# THE THREATENED EROSION OF PRIVACY IN HEALTHCARE AND THE SEARCH FOR A "CURE": PURSUING A LEGAL FRAMEWORK FOR HEALTH INFORMATION PRIVACY IN EHEALTH AND TELEMEDICINE*

*Arvin Kristopher A. Razon***

**ABSTRACT**

The advances of electronic technology in the field of healthcare has placed the privacy of health information in a precarious position. More people and entities can gain access to the patient's health information. The right to privacy guaranteed by the Constitution applies only to state actors, but private players have substantial participation in how health information is processed. Remedies based on tort are limited to right to damages. Evidentiary rules on doctor-patient privilege are likewise limited for evidentiary purposes. This paper argues that health information is protected by the Data Privacy Act of 2012 and falls under the classification of sensitive personal information given utmost protection by the Act.

> *"The real danger is the gradual erosion of individual liberties through automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable."*
> —U.S. Privacy Protection Study Commission[1]

---

* *Cite as* Arvin Kristopher A. Razon, *The Threatened Erosion of Privacy in Healthcare and the Search for a "Cure": Pursuing a Legal Framework for Health Information Privacy in eHealth and Telemedicine*, 90 PHIL. L.J. 734, (page cited) (2017).

** Associate, SyCip Salazar Hernandez & Gatmaitan (2015-present); Associate Professor, University of Perpetual Help System DALTA (2016-present); J.D., Dean's Medalist for Academic Excellence (2014), B.A. Organizational Communication, *magna cum laude* (2010), University of the Philippines. Member, PHILIPPINE LAW JOURNAL, Vol. 87, 88. Member, Order of the Purple Feather (2010-2014).

[1] U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission* (1977), *available at* https://epic.org/privacy/ppsc1977report/c13.htm (last accessed on Apr. 24, 2017).

Technology has penetrated the Philippines at an unprecedented scale, to the point that it now forms an inextricable aspect of an average Filipino's life. The field of healthcare is no exception. The solutions offered by technology to the various pernicious problems in healthcare—from improving access to healthcare in geographically isolated areas to revolutionizing clinical research—are innovative and practical, so much so that it is easy to lose sight of what we are giving up in exchange of the promises of automation, integration, and interconnection.

To be specific, privacy in healthcare is often the least of a patient's concern. Where a person's health is put forth as an issue, the immediate reaction is to make an accurate diagnosis and provide adequate relief. The regard for that person's right to informational privacy is an afterthought, if considered an issue at all. But the matter of health information privacy—that is, privacy with regard to personal information processed for clinical care purposes—should no longer be summarily bypassed.

Imagine a situation where a patient who has previously undergone drug rehabilitation without state intervention and whose health information was at one point entered into a private hospital's electronic medical records. Our hypothetical patient now requires clinical care for an altogether different matter. With the current emphasis on information interoperability, his entire medical history is now laid out in the open, regardless of its relevance to his immediate health concern. Worse, if such information relating to his previous drug dependency, which has been managed and is entirely a non-issue, is shared to local government units or to law enforcement officers–there is a real possibility that his past can haunt him in undesirable ways, especially in light of the current administration's policy on the war on drugs.[2]

[2] Rep. Act No. 9165 (2002), or the Comprehensive Dangerous Drugs Act of 2002, provides for the confidentiality of records under both its voluntary and compulsory submission programs. According to § 60, "[j]udicial and medical records of drug dependents under the voluntary submission program shall be confidential and shall not be used against him for any purpose, except to determine how many times, by himself/herself or through his/her parent, spouse, guardian or relative within the fourth degree of consanguinity or affinity, he/she voluntarily submitted himself/herself for confinement, treatment and rehabilitation or has been committed to a Center under this program." According to § 64, "[t]he records of a drug dependent who was rehabilitated and discharged from the Center under the compulsory submission program, or who was charged for violation of use of dangerous drugs under Section 15 of this Act, shall be covered by Section 60 of this Act." However, the author is considering a scenario where the previous drug dependent did not undergo the voluntary submission program or compulsory submission program of the government.

The foregoing example is just one of the many possibilities, and highlights the fact that health information privacy can no longer be taken for granted considering the unpredictable growth and uncertain direction of eHealth and telemedicine. There has to be a deliberate effort to find a redress mechanism in the current laws that will allow a patient to assert his right to health information privacy, with clear consequences for the violators concerned. This effort has to be grounded in practice and theory, directly applicable and available to the average Filipino.

This paper is divided into four parts. First, the author explores the current status with regard to eHealth. Next discussed are the risks associated with the apparent lack of legal safeguards. Third, the author proceeds to examine the relevant laws that have probable application in the field. Lastly, the author argues that the Philippine Data Privacy Act can provide a legal framework for healthcare institutions and professionals to uphold the right to health information privacy. Ultimately, the author argues that consent by the patient should be the primary driver for the processing of health information by a healthcare institution or a health professional. Such consent must be specific to the purpose of the processing, and must be time-bound—that is, prior to such processing performed by the healthcare institution or health professional—and consistent with the right of the patient to self-autonomy.

## I. THE FOUNDATION OF EHEALTH AND TELEMEDICINE AND ITS ROLE IN THE PHILIPPINES

Several factors contribute to health disparities in the Philippines: (1) economic inequality and persistent poverty; (2) the high population growth rate; (3) areas inflicted with insurgency; (4) distorted development of the economy; (5) geographical makeup of the country; and (6) recurrent calamities aggravated by climate change.[3] All these factors converge to paint an unfortunate picture that is health inequity across the Philippines.

There is no one solution to persistent health disparities in the Philippines. It is after all a complex problem that requires the massive collaboration of various stakeholders. There have been, however, efforts to mitigate the increasingly pressing situation, many of which are rooted in the field of eHealth, as discussed below.

---

[3] Oscar Picazo, et al., *Explaining the Large Disparities in Health in the Philippines*, PHILIPPINE INSTITUTE FOR DEVELOPMENT STUDIES POLICY NOTES NO. 2013-08 (2013), *available at* http://dirp3.pids.gov.ph/ris/pn/pidspn1308.pdf (last accessed Apr. 19, 2017).

### A. eHealth, Telemedicine and Health Information

While the meaning of the term eHealth is contested and widely varies, eHealth covers "health, technology, and commerce."[4] Health is referred to as a "process,"[5] with technology as a "tool to enable a process/function/service and as the embodiment of eHealth itself [.]"[6] More specifically, technology is "portrayed as a means to expand, to assist, or to enhance human activities, rather than as a substitute for them."[7]

While eHealth denotes the broad field of health in information and communication technology (ICT), telemedicine is a narrower field of e-health that has existed as far back as the 1970s.[8] It is defined thus:

> [It is the] delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities.[9]

Generally, telemedicine involves four elements:

1. Its purpose is to provide clinical support.

2. It is intended to overcome geographical barriers, connecting users who are not in the same physical location.

3. It involves the use of various types of ICT.

4. Its goal is to improve health outcomes.[10]

In telemedicine, a variety of healthcare solutions, ranging from diagnosis to treatment choice, are formulated based on "data and health

---

[4] Hans Oh et al., *What is eHealth (3): A Systematic Review of Published Definitions*, 7 J. MED. INTERNET RES. 1, 8 (2005).

[5] *Id.* at 9.

[6] *Id.*

[7] *Id.*

[8] World Health Organization, *Telemedicine: Opportunities and Developments in Member States* (Report on the Second Global Survey on eHealth), 2 GLOBAL OBSERVATORY FOR EHEALTH SERIES 8 (2010), *available at* http://www.who.int/goe/publications/goe_telemedicine_2010.pdf (last accessed April 20, 2017).

[9] *Id.* at 9.

[10] *Id.*

information transmitted via telecommunications system."[11] Various ICT tools are used, such as text messaging, two-way video conferencing and email.[12] Essentially, telemedicine refers to the active delivery of clinical services.

There is no comprehensive definition of health information in the context of privacy under Philippine laws. For this purpose, the author borrows the comprehensive definition of health information found in the Privacy Act 1988 of Australia:

> (a) information or an opinion about:
>
> (i) the health, including an illness, disability or injury, (at any time) of an individual; or
>
> (ii) an individual's expressed wishes about the future provision of health services to him or her; or
>
> (iii) a health service provided, or to be provided, to an individual; that is also personal information; or
>
> (b) other personal information collected to provide, or in providing, a health service; or
>
> (c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
>
> (d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.[13]

It is also worthy to note that under the Privacy Act 1988, health information about an individual is considered sensitive information.[14]

### B. Current Trends in eHealth and Telemedicine in the Public Sector

In the Philippines, the Department of Health (DOH) has updated its eHealth framework to support universal health care in a program known as

---

[11] National Telehealth Center, *Infographic: How does telemedicine work in NTHC*, *at* https://telehealth.ph/2015/02/18/infographic-how-does-telemedicine-work-in-nthc/ (last accessed Apr. 20, 2017).

[12] *Id.*

[13] *Privacy Act 1988*, § 6FA (Austl.).

[14] Pt. II, Div. 1, § 6.

*Kalusugan Pangkalahatan*.[15] Based on the Philippines eHealth Strategic Framework and Plan 2014-2020 (hereinafter "Philippine eHealth Framework"), concrete efforts have been made to create a national eHealth policy. Three concrete measures highlight the necessity of collaboration: (a) the implementation of telemedicine in selected pilot areas, (b) the development and implementation of mobile technology solutions through the Surveillance in Post Extreme Emergencies and Disasters or SPEED, and (c) the development and implementation of several mobile technology applications, including the inventory of tuberculosis drugs and routine health data reporting.[16]

A critical eHealth component for the implementation of the Philippine eHealth Framework is "the widespread adoption of health information systems and technologies standards/health data standards (HISS/HITS/HDSs) to improve the accessibility, availability, exchange and use of medical/health information across geographical and health sector boundaries."[17] Clearly, the national eHealth policy relies on the creation of networks and information systems that collect, share, and exchange information for more responsive solutions that will ultimately benefit Filipinos. There is an emphasis on collaboration among sectors to further the national health agenda: government agencies (such as the DOH and Department of Science and Technology (DOST)), private firms or organizations, local government units, non-government organizations, the academe, research institutions, and international organizations are included in such agenda.

To implement the Philippine eHealth Framework, the DOH and DOST constituted the DOH-DOST National Governance Steering Committee and Technical Working Group on eHealth through the Joint DOH-DOST Department Memorandum No. 2013-0200.[18] The partnership between DOH and DOST affirms the intersection of ICT and quality health services in implementing the national eHealth policy.

The government aims to provide health services to far-flung areas through telemedicine. The National Telehealth Center, a government arm focused on telehealth, has developed the National Telehealth Service

---

[15] Dep't of Health (DOH), *Philippines eHealth Strategic Framework and Plan 2014-2020*, at 5, *available at* http://ehealth.doh.gov.ph/images/eHealthPDF/PeHSFP20132017.pdf (last accessed Apr. 20, 2017).

[16] *Id.* at 6.

[17] DOH, Adm. Order No. 2015-0037, at 1 (2015). National Implementation of Health Data Standards for eHealth Standardization and Information Interoperability.

[18] Joint DOH-Dep't of Science and Technology (DOST) Dep't Memo. No. 2013-0200 (2013). Creation of Joint DOH-DOST National Governance Steering Committee and Technical Working Group on eHealth.

Program.[19] One of its pioneer programs is the Doctor-to-the-Barrios program. It assigns doctors to rural municipalities who are then able to consult with clinical specialists in the Philippine General Hospital and other telehealth centers through text messaging or e-mail, thus decreasing the need for travels and hospitalizations for Filipinos located in such areas.[20] The National Telehealth Service Program covers the following clinical domains: cardiology, dermatology, radiology, surgery, obstetrics and gynecology, internal medicine, family medicine, otorhinolaryngology, pediatrics, legal medicine, ophthalmology, and neurology.[21]

Another program that involves the management of information to fully and efficiently deliver health care is the Community Health Information Tracking System ("CHITS"). CHITS is "an electronic medical record system developed by the NTHC to improve health information management at the [rural health unit] level."[22] As described:

> It was developed alongside health workers and features a workflow much akin to what is employed in local health centers nationwide. It is also built to gather data and generate reports which health workers need and decision makers require. CHITS is made up of several components which are envisioned to lead to the collection and delivery of good quality data. CHITS is primarily a capacity-building program which instils relevant health information systems components among health workers. By using free and open source software, CHITS makes itself flexible and compliant to the needs of RHU's and local health centers as well as the DOH. Once installed, CHITS becomes a platform for the facility to explore other eHealth applications such as telemedicine and eLearning.[23]

Information consolidation and collaboration are the primary thrusts of CHITS. It also intends to share its developed electronic records systems to local government units for the latter to improve its decision-making.[24] CHITS aims to provide an alternative to data collection and analysis in rural health units, where the previous practice resulted in disorganized data that are tediously collected via manual, paper-based methods, and often lead to the staleness of data.[25]

---

[19] National Telehealth Center, *supra* note 11.

[20] *Id.*

[21] *Id.*

[22] National Telehealth Center, *CHITS*, *at* https://telehealth.ph/project-chits/ (last accessed Apr. 20, 2017).

[23] *Id.*

[24] *Id.*

[25] *Id.*

Further in the field of telemedicine, a resourceful innovation and collaborative tool in telemedicine is the RxBox.[26] The RxBox is "a telemedicine device capable of capturing medical signals through built-in medical sensors, storing data in an electronic medical record (CHITS), and transmitting health information via internet to a clinical specialist in the Philippine General Hospital for expert advice."[27] The RxBox allows the measurement of various vital signs—heart rate and electrical activity, blood pressure, oxygen saturation of blood, tocometer, fetal heart tones, and partograph to name a few. Once the RxBox measures these vital signs, they are then transmitted online via the Internet to a medical specialist in an urban health center.[28]

In the implementation of the Philippine eHealth Framework, the Philippine Health Information Exchange ("PHIE") was created:

> Guided by the [Philippine eHealth Framework], one of the identified critical eHealth projects is the [PHIE]. The PHIE is a platform for secure electronic access and efficient exchange of health data and/or information among health facilities, health care providers, health information organizations and government agencies in accordance with set national standards in the interest of public health. The PHIE is envisioned to become an integral component of the health care delivery system as party of health services to all patients. It shall integrate and harmonize health data coming from different electronic medical record systems and hospital information systems. It shall provide an infrastructure for data/information sharing between health care providers, and support access to patients' records across providers in all geographic areas of the country; thereby, improving efficiency and reliability of communication among participating health care providers. In general, its implementation shall promote public health, improve total patient care and better decision making, while safeguarding the right to privacy of every individual.[29]

### C. Current Trends in eHealth and Telemedicine in the Private Sector

The movement of telemedicine in the private sector is just as rapid. There are already a number of healthcare institutions that offer such services.[30]

---

[26] RxBox, *What is RxBox*, *at* https://rxbox.chits.ph/what_is_rxbox/.

[27] *Id.*

[28] *Id.*

[29] Joint DOH-DOST-Philippine Health Insurance Corporation (PHIC) Joint Adm. Order No. 2016-0001, at 2 (2016). Implementation of the Philippine Health Information Exchange.

[30] These are some of the telemedicine providers in the Philippines: (1) the MedConnect mobile application of St. Luke's Medical Center (St. Luke's Medical Center,

Often touted as a novel way to provide healthcare services, healthcare specialists often use a mobile platform to conduct consultations and give health care advice to patients.

For one, telemedicine has helped in fast-tracking pre-employment medical examinations, primarily through the delivery of pre-employment medical evaluation results via text messages sent to patients' cellphones. Teleconsultations are also made possible because of telemedicine, especially in certain fields such as dermatology, endocrinology, gastroenterology, cardiology, nephrology, and radiology.

Private hospitals have harnessed the power of eHealth to provide value-added services to patients. It is not unusual for hospitals to provide a downloadable mobile application that allows patients to schedule appointments, settle bills and make payments, view laboratory results, and contact the hospital in case of emergencies.

Even businesses that do not traditionally venture into healthcare can establish their presence in the field. A telecommunications provider has started a telemedicine hotline, staffed by Filipino physicians all over the country. The service has proven to be beneficial to patients located in rural areas, and has provided health professionals an avenue to dispense urgent medical advice in emergency situations.[31]

The promise of telemedicine in providing cost-efficient healthcare is difficult to ignore for business enterprises. Not only does telemedicine allow them and their healthcare specialists to cater to as many patients as possible, without the usual difficulties posed by geographical and time barriers, it also allows patients to choose their health professional of choice with less restrictions posed by the same barriers. In turn, telemedicine also benefits from the involvement of the private health sector. After all, it is the private sector, with its vast resources, that can best develop technologies that would help the field advance further. Imagine a private healthcare institution interested in being a pioneer in telemedicine, and for this purpose invests its time and resources in the latest facilities that government agencies cannot possibly compete against. Clearly, then, the private sector is in the best position to

---

*MedConnect App*, *at* http://www.stluke.com.ph/medconnect-app.html); (2) MyDocNow (Avizia, *Telemedicine service "MyDocNow" launches in the Philippines*, *at* https://www.avizia.com/ mydocnow-telemedicine-service-launches-philippines/); and, (3) Telemedicine of MedWay (MedWay, *Our Telemedicine*, *at* http://www.medway.com.ph/index.php/telemedicine).

[31] For instance, KonsultaMD, a telemedicine services solutions provider, is powered by a telecommunications provider, Globe Telecom.

invest the resources, such as highly advanced broadband infrastructure and software, that can raise the standards in the field of eHealth.

Healthcare, at the end of the day, is *still* a business, and healthcare institutions will continually want to be viewed as a leader in telemedicine, by consistently leveraging technology to deliver health care solutions. The role of the private sector in telemedicine cannot be underemphasized.

Although the author does not claim that the foregoing is a comprehensive sweep of current telemedicine initiatives in the public and private sectors, the illustrations above reveal that telemedicine and eHealth in both the public and private sectors are moving at a fast pace. Currently, it is a highly unregulated field. The need to determine the legal obligations of healthcare institutions in eHealth and telemedicine is pressing—to ensure that no liberties are violated at the expense of patient care.

## II. LEGAL RISKS POSED BY THE LACK OF A LEGAL FRAMEWORK

Without question, and optimistically for better than for worse, cyberspace is here to stay. The intersection of health and cyberspace calls for a much-needed assessment of the implications to the privacy of individuals whose health information are necessarily affected. Decidedly, the dilemma of the right of informational privacy can be more easily resolved if mere commercial interests were concerned:

> Critics of a right to information privacy have raised the First Amendment as a potential defense against any declaration of a constitutional right to information privacy. These critics usually include businesses engaged in the sale of personal information, and marketers who find the detailed information available about individuals a valuable tool in promoting and selling their products. They argue that the First Amendment's guarantee of free speech is superior to any information privacy rights of the data subject. Those with an interest in the for-profit dissemination of personal information have a legitimate First Amendment right in free speech. However, the Court has held that speech which does nothing more than propose a commercial transaction has a lower value and, therefore, can be subject to regulation. The Supreme Court has held that commercial speech rights are in a "subordinate position in the scale of First Amendment values" and that commercial speech is less likely to be deterred by regulation than is core political speech.[32]

---

[32] Sandra Byrd Peterson, *Your Life as an Open Book: Has Technology Rendered Personal Privacy Obsolete?*, 48 FED. COMM. L.J. 163, 173 (1995). (Citations omitted.)

With regard to health information privacy, the stakes are higher: health information is more than just a business or contractual concern, and touches on more matters than just commercial speech. Thus, there are several interests involved: the interest in providing adequate clinical care, the right to free speech by healthcare institutions and professionals, and the right to privacy of health information of patients. These interests must be delicately balanced, as one cannot simply be dismissed in favor of the others in the same way that commercial speech is easily trumped by the general right to information privacy.

The lack of adequate safeguards, or even the prevailing awareness that it is absent, has far-reaching implications ranging from the esoteric to the concrete. For one, information interoperability means that more organizations are able to utilize health information for purposes beyond the immediate health concern. Also, the lack of uniform privacy standards for the compliance of both the private and public sectors results in a compromise of a patient's rights.

Information interoperability is an integral component of eHealth. Defined as the "ability to transfer and use information in a uniform and effective manner across multiple organizations and information technology systems,"[33] information interoperability will ideally result in efficiency in the delivery of health services, as it is expected to "provide the means to merge different systems and facilitate sharing of data/information."[34] Information interoperability is expected to result in a merger of different information systems, because it includes both the public and private health sectors, i.e. "national agencies and local government units, government and private health facilities, development partners, academe, research partners, civil society groups, purchasers of healthcare, producers, distributors, financial services, healthcare providers, sellers, donors, and other stakeholders in the health sector."[35] While favorable to healthcare institutions, this is a problem to a patient, because there is as yet no uniform data privacy standards by which healthcare institutions in both the private and public sectors are bound.

Thus, a serious concern is the grant of access to medical records given to various stakeholders, including doctors, hospitals, health insurance companies, and various businesses:

---

[33] DOH Adm. Order No. 2015-37, Part V, ¶ 9 (2015). National Implementation of Health Data Standards for eHealth Standardization and Information Interoperabilty.

[34] Pt. II, ¶ 4.

[35] Pt. IV.

> [T]here is now a broader audience for patient information: whereas previously, only the patient's primary provider had access to their record, the use of health information technology systems means that software developers, programmers, network operators, and other individuals operating behind the scenes to maintain the system can, but may not necessarily, peer into an individual's private data.[36]

Such openness puts the patient in undue risk; virtually every aspect of a person's health information is open to whomever is granted access to the medical records. Businesses can easily use such information to make a determination as to a person's health status, from past illnesses to lifestyle habits. The worst case scenario is not difficult to picture: with large amounts of patient data aggregated into interoperable network databases, the threat to security has never been greater. If leaked, a patient's entire medical history is open for exploitation for various purposes to the public. As previously discussed, telemedicine is a field that even organizations not traditionally in the business of providing healthcare engage in, such as telecommunications companies. The possibility that personal data as sensitive as health information can be used beyond its supposed purpose is more real than imagined.

Indeed, "[u]sing health information technology and telemedicine, and storing patient data in electronic form all amplify the privacy issues in the context of the relationship between health provider and patient."[37] The risk that technology in the field of healthcare poses to the erosion of our privacy rights exists, such that to delay the process of coming up with a policy and legal framework that adequately addresses the issue can no longer be delayed.

Upholding the right to health information privacy is also consistent with the principles that guide the practice of medicine. One of the four principles of biomedical ethics, the principle of non-maleficence "requires that a physician must not act in a way that entails harm or injury to patients [...] [by following] strictly the proper standard of care that avoids the risk of harm."[38] The principle of non-maleficence necessitates the protection of health information:

> When personally identifiable health information, for example, is disclosed to an employer, insurer, or family member, it can result in stigma, embarrassment, and discrimination. Thus, without some

---

[36] Carl A.T. Antonio et al., *Health Information Privacy in the Philippines: Trends and Challenges in Policy and Practice* 3, *available at* https://www.academia.edu/4727321/Health_information_privacy_in_the_Philippines_Trends_and_challenges_in_policy_and_practice (last accessed April 21, 2017).

[37] *Id.* at 4.

[38] PETER P. NG & PHILIPP U. PO, MEDICAL LAWS AND JURISPRUDENCE 102 (2005).

> assurance of privacy, people may be reluctant to provide candid and complete disclosures of sensitive information even to their physicians. Ensuring privacy can promote more effective communication between physician and patient, which is essential for quality of care, enhanced autonomy, and preventing economic harm, embarrassment, and discrimination. However, it should also be noted that perceptions of privacy vary among individuals and various groups. Data that are considered intensely private by one person may not be by others.[39]

Following the guiding principle of non-maleficence, healthcare institutions and health professionals that violate a person's privacy of health information are essentially causing harm or injury to patients. It is argued that the principle of non-maleficence is not limited to mere physical injury, but also to legal harm to the patient.

One attempt to "plug" the legal risks posed by the lack of a legal framework on health information privacy is Joint Administrative Order No. 2016-002[40] jointly issued by the DOH, DOST, and the Philippine Health Insurance Corporation ("PHIC") (hereinafter "Joint DOH-DOST-PHIC AO 2016-02"). However, Joint DOH-DOST-PHIC AO 2016-02, aside from certain issues in the issuance itself,[41] falls short of providing a legal framework uniformly applicable to both the public and private sectors. It is only applicable to the Philippine Health Information Exchange system, participating healthcare providers, and natural and juridical persons involved in the processing of health information within the PHIE framework.[42] Essentially, if certain government telemedicine initiatives, such as the CHITS, opt out of participation in the PHIE, then they are free not to comply with the directives in Joint DOH-DOST-PHIC AO 2016-02. Moreover, the issuance does not always apply to private healthcare institutions, which are basically free to craft its own privacy policy standards, with minimal state interference or regulation.

---

[39] COMMITTEE ON HEALTH RESEARCH AND THE PRIVACY OF HEALTH INFORMATION: THE HIPAA PRIVACY RULE, BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY RULE, IMPROVING HEALTH THROUGH RESEARCH 77 (Sharyl J. Nass et al., eds., 2009) (2009).

[40] Joint DOH-DOST-PHIC Adm. Order No. 2016-02 (2016). Privacy Guidelines for the Implementation of the Philippine Health Information Exchange.

[41] *See* Pt. IV discussion, *infra*.

[42] Joint DOH-DOST-PHIC Adm. Order No. 2016-02, Pt. IV, ¶ 1 (2016).

## III. APPLICABLE PRIVACY LAWS IN THE FIELD OF EHEALTH AND TELEMEDICINE

### A. The Right to Health Information Privacy as a Form of Constitutional Information Privacy

The individual's constitutional right to privacy was conceptualized by Justice Louis Brandeis at around 1890, considered as the "most profound development in privacy law."[43] Since then, courts of the United States (U.S.) have cited the Fourth Amendment to the U.S. Constitution, which guarantees a person's right against unreasonable searches and seizures, to uphold individuals' right to privacy against governmental intrusions, as well as their state laws to protect against private intrusions. Later on, pieces of privacy legislation against intrusions by businesses were enacted.[44]

In the Philippines, a universal framework for privacy remains elusive:

> *A unified privacy framework is imperative.* At present, our jurisprudence is grounded in *Morfe*, *Ople* and the right against unreasonable search. Combined with the Philippine hypertextualist mindset, the constitutional framework stands to be reduced to a chore of itemizing zones of privacy and textual hooks to whatever constitutional or statutory provision presents a plausible fit. *We must move towards consciousness that the right to privacy protects a multiplicity of values, and that these converge to ultimately preserve a sphere of personal integrity and dignity in which an individual is free to function within society.*[45]

The constitutional right to privacy finds basis in the Bill of Rights:

> The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law.[46]

The right to privacy has two legs:

1. Decisional privacy: "the interest in independence in making certain kinds of important decisions"

---

[43] Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY 10 (Kristen J. Matthews ed., 2006).

[44] *See id.*

[45] Oscar Franklin Tan, *Articulating the Complete Right to Privacy in Constitutional and Civil Law: A Tribute to Chief Justice Fernando and Justice Carpio*, 82 PHIL. L.J. 78, 81 (2008). (Emphases supplied, citation omitted.)

[46] CONST. art. III, § 3(1).

> 2. Informational privacy: "the individual interest in avoiding disclosure of personal matters"[47]

As held by Chief Justice Fernando in *Morfe v. Mutuc*,[48] informational privacy finds its roots in the "right to be let alone [as] the beginning of all freedom."[49] The concept of informational privacy was discussed in the case of *Ople v. Torres*,[50] where the formation of a national identification card system was assailed as violating the right to privacy.[51] In striking down the concept of a national identification card system, in the pretext of delivering basic government services, the Supreme Court held:

> The right to privacy is one of the most threatened rights of man living in a mass society [...] In the case at bar, the threat comes from the executive branch of government which by issuing A.O. No. 308 pressures the people to surrender their privacy by giving information about themselves on the pretext that it will facilitate delivery of basic services.[52]

The acknowledgement of the right to privacy in the Constitution—insofar as it encompasses informational privacy—is only partially effective in telemedicine since the protection would only apply against government intrusion and cannot be used as a basis for the protection of health information against non-state actors. But in telemedicine, the government is only one of the many players in the recording, retention, and processing of health information.

### B. Health Information Privacy Violation as a Tort

Article 26 of the New Civil Code provides that "[e]very person shall respect the dignity, personality, privacy and peace of mind of his neighbor and other persons."[53]

A question arises as to the applicability of Article 26 to violations of health information privacy. In this regard, there is a dearth of Supreme Court jurisprudence that recognizes a cause of action relating to the unauthorized disclosure of personal information, much less health information, without the consent of the affected individual. The lack of jurisprudence should not come as a surprise. Even in the United States, the definition of privacy has not been

---

[47] Tan, *supra* note 45, at 89, *citing* Whalen v. Roe, 429 U.S. 589, 599-600 (1977).
[48] G.R. No. 20387, 22 SCRA 424, Jan. 31, 1968.
[49] Tan, *supra* note 45, at 98, *citing id.* at 443.
[50] G.R. No. 127685, 293 SCRA 141, July 23, 1998.
[51] *Id.*
[52] *Id.* at 170. (Citation omitted.)
[53] CIVIL CODE, art. 26.

settled.[54] Information privacy tort cannot be precisely classified as one of the four privacy torts under U.S. law:[55]

> The first of these four torts is "[p]ublicity which places the plaintiff in a false light in the public eye." The second tort was defined as "[i]ntrusion upon the plaintiff's seclusion or solitude, or into his private affairs." Third, Prosser identified "[p]ublic disclosure of embarrassing private facts about the plaintiff." He categorized the fourth tort as "[a]ppropriation, for the defendant's advantage, of the plaintiff's name or likeness." Plaintiffs have had little or no success bringing actions under this scheme of privacy torts when the invasion is one of information privacy. However, these torts are defined broadly enough that courts could expand their application to the information privacy arena.[56]

Even if Philippine courts eventually uphold the right to privacy as a tort under the Civil Code, the remedy may be deemed inadequate because the Civil Code only guarantees the right to damages. Other remedies such as the deletion of the information are not provided.

### C. Privacy in the Context of the Physician-Patient Privilege

The right to privacy in a physician-patient setting is more specifically dealt with under the physician-patient privilege under the Rules of Court:

> Section 24. Disqualification by reason of privileged communication. — The following persons cannot testify as to matters learned in confidence in the following cases:
>
> ***
>
> c) A person authorized to practice medicine, surgery or obstetrics cannot in a civil case, without the consent of the patient, be examined as to any advice or treatment given by him or any information which he may have acquired in attending such patient in a professional capacity, which information was necessary to enable him to act incapacity, and which would blacken the reputation of the patient.[57]

The foregoing rule is applicable in strictly limited cases, and requires the concurrence of the following requisites:

---

[54] Peterson, *supra* note 32, at 165.

[55] *Id.*

[56] *Id.* at 175. (Citations omitted.)

[57] RULES OF COURT, Rule 130, § 24(c).

a) The privilege is claimed in a civil case;

b) The person against whom the privilege is claimed, is one duly authorized to practice medicine, surgery, obstetrics, or nursing;

c) The person acquired the information while he was attending the patient in his personal capacity;

d) The information was necessary to enable him to act in that capacity; it was confidential; and, if disclosed, shall tend to blacken the character of the patient.

Further, the privilege is applicable only to the testimony of the physician, or to an affidavit and medical records of hospitals containing privileged matters. The physician-patient privilege hardly protects against the kinds of data privacy violations that may occur in telemedicine. In fact, it may only be claimed when a civil case has already commenced.

## IV. CREATING A LEGAL FRAMEWORK FOR THE PROTECTION OF HEALTH INFORMATION PRIVACY BY APPLYING THE DATA PRIVACY ACT

Considering the inadequacy of privacy laws arguably applicable in health information privacy, creating a legal framework that protects that of patients' is imperative. While the traditional view of privacy in the field of patient care is confined to physician-patient confidentiality, the understanding of health information privacy must be expanded to integrate the rights and obligations of a healthcare institution processing the health information of a patient. In this regard, the Data Privacy Act ("DPA")[58] can provide the legal basis to compel the compliance of healthcare institutions and the various institutions in eHealth.

Enacted in August 15, 2012, the DPA is the primary and most comprehensive Philippine law that deals with the protection of individual personal information in information and communication systems in the government and the private sector. Its implementing agency, the National Privacy Commission (NPC), has the mandate to "administer and implement the provisions of the DPA, and to monitor and ensure compliance of the country with international standards set for data protection[.]"[59]

---

[58] Rep. Act No. 10173 [hereinafter "DPA"] (2012). Data Privacy Act of 2012.

[59] § 7.

Until the relatively recent formation of the National Privacy Commission, the enforcement of the DPA has essentially been absent.[60] Soon after the NPC was constituted, the implementing rules and regulations[61] of the DPA were issued on August 24, 2016.

### A. Applying the Definitions of the DPA in eHealth and Telemedicine

The DPA identifies specific stakeholders in personal information. In a healthcare setting, the physician or the hospital is the personal information controller, which refers to "a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf."[62] "Control" exists when the natural or juridical person decides on "what information is collected, or the purpose or extent of its processing."[63] "Processing" is a blanket term that encompasses various actions performed by a physician:

> [A]ny operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system.[64]

The patient is the "data subject," whose "personal, sensitive personal, or privileged information is processed."[65]

The DPA also introduces the concept of a personal information processor, which in ICT is an entity to which certain processing functions are outsourced. Specifically, a personal information processor is defined as "any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining

---

[60] The first Commissioner of the National Privacy Commission was appointed only on March 7, 2016, almost four years after the enactment of the DPA. *DOST exec named first commissioner of National Privacy Commission*, NEWSBYTES.PH, Mar. 7, 2016 *at* http://newsbytes.ph/2016/03/07/dost-exec-named-first-commissioner-of-national-privacy-commission/.

[61] Implementing Rules and Regulations of the Data Privacy Act of 2012 [hereinafter "DPA IRR"].

[62] § 3(m).

[63] § 3(m).

[64] § 3(o).

[65] § 3(d).

to a data subject."[66] The complexity of telemedicine and eHealth usually involves the participation of a personal information processor. Various players are tapped in the provision of clinical care services. Ultimately, however, it is the responsibility of the personal information controller to ensure the compliance of the personal information processor with the standards set by the DPA. Numerous provisions in the DPA assure this responsibility. For one, the personal information controller "must ensure that the third parties processing personal information on its behalf shall implement the security measures" required by the DPA.[67]

### B. Health Information as Sensitive Personal Information

More than the players involved in the processing of personal information in a healthcare setting, an important feature of the DPA is the distinction it makes between "personal information" and "sensitive personal information." The two concepts are defined as follows:

> l. "Personal information" refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual;[68]
>
> ***
>
> t. Sensitive personal information refers to personal information:
>
> 1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
>
> 2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
>
> 3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

---

[66] § 3(n).
[67] Data Privacy Act of 2012, § 20(d).
[68] *DPA IRR*, § 3(l).

> 4. Specifically established by an executive order or an act of Congress to be kept classified.[69]

Whereas any information that makes a person identifiable readily falls under the personal information basket, sensitive personal information goes the extra mile to narrow down what is expressly classified as sensitive personal information. Privileged information more simply refers to the "data which under the Rules of Court and other pertinent laws constitute privileged communication."[70]

The distinction is relevant because of the different thresholds for processing personal information and sensitive personal information.

The criteria for processing personal information is laid down as follows:

> SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
>
> (a) The data subject has given his or her consent;
>
> (b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
>
> (d) The processing is necessary to protect vitally important interests of the data subject, including life and health;
>
> (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
>
> (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a

---

[69] *DPA IRR*, § 3(t).

[70] Data Privacy Act of 2012, § 3(k).

> third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution."[71]

Legally, the processing of personal information is fairly straightforward. It can be processed as long as any one of the six conditions exists. It is also easier to defend. For instance, in case the consent of the data subject cannot be readily obtained, a personal information controller can simply justify the processing of personal information as necessary to protect the "vitally important interests" of the data subject, under the fourth condition mentioned above.

Sensitive personal information requires more rigid standards for its processing. To be precise, processing is prohibited as a general rule, and is justifiable only as an exception:

> SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
>
> (a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
>
> (b) The processing of the same is provided for by existing laws and regulations: *Provided*, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further*, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
>
> (c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
>
> (d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided*, That such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further*, That the sensitive personal

[71] § 12.

> information are not transferred to third parties: *Provided, finally*, That consent of the data subject was obtained prior to processing;
>
> (e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
>
> (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.[72]

The question, then, is whether health information should fall under the general definition of personal information or the narrower definition of sensitive personal information. Under the proposed definition of health information in this paper, health information must in all cases be considered sensitive personal information.

First, the definition of sensitive personal information itself provides that it pertains to personal information about an "individual's health, [...] genetic or sexual life [...]."[73] Also, although some types of patient data arguably fall under the general definition of "personal information" (for instance, the name of a person is ordinarily not considered sensitive personal information but merely personal information), such data must still be considered sensitive personal information. This is because any personal information collected from the patient is for the overall purpose of providing a health service, as health information ought to be defined.[74] Thus, health information should be aggregately considered as sensitive personal information, the processing of which requires a higher standard under the DPA. Further, the legal risks obtaining from the exposure or breach of sensitive personal information are far too great for it to be considered as merely personal information.

This is the loophole in Joint DOH-DOST-PHIC AO 2016-02. Aside from being applicable only to participants in the PHIE[75] and in spite of its recognition of the DPA,[76] it *still* considers certain health information as mere

---

[72] § 13.
[73] § 3(l)(2).
[74] As argued in Pt. I.A., *supra*.
[75] Joint DOH-DOST-PHIC Adm. Order No. 2016-02, Pt. IV, ¶ 1 (2016).
[76] Pt. I, ¶ 4; Pt. II, ¶¶ 2, 6.

personal information and not sensitive personal information.[77] It merely copies the definitions of personal information and sensitive personal information in Annex 2 of the issuance.[78] Further, consent, although obtained from the patient prior to the processing of health information, refers to consent only to participation in the PHIE, and not the various purposes for which the PHIE may use it.[79] This, in the author's opinion, is not the purpose-specific consent required in processing sensitive personal information under the DPA. The consent must also include all the specific purposes envisioned by the PHIE for the patient's health information, and should not merely refer to a blanket "participation" in the system.

### C. Consent as an Enabler in the Processing of Health Information

Consent is indubitably the clearest way of complying with the criteria for processing both personal and sensitive personal information.

In the processing of sensitive personal information, consent by the data subject is qualified in that it must be purpose- and time-specific: *first*, the purpose must be specified; and, *second*, it must be provided *prior* to the processing.[80] In contrast, consent in the processing of personal information may be obtained from the data subject at the next practical opportunity—even after the processing has already been performed.[81]

In a clinical care scenario, consent to the processing of sensitive personal information must be obtained *prior* to the processing. A direct application of this is a scenario where a physician conducts teleconsultation with a patient, or a hospital collects the health information of a patient prior to admission or consultation, or a healthcare institution that encodes a person's medical history into its electronic medical records.

By obtaining the patient's consent specific to the processing of his personal information, and not just the usual consent obtained to commence the physician-patient relationship, prior to the processing, healthcare institutions, including hospitals and doctors, can no longer just collect, store, and modify health information without indicating the specific purpose for doing so. This minimizes the sometimes needless collection of health information that bears no relevance to the present health concern requiring

---

[77] Pt. VIII.
[78] Annex 2, items 19, 28.
[79] Pt. VIII.A.1.d.
[80] DPA IRR, § 22(a).
[81] § 21(a).

medical attention. As a matter of protocol, the healthcare professional must advise the patient of what sensitive personal information will be collected and the purpose for the same before proceeding to the actual collection.

Further, by requiring purpose- and time-specific consent, a greater consciousness towards health information privacy is raised among healthcare institutions and patients. While providing medical care is still the primary concern, health information is no longer relegated to the background as mere "paperwork" or "standard procedure"—healthcare institutions would have to be more deliberate in outlining the reasons why they require the processing of health information in the first place.

Lastly, framing consent as a contractual requisite makes it clear to the patient, physician, and healthcare institution that there is a contract between them revolving around the processing of health information—that there is a meeting of minds between the physician or the healthcare institution on the one hand, and the patient on the other, whereby one party binds himself with respect to the other, to the processing of health information or to be provided adequate clinical care services, as the case may be. It then also becomes clear that an aggrieved party can avail of remedies[82] when a breach is committed by either party.

Of course, the problem of upholding health information privacy does not fall away completely by requiring the consent of the affected individual in all cases, as this is realistically not always feasible. For instance, a patient in need of urgent care and relies on technology to provide much-needed attention obviously cannot provide the consent required by law. In fact, it is difficult to anticipate when a physician-patient relationship will arise, and therefore, consent by the patient as the data subject is not always possible. In such cases, the provider of consent may be expanded to include the following actors, in the following order of hierarchy: (a) capacitated patient, (b) spouse, (c) parent or natural guardian in case of a person who has not reached the age of majority, and (d) a legal guardian appointed by the court.

### D. Applicability of the Other Criteria for Processing Sensitive Personal Information

A review of the criteria for processing sensitive personal information would give the impression that healthcare institutions can get away with the requirement of obtaining consent from patients by mere resort to the other

[82] The traditional remedies in cases of breach of contract under the Civil Code include specific performance, damages, or resolution. CIVIL CODE, arts. 1167, 1170, 1191.

exceptions: (a) the processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;[83] and, (b) the processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured.[84]

Neither the DPA nor the DPA Implementing Rules and Regulations ("DPA IRR") define the standard of necessity to protect the life and health of the data subject. There is also no definition of what constitutes "medical treatment" that allows non-consensual processing of sensitive personal information.

It is thus the NPC's urgent obligation to clarify what this means, taking into account and fully respecting the patient's right to self-determination. A healthcare institution cannot simply process health information without the patient's consent, on the mere claim that it is vital to protect the health of the patient or that it is necessary for medical treatment. After all, consent may simply be expanded to include the actors mentioned in Part IV.C., instead of doing away with it under the pretext of it being vital to protect the patient's health, or being necessary for medical treatment. In other words, consent is paramount. After all, informed consent, or the right to self-determination, is an important principle in the practice of medicine:

> The patient's right to self-determination is reinforced by noting that a physician has a legal as well as a moral or ethical duty to respect a person's autonomy. It is worthwhile to note that it is the respect for a person's autonomy that morally underpins the legal requirement for consent. That a legal requirement for consent is based on the moral principle of respect for another person's autonomy is merely a specific example of the general rule. "...every legal duty is founded on a moral obligation." Again, what is legal ought to be moral.
>
> Consent has both a moral aspect (principally by virtue of the Principle of Respect for Autonomy) and a legal aspect and that undoubtedly, it underlies the whole of medical practice. There is no doubt—especially since there is no separate category of 'medical touchings'.[85]

The same standard of respect for a person's right to self-determination should be applied to the processing of health information. A person must be

---

[83] Data Privacy Act of 2012, § 13(c).

[84] § 13(e).

[85] NG & PO, *supra* note 38, at 196.

given the autonomy to decide whether to give up his health information. The processing of health information is an irremovable aspect of the physician-patient relationship, and there is no change in the roles played by the respective parties just because health information is perceived to be of lesser importance than the urgent need to provide clinical care. Before a patient agrees to medical treatment, he must first consent to the processing of his sensitive personal information, as both consents are founded on the underlying right to self-determination of the patient.

### E. Recognition of the Rights of the Patient as a Data Subject

It would be difficult for healthcare institutions to obtain and process a patient's sensitive personal information without the latter's consent, and still remain respectful of the rights of the patient under the terms of the DPA. These are outlined in the DPA itself, as the rights to:

> (a) Be informed whether health information pertaining to him or her shall be, are being or have been processed;
>
> (b) Be furnished certain information (e.g., description of said health information; purposes for processing, scope and method, recipients of such information, methods for automated access; identity and contact details of personal information controller; the period of storage) into the electronic medical records, or at the next practical opportunity;
>
> (c) Reasonable access to the health information;
>
> (d) Dispute the inaccuracy or error in his health information;
>
> (e) Suspend, withdraw, or order the blocking, removal or destruction of his or her personal information from the electronic medical records;
>
> (f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of health information.[86]

In one way or another, the patient has to be informed of such rights specific to their health information privacy. Simple waivers of consent cannot under any circumstances be acceptable. Instead, healthcare institutions and health professionals should be encouraged to come up with an entirely separate contract addressing health information privacy concerns.

---

[86] Data Privacy Act of 2012, § 16.

The commonly accepted practice of organizations is to prescribe these rights in the form of a comprehensive privacy policy that is consented to by a data subject. The adoption of such practice is imperative in telemedicine. It is about time for healthcare institutions and professionals to introduce the concept of a privacy policy, in a language understandable to the average Filipino, while paying attention to the standards for processing health information under the DPA.

### F. Security Measures for the Protection of Health Information

Thus far, what has been discussed involves the confidentiality obligation of healthcare information controllers:

> Confidentiality safeguards information that is gathered in the context of an intimate relationship. It addresses the issue of how to keep information exchanged in that relationship from being disclosed to third parties. Confidentiality, for example, prevents physicians from disclosing information shared with them by a patient in the course of a physician–patient relationship. Unauthorized or inadvertent disclosures of data gained as part of an intimate relationship are breaches of confidentiality.[87]

An equally important aspect of health information privacy that requires the attention of healthcare institutions is security, the "procedural and technical measures required (a) to prevent unauthorized access, modification, use, and dissemination of data stored or processed in a computer system, (b) to prevent any deliberate denial of service, and (c) to protect the system in its entirety from physical harm."[88] The DPA requires personal information controllers to comply with "reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data."[89] The goal of requiring these security measures is quite sweeping: they are aimed at protecting "personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination."[90]

With the DPA IRR already in effect, the NPC fully exercising its administrative power over the relevant stakeholders, and a clear deadline of

---

[87] COMMITTEE ON HEALTH RESEARCH AND THE PRIVACY OF HEALTH INFORMATION: THE HIPAA PRIVACY RULE, *supra* note 39, at 76.

[88] *Id.* at 18.

[89] *DPA IRR*, § 25, ¶ 1.

[90] § 25, ¶ 3.

September 9, 2017 set for compliance with the DPA and the DPA IRR, healthcare institutions need to take a very close look at their privacy obligations, especially the concrete organizational,[91] physical,[92] and technical[93] security measures that they need to institute. To ignore this deadline is to risk facing the penalties imposed by the DPA. The unauthorized processing of personal sensitive information without the consent of the data subject is penalized by imprisonment ranging from three years to six years and a fine of not less than PHP 500,000 but not more than 4 million pesos.[94] This is but the tip of the iceberg of burdensome penalties that healthcare institutions and health professionals stand to face: accessing sensitive personal information due to negligence,[95] improper disposal of sensitive personal information,[96] processing for unauthorized purposes,[97] unauthorized access or intentional breach,[98] concealment of security breaches,[99] and malicious disclosure,[100] to name a few.

For instance, organizational security measures include the appointment of a compliance officer who shall be accountable for ensuring compliance with the DPA and the DPA IRR,[101] the implementation of a data protection policy consistent with the data protection principles,[102] the maintenance of records of processing activities undertaken by the health information controller,[103] and the consummation of contracts between personal information controllers and processors that shall ensure the compliance of the latter with the DPA,[104] to name a few.

The physical security measures required by the DPA IRR include (a) the implementation of policies and procedures to monitor and limit access to and activities in the room, workstation or facility; (b) design of office space and work stations that provides privacy to anyone processing health information; (c) clearly defined duties, responsibilities and schedule of individuals involved

---

[91] *See* § 26.
[92] *See* § 27.
[93] *See* § 28.
[94] Data Privacy Act of 2012, § 25(b).
[95] § 26.
[96] § 27.
[97] § 28.
[98] § 29.
[99] § 30.
[100] § 31.
[101] *DPA IRR*, § 26(a).
[102] § 26(b).
[103] § 26(c).
[104] § 26(f).

in the processing of health information; and, (d) the adoption of policies and procedures that prevent the mechanical destruction of files and equipment.[105]

Technical security measures include (a) the adoption of a security policy, and safeguards to protect the computer network against accidental, unlawful or unauthorized usage; (b) regular monitoring for security breaches; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) the encryption of personal data during storage and while in transit, authentication process; and other technical security measures that control and limit access.[106]

For government agencies, an added layer of security pertaining to on-site and on-line access, as well as off-site access by agency personnel to sensitive personal information (in this case, health information), must be complied with.[107]

## CONCLUSION

The DPA provides protections to the right to health information privacy of a patient, where such legal protections were virtually inexistent before its effectivity and the recently renewed interest in its implementation. It provides an adequate legal framework, which, if refined by the NPC, will address the rights and obligations of the various stakeholders in an eHealth or telemedicine scenario. But the contextualization of the DPA to telemedicine, with the goal of upholding health information privacy, is a mere first step. The succeeding step—and a more important one at that—is the awareness of such contextualization and applicability among healthcare institutions and health professionals. Again, this is not a mere option that the players in the industry can opt out of.

The DPA contains firm penalties and sanctions that are readily enforceable by the NPC. The "cure", in a manner of speaking, already exists; it is just a matter of taking a second closer look, and ensuring that the obligatory force of the law does not lose its teeth, as is often the case in the administration of laws in the Philippines. The payoff is too significant to dismiss: a step in the right direction towards the protection of the often disregarded yet crucial right to health information privacy.

**- o0o -**

---

[105] § 27.
[106] § 28.
[107] § 31.