, the National Telehealth Center is performing a governmental function. Governmental functions are those that concern the health, safety and the advancement of the public good or welfare as affecting the public generally.²⁵ In our jurisdiction, a government hospital performing a governmental function is generally considered to be immune from suit.²⁶ The National Telehealth Center, being a government agency, presumably enjoys immunity from suit. This immunity is founded on the Constitutional provision, declaring that the State may not be sued without

its consent.²⁷ This provision is premised on a recognition of the sovereign character of the State and an express affirmation of the unwritten rule effectively insulating it from the jurisdiction of courts.

While the government is immune from suit, immunity is different from suability. The NTHC may be sued, in which case, it may raise its immunity as a defense. This immunity, however, applies only to a damage suit, but does not extend to personal actions that may be brought against the participants such as the domain experts or remote physicians. These physicians may be brought to court for civil or criminal charges, or to the Professional Regulation Commission (PRC) for an administrative complaint where they stand to lose their license. The liability of NTHC will be limited to the civil aspect and NTHC may continue to invoke its defense of immunity. To a limited degree, if the participants claim they are performing public functions and acting within the parameters of authority, or they are acting as agents of the NTHC, the immunity may extend to them.

While the National Telehealth Center may be presumed to enjoy immunity from suit, there was still some discussion in the panel with regard to the possible liability of NTHC in failing to provide services according to the legal concept of the standard of care. The roundtable discussions recognized that defining the “standard of care” might be a legal pitfall. Under jurisprudence, a breach of duty follows from failure to observe the standard of care. If the standard of care is defined then a breach of duty may be deduced even without the need for experts by simply pointing out a particular written standard which has not been followed.

On the practical aspect, it would be unrealistic to define in detail the standard of care because of the numerous facets involved in providing Telehealth services. Medicine is complex in itself, and the science of healing is never exact. Telemedicine goes beyond medicine in that it involves the use of available information and communications technology. The determination of standard of care for telemedicine requires an understanding of the process of providing care over a distance, the inherent limitations both from the practice and the technology. The standard of care, when inquired upon, should thus be determined based on prevailing telemedicine practice.

An agreement that it would be difficult to define the standard of care does not mean that the National Telehealth Center is precluded from implementing guidelines for the practice of Telemedicine. These guidelines will provide for the internal policies on accreditation, certification, operational framework, privacy and security. Internal policies do not define the standard of care but they affirm that even in the absence of a specific law governing telemedicine, there is a responsibility to exercise due care in the provision of telehealth services.

To this end, the National Telehealth Center has engaged in the training, accreditation or certification of persons

participating in the provision of health services through Telehealth or e-health. In including capability building and training as a component of NTSP, there is recognition that even if there are no statutory requirements in place, the person practicing telemedicine will need additional skills and knowledge.

In addition to certification, the National Telehealth Center will have statutory duties under the law. Guidelines or internal policies will have to consider these laws. Legislations that must be considered include the Data Privacy Act, the Electronic Commerce Act, and the Anti-Wiretapping Act. The Data Privacy Act imposes duties on those who process and control personal and sensitive information, which would include the National Telehealth Center.²⁸ The provisions in the Data Privacy Act are also important with regard to the requirement of obtaining informed consent in the processing of health data. The Electronic Commerce Act applies to any kind of data message and electronic document used in the context of commercial and non-commercial activities.²⁹ The Electronic Commerce Act of 2000 provides that any person with access to electronic data messages or documents has the obligation of confidentiality or the duty not to convey the information to, or share it with, any other person.³⁰ Under this law, unauthorized access to computer systems is punishable by a fine and mandatory imprisonment.³⁰ The Anti-Wiretapping Law may also be applied where a person who is not authorized by parties to a private communication record or communicate its contents.³¹

While the risk for liability of the NTHC may be minimal, it has to be cognizant of its responsibilities, not only for accountability, but in order to provide quality service to patients, and to achieve its public health purpose.

Privacy, Confidentiality and Security

The right to privacy is enshrined in the constitution.³² One aspect of this right is information privacy. Today, information is power, and people have come to recognize that they have a right to keep as private all types of personal information. In the era of great advancements in information and communications technology, and the Internet, huge amount of personal data can be stored and transmitted electronically and can be readily accessible when no safeguards are in place.

Health information, for a patient, is highly personal and very private. In providing information to healthcare providers, patients make themselves vulnerable, and they open up to the physicians, disclosing innermost secrets at times. This is premised on the belief that full disclosure would improve the care they would receive, and that the physicians will hold as sacred their duty of confidentiality. Indeed, the Hippocratic oath requires the physician to respect the privacy of patients.^{33,34} The physician has an ethical duty to hold as sacred and highly confidential

whatever may be discovered or learned pertinent to the patient even after death.^{35,36} Under the Rules of Court, the communication between physicians and patient is considered privileged communication.³⁷

This duty of confidentiality to patients takes a new dimension in the context of Telehealth. The advancements in technology present new challenges to maintaining health privacy. Under the NTSP, personal health information is being stored, processed and transmitted through ICT and the Internet. Information gathered by a remote physician is shared with the domain expert. The patient's information is also processed and transmitted for public health purposes. This means patients will no longer just worry about whether the physician in a face-to-face consult will talk about private information with other people, but they have to contend with the risk that information transmitted through technology will be susceptible to unauthorized access or cyber-attacks.

The existence of risks only means that in providing telehealth services, due regard for patient privacy should be a priority. Respect for privacy, in general, is provided in the Constitution, and further articulated in the Civil Code.³⁸ There are also specific health privacy legislation that imposes duties on health care providers and those who handle patient records, including: (1) Philippine AIDS Prevention and Control Act of 1998 (Republic Act No. 8504) imposes the duty of maintaining patient confidentiality, both the identity and status, of persons with HIV, on all persons involved in handling and maintaining patient records; (2) Comprehensive Dangerous Drugs Act of 2002 (Republic Act No. 9165) provides for the confidentiality of records of those who have undergone drug rehabilitation; and Anti-Violence Against Women and Their Children Act of 2004 (Republic Act No. 9262) provides for the confidentiality of records pertaining to cases of violence against women and their children.^{39,40,41}

In 2012, the Data Privacy Act was enacted into law.²⁸ The Act applies to the processing of all types of personal and sensitive information. Processing refers to any operation performed upon personal information including the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.⁴² The law would apply to the National Telehealth Center, and in the implementation of the NTSP, the provisions of the Data Privacy Act should be complied with. It must be noted that the law provides that it shall not apply if personal information is processed for research purposes, or to information necessary to carry out the functions of public authority.^{43,44} While the NTSP may be included in these exceptions, it would be more prudent to observe the principles provided by law in the processing of personal health data, which under the law is considered both personal and sensitive.^{45,46}

In complying with requirements of the law in processing of personal and sensitive information, the Data Privacy Act adheres to the principles of transparency, legitimate purpose and proportionality in the collection and processing of data.⁴⁷ The principle of transparency requires that processing of personal information must be open, and known to the person providing information (data subject). To a limited degree, the data subject must be able to influence the processing of data, such as being given reasonable access and means to correct data, adequate information on the processes involved, and options to withhold or revoke consent. The principle of legitimate purpose requires that data be processed fairly and lawfully, and that data is collected for a specified purpose that must not be contrary to law or public policy. The principle of proportionality requires that the amount of data to be collected and processed will not exceed that which is necessary for the purpose of processing, and limited only to data that is relevant or accurate and that to which consent has not been given. The personal or sensitive information should also not be retained longer than necessary to achieve the specified purpose. These general principles should guide the internal policies of the National Telehealth Center.

The Data Privacy Act also requires that the person providing information (data subject) must give consent prior to the collection and processing of personal and sensitive information.⁴⁸ In the implementation of NTSP, the data subject is the patient, and the information is usually provided by the patient to a remote doctor. In order to comply with the requirements of the law, the patient must agree to the collection and processing of his or her health data. This consent must be freely given after being informed of what data will be collected, transmitted and processed including the purpose and intended possible uses of data collected. The benefits, potential risks, limitations of Telehealth services and the fact that security measures are in place to minimize risks must be also known to the patient. If a patient does not consent to a telemedicine consult, patient autonomy should be respected. In all cases, the patient must be given the option to withhold or revoke consent.

The Data Privacy Act likewise requires the data controller to put in place security measures for the protection of processed data. Under the NTSP, the National Telehealth Center collects, holds and processes personal information. This implies that the duties and responsibilities of a personal information controller would be imposed on the NTHC. One of these obligations is the requirement to implement organizational, physical and technical security measures.⁴⁹

Organizational security measures will require an inquiry into the policies and procedures observed by NTHC. In setting parameters for collection, processing and storage of information, the protocol should be geared towards protecting patient privacy, and should adhere to guiding

principles of transparency, legitimate purpose and proportionality. There must be protocols in place in case of security breach or other technical problems. The duties and responsibilities of data collectors and handlers must be clearly identified in order to evaluate accountability in case of security breach or related problems. One of the recommendations in the panel is to have data security and privacy officers who will be in charge of implementing rules on different aspects of security at all stages of data handling, as well in evaluating and monitoring compliance with security measures.

The need for physical security looks into measures that would prevent unauthorized physical access to health data, and would include looking into the facility and equipment where information is collected or stored. The technical aspect of security requires putting in place safeguards in the network and computer systems. These would include use of privacy-enhancing technology and software that would protect data and network security. Security measures should allow data encryption, and de-identification, and putting in place effective authentication process such as passwords or automatic log-out in computer systems, role-based access and other processes to control and limit access to electronic data.

The emphasis on privacy and security is warranted because the Data Privacy Act imposes penalties for violation of its provisions, and is applicable even to government officials and employees. Acts that are punishable under the law include: Unauthorized processing of personal and sensitive information (sec. 25), Accessing personal information due to negligence, both for the person who actually gained access, and the person who allowed access due to negligence (sec. 26), Improper disposal or personal and sensitive information (sec. 27), Processing of personal or sensitive information for unauthorized purposes (sec. 28), Unauthorized access or intentional breach through breaking into any system where personal or sensitive information is stored (sec. 29), Concealment of security breaches (sec. 30) and Malicious (sec. 31) and unauthorized disclosure (sec. 32).⁵⁰

Conclusion

The National Telehealth Service Program aims to address the inequity in health, and to utilize the advancements in information and communication technology to improve health outcomes in the country. While there are no laws that govern Telehealth, there are existing laws that would affect its implementation. These laws should not be a hindrance to the development and sustainability of the NTSP but rather should serve as means of improving the quality and accessibility of Telehealth services without compromising the rights of the patients and all other persons involved in providing Telehealth Services.

The Round Table Discussions were effective in identifying key issues such as the nature of the practice of telemedicine, liability issues for stakeholders, and the

privacy concerns in Telehealth. Their legal implications were discussed from the point of view of the different stakeholders and participants from various disciplines. The recommendations discussed in the preceding sections have been summarized below.

Accountability and Liability

The duty of care for physicians practicing telemedicine should take into consideration the limitations of technology and the inherent differences between telemedicine and face-to-face doctor-patient consultations. The standard of care to be observed by physicians engaged in providing health care through telemedicine should be that standard observed by other members of the profession in good standing and similarly engaged in telemedicine, taking into consideration the state and prevailing practice of telemedicine in the country.

The domain expert is providing medical specialty advice. The final discretion on the management of the patient remains to be the professional responsibility of the remote physician, who is directly in contact with the patient.

In order to afford protection to the stakeholders:

1. The remote doctors must have an agreement either by contract or memorandum that they remain to be the primary physician of the patient with full control over the patient's management. The nature of the medical specialty consult with a domain expert is only advisory.
2. The remote doctors, in practicing their profession, must recognize an emergency, and know when to refer, at all times informing the patient of the management plan, and limitations of the physician and facility.
3. Domain experts in providing advice to the remote doctor must exercise due diligence. In giving advice, domain experts should always have a caveat that clinical correlation is required, and advice is based on limited information available.
4. Patient must give his or her consent to the Telemedicine consult, understanding that the advice to be given is only recommendatory, and such advice shall be given without a face-to-face consult and other limitations inherent in Telemedicine.

The absence of a law governing telemedicine is not a hindrance to the National Telehealth Center to implement and continually improve its policies for the provision of health services through telemedicine. While the National Telehealth Center may raise immunity from suit as a defense for civil cases for damages, it has to observe statutory duties in the processing of health data as well as a general duty of care to patients availing telemedicine service.

The National Telehealth Center should review its manual of operations and existing protocols. Policies should be in place that would serve as guidelines for operations, certification and training, monitoring and evaluation. The National Telehealth Center should continue capability building through training and certification, and continue to support research and further technological development. Stakeholders to telemedicine should have an understanding of the processes involved in telehealth, the limitations of technology, and the risks associated with telehealth. In improving quality, there must likewise be policies in place for monitoring and review of existing programs and processes.

Privacy, Confidentiality and Security

The National Telehealth Center should develop policies to ensure compliance with requirements of law, particularly with regard to the processing of personal health information. The principles of transparency, legitimate purpose and proportionality in the collection and processing of personal data should be incorporated in these policies. NTHC should also actively put in place organizational, physical and technical security measures to protect patient privacy and comply with requirements of the Data Privacy Act:

1. Establish protocol for obtaining patient consent prior to processing of health data and availing of telemedicine services.
2. Clear guidelines in place on the extent of information to be collected, transmitted and further processed as well as policy with regard to disposal of data.
3. Purpose for collection of data should be identified and should be made known to the patient. It is likewise important that patient is aware of options in withholding or revoking consent.
4. There must be a framework for the processing of data, from the time of collection to disposal, which should include a clear description of duties of all those who handle patient information, the points of access to the information being handled, both physical and electronic access, and guidelines with regard to de-identification of patient information.
5. The NTHC should implement technical measures to protect data and network security.

References

1. Poverty Incidence for Basic Sectors, Philippine Statistics Authority, National Statistics Coordinating Board [Online]. [cited 2014 Sept]. Available from <http://www.nscb.gov.ph/poverty/>.
2. Bernabe K. Health Care beyond reach of poor, say critics. *Philippine Daily Inquirer* [Online]. 2010 [cited 2014 Sept].

- Available from <http://newsinfo.inquirer.net/inquirerheadlines/nation/view/20100413-263926/Health-care-beyond-reach-of-poor-say-critics>.
3. Department of Health, Distribution of Licensed Private Hospitals and Other Health Facilities by Service Capability/Authorized Beds by Center for Health Development, Year 2005, in Database [Online]. 2005 [cited 2008 June]. Available from http://www2.doh.gov.ph/bhfs/hosp/pvthosprovcit_05.pdf.
 4. 2011-2016 National Objectives for Health, Health Sector Reform Agenda Monographs 8-9 [Manila, Republic of the Philippines – Department of Health, 2011 (DOH HSRA Monograph No. 12).]
 5. Editorial ‘Doctors to the Barrios’ *Philippine Daily Inquirer* [Online]. 2012 November 3 [cited 2013 July]. Available from <http://opinion.inquirer.net/40754/doctors-to-the-barrios#ixzz2YS1COapl>.
 6. Crisostomo S. PMA warns of worsening shortage of doctors. *The Philippine Star* [Online]. 2014 Jan 31 [cited 2014 Sept]. Available from <http://www.philstar.com/headlines/2014/01/31/1285056/pma-warns-worsening-shortage-doctors>.
 7. Official Web Site of the Philippine Medical Association. 2005 Medical Summit [Online]. [cited 2007 Dec]. Available from http://www.pma.com.ph/2006_09MedicalSummit.asp.
 8. World Medical Association Statement on the Ethics of Telemedicine, Adopted by the 58th WMA General Assembly. Copenhagen, Denmark. October 2007.
 9. Maheu M, et al. eHealth, Telehealth, and Telemedicine 3 citing World Health Organization (1997). 2001.
 10. Maheu M, et al. eHealth, Telehealth, and Telemedicine 3 citing McLendon. 2001.
 11. Fernandez-Marcelo P. Updates on the National Telehealth Service Program, National Telehealth Center University of the Philippines – Manila. April 8, 2011.
 12. The Medical Act of 1959 [Medical Act], Republic Act No. 2382. 1959. p. 10; An Act to Amend Certain Sections of Republic Act No. 2382, otherwise known as “The Medical Act of 1959,” Republic Act No. 4224. 1965. Republic Act No. 4224 amends sections 3-7, 9-16, and 18- 21 of the Medical Act of 1959.
 13. Solis PP. *Medical Jurisprudence*. 1998. pp. 38-9.
 14. Tuano LV. G.R. No. 178763. April 21, 2009.
 15. Olick RS, Bergus GR. Malpractice liability for informal consultations. *Fam Med*. 2003; 35(7):476-81.
 16. An Act to Ordain and Institute the Civil Code of the Philippines [New Civil Code], Republic Act No. 386, arts. 19-21. 1950.
 17. *People vs. Vda. de Golez*, 108 Phil. 855, 859 citing *U.S. vs. Feliciano Divino*, 12 Phil., 175. 1960.
 18. *Cruz vs. Court of Appeals*, 282 SCRA 188, 199-200. 1997.
 19. *Runez v. Jurado*, A.M. No. 2005-08-SC. December 9, 2005.
 20. Code of Ethics, Professional Regulation Commission Board of Medicine, art II, Section 3-4.
 21. Philippine Constitution. Art 2. p. 15.
 22. Philippine Constitution. Art XIII. p. 11.
 23. *Republic v. City of Davao*, 388 SCRA 691. 2002.
 24. Solis PP. *Medical Jurisprudence*. 1998. pp. 313-5.
 25. Philippine Constitution. Art XVI. p. 3.
 26. An Act Protecting Individual Personal Information in Information Systems in the Government and the Private Sector, Creating for this Purpose A National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], R.A. 10173. 2012.
 27. An Act Providing for the recognition and use of electronic Commercial and Non-Commercial Transactions and Documents, Penalties for Unlawful use therefor and other purposes, [Electronic Commerce Act of 2000], R.A. 8792. 2000.
 28. R.A. 8792, Electronic Commerce Act of 2000. pp. 5,7,31-3.
 29. An Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication, and for Other Purpose [Anti-wiretapping law], R.A. No. 4200. 1965. pp. 1-2.
 30. Philippine Constitution. Art III. pp. 1,2,6,8,17.
 31. Hippocratic Oath. The World Medical Association Declaration of Geneva, Physician’s Oath [Online]. 1948 [cited 2014 Sept]. Available from <http://medical-dictionary.thefreedictionary.com/Hippocratic+Oath>.

32. Code of Ethics, Professional Regulation Commission Board of Medicine, art II. p. 6. Code of Ethics, Philippine Medical Association, art 2. p. 6.
33. Revised Rules of Evidence, Rules of Court, Rule 28. 1989. p. 24(c).
34. An Act to Ordain and Institute the Civil Code of the Philippines [NEW CIVIL CODE], Republic Act No. 386, art. 26 and 32. 1950.
35. Prevention and Control of HIV/AIDS in the Philippines, Instituting a Nationwide HIV/AIDS Information and Educational Program, Establishing a Comprehensive HIV/AIDS Monitoring System, Strengthening the Philippine National Aids Council, and for Other Purposes, "Philippine AIDS Prevention and Control Act of 1998", Republic Act No. 8504. February 13, 1998.
36. An Act Instituting the Comprehensive Dangerous Drugs Act of 2002, Repealing Republic Act No. 6425, Otherwise Known as the Dangerous Drugs Act of 1972, as Amended, Providing Funds Therefor, and for Other Purposes, "Comprehensive Dangerous Drugs Act of 2002", Republic Act No. 9165. June 7, 2002.
37. An Act Defining Violence Against Women and Their Children, Providing for Protective Measures for Victims, Prescribing Penalties Therefore, and for Other Purposes, "Anti-Violence Against Women and Their Children Act of 2004", Republic Act No. 9262. March 8, 2004.
38. Updates on the National Telehealth Service Program, National Telehealth Center University of the Philippines – Manila. April 8, 2011. Code of Ethics, Professional Regulation Commission Board of Medicine, art II §6; *See also* Code of Ethics, Philippine Medical Association, art 2 §6.
39. Updates on the National Telehealth Service Program, National Telehealth Center University of the Philippines – Manila. April 8, 2011. Lucas v. Tuano G.R. No. 178763, April 21, 2009.
40. An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for other purposes, Data Privacy Act 2012, Republic Act No. 10173. 2012.
41. Data Privacy Act of 2012. p. 3(j).
42. Data Privacy Act of 2012. p. 4(d).
43. Data Privacy Act of 2012. p. 4(e).
44. Data Privacy Act of 2012. p. 3(h).
45. Data Privacy Act of 2012. p. 3(l).
46. Data Privacy Act of 2012. p. 11.
47. Data Privacy Act of 2012. p. 11.
48. Data Privacy Act of 2012. p. 3(b),12-3.
49. Data Privacy Act of 2012. p. 25-37.
50. Data Privacy Act of 2012. p. 20.