SyCipLaw COVID-19 Legal Information Bulletin: TMT

The Philippine Government has issued a slew of resolutions and circulars as part of its response to the COVID 19 pandemic and unsurprisingly, a number of legal and practical issues have beset businesses and persons under the Luzon-wide enhanced community quarantine (ECQ).[1] Like the rest of the world, the country is bracing itself for a new normal – in the way enterprises are run, services are rendered, everyday tasks are undertaken.

This legal briefing series touches on Philippine issues in TMT triggered by the current crisis, or which have become more relevant because of it.

Data Privacy vs. Public Health?

The need to do contact tracing and protect public health has created some tension between insistence on individuals' right to privacy and calls to disclose personal information to prevent the spread of COVID-19. The Philippine National Privacy Commission (NPC), the agency tasked to administer the Data Privacy Act of 2012 (the country's general data privacy statute) believes that existing laws are already adequate and does not think there is a material gap between these interests.

Personal data, including sensitive personal information such as a person's health condition, can be collected and processed even without the consent of a data subject where, among others, the collection and processing are done for purposes of medical treatment, protecting the life and health of individuals, responding to a national emergency, or when allowed under existing laws and regulations. Here, the NPC has noted that under Republic Act No. 11332, or the "Mandatory Reporting of Notifiable Diseases and Health Events of Public Concern Act", physicians, medical personnel, hospitals, clinics, laboratories, schools, and workplaces that have information on infected individuals are already mandated to disclose this to the local and regional health officers and the Department of Health (DOH). Given the declaration of the state of public health

[1] Luzon is one of the Philippines' main islands, and is where the country's national capital region is located. The ECQ began on 17 March 2020, and is scheduled to end on 30 April 2020 (subject to the extensions of the ECQ until 15 May 2020 over the national capital region and other high-risk areas).

emergency in response to the COVID-19 pandemic, persons who may have been infected and their close contacts in fact have the obligation to disclose certain information to the health authorities, including among others, their personal information, health status, travel history, and frequented places for purposes of contact tracing and monitoring.

There had been calls by the Integrated Bar of the Philippines, the Philippine Medical Association, and the Philippine College of Surgeons, as well as some local government officials for persons to "voluntarily consent" to the disclosure of their personal data. On this, the NPC said that a call for "voluntary consent" is unnecessary, noting the availability of other criteria for lawful processing, and that individuals were even obliged to disclose information to the appropriate authorities under Republic Act No. 1132. The NPC cautioned the persons calling for "voluntary consent" that while collection and processing of personal data may be justified by an available criterion under the Data Privacy Act (DPA), these must still be conducted in accordance with the data privacy principles of legitimate purpose, transparency, and proportionality. Thus, there should be no indiscriminate disclosure of personal information. Disclosure should only be made to relevant authorities and involve necessary information, and to the extent possible, any personal data intended for disclosure must be anonymized.

In this regard, on 8 April 2020, the Inter Agency Task Force (IATF) (a body formed by the Philippine Government to help lead the response to the pandemic) issued a resolution adopting the policy of "mandatory public disclosure" of personal information relating to patients who have tested positive for COVID-19 with the view of enhancing the contact-tracing efforts of government. The resolution itself is not clear as to what this policy means in the context of the DPA, and what kind of disclosure is now allowed from the IATF perspective. The resolution, however, also provides that the contact-tracing efforts of the government will now be handled by the Office of Civil Defense (OCD), in coordination with local government units and other agencies. This could be interpreted to mean that despite the broad language of the policy statement, any such disclosure will only be directed to the OCD and the DOH. In press conferences, Cabinet Secretary Karlo Nograles appears to clarify that this is what is contemplated by the IATF resolution. As of the time of this writing, the NPC has not issued any related statement.

Data Privacy From Home?

With the strict home quarantine being imposed on Metro Manila (as well as the rest of Luzon Island), some enterprises that can continue to operate have found themselves struggling to implement work-from-home arrangements (WFH). Companies that heavily rely on communications and technology like BPOs and are thought to be better equipped at implementing WFH have also not been spared. They face the additional challenge of complying with data privacy requirements under both law and their existing contracts.

In the midst of the COVID-19 situation, some enterprises have asked if the application of the Philippine DPA has been suspended with the adoption of the ECQ and the government policy of encouraging WFH. The simple answer is no. The DPA continues to be in force. Thus, in order to comply with the law, controllers and processors will need to find ways to migrate their policies, procedures, and safeguards to a work-from-home setting. In this regard, the DPA does not require

the implementation of specific safeguards (except for certain organizational requirements which should not be impacted by WFH), but it requires security measures to be "appropriate". In some cases, the more difficult challenge may be ensuring compliance with specific data privacy standards and procedures provided for by contract.

There is as yet no specific local law guidance on whether the pandemic and its effects can be considered force majeure, and whether this provides a defense or basis for non-compliance or modification of data privacy undertakings without penalty. This will likely depend on the relevant contract and circumstances with respect to a specific claim. Companies like BPOs would do well to discuss and agree on their WFH security measures with clients.

Data protection officers of businesses implementing WFH arrangements and which need to ensure that data privacy measures are in place, may consider "best practices" such as:

- Regularly and consistently reminding employees of the need to ensure the security of personal information and other confidential data;
- Advising employees on how to avoid and handle phishing and similar attacks;
- Reviewing data breach and security incident response plans and updating if necessary;
- Mandating regular password and login information changes; and
- Continuing to monitor and audit the situation so that gaps are immediately identified and addressed.

The Doctor is at Home: Philippine Legal Issues for Telemedicine

Part of the Philippine Government's response to the pandemic is to provide guidelines on the use of telemedicine. On 28 March 2020, the DOH and NPC issued Joint Memorandum Circular No. 2020-0001 (JMC No. 2020-0001) setting out these guidelines, which include (i) requiring telemedicine services to adhere to the standards of the practice of medicine and health privacy under applicable laws, (ii) promoting the use of electronic documents in providing health services, (iii) prescribing coordination between telemedicine partners and healthcare providers, and (iv) ensuring that emergencies and serious conditions are not managed via telemedicine.

The DOH defines *telemedicine* as "the practice of medicine by means of electronic and telecommunications technologies, such as phone call, chat or short messaging service (SMS), audio- and video-conferencing, to deliver healthcare at a distance between a patient at an originating site and a physician at a distant site."

But, the DOH-NPC guidelines are only temporary; JMC No. 2020-0001's effectivity automatically ceases once ECQ is lifted. When this happens, part of the new normal will likely be a greater interest in, and need for, telemedicine. While there is a bill seeking to establish a Philippine eHealth system that regulates the delivery of telehealth and telemedicine services, the measure is still currently pending in Congress. Meanwhile, persons interested in providing telemedicine services, including non-resident enterprises, will need to contend with certain Philippine legal issues, including:

1. *A need for consultants to obtain a license to practice medicine in the Philippines.* All persons providing medical or clinical services via ICT must be duly qualified and licensed in accordance with the Medical Act of 1959 and related rules. Foreign health professionals seeking to render medical services in the Philippines may be permitted to practice medicine here, subject to conditions. Any person found to be engaged in the illegal practice of medicine may be subject to criminal prosecution and punishment.

2. *A need for relevant devices to be registered with the FDA***.** Telemedicine devices, such as apparatuses or equipment with built-in medical sensors that store and electronically transmit a patient's health data to medical providers via ICT, are considered *medical devices*. These must be registered with the Food and Drug Authority. Software that performs particular clinical functions such as generating a preliminary diagnosis based on symptoms specified by a user can be considered a medical device and would have to be registered.

3. *Compliance with Philippine data privacy laws*. Telemedicine providers would be collecting and using personal data of clients and would therefore likely be considered data controllers under the DPA. Apart from complying with requirements under this general privacy law, providers may need to consider any applicable codes and guidelines for medical professionals.

These regulatory concerns are, of course, in addition to other legal issues, such as that of the relevant standard of diligence and accountability for telemedicine companies, and the duty of care in a situation where diagnosis and treatment are done remotely or *via* a web-based machine or software. At present, questions of this nature would likely need to be examined from the perspective of local civil law principles.

Quick Round-Up: Philippine Payment Services Regulation

Anyone stuck at home in a lockdown and looking for a pizza or needing to transfer funds probably understands that a significant shift in the Philippines from traditional methods of banking and financial transactions to online platforms needs to be part of the new normal. The *Bangko Sentral ng Pilipinas* (BSP or the Philippine Central Bank), while assuring the public of the continued availability of banking services, encouraged the use of electronic banking and digital payment services as safer alternatives.[2] For humanitarian delivery of cash and voucher assistance, the Global Health Cluster led by the World Health Organization has likewise stressed that contactless electronic or mobile payments should be the preferred option to reduce the risk of COVID-19 transmission. Perceptions that cash, debit or credit card terminals or PIN pads potentially spread pathogens may also affect the payment behavior of individual and institutional clients.

Any uptake in the volume of cashless transactions in the Philippines will happen at a time when local regulation of payment services in the Philippines is relatively nascent. The National Payment Systems Act (NPSA), enacted in October 2018, gave the BSP regulatory power over the operation

[2] BSP, *The BSP Assures the Public of Continuing Banking Services*, March 16, 2020, at http://www.bsp.gov.ph/publications/media.asp?id=5311 (last visited April 16, 2020).

of payment systems, with the aim of controlling systemic risks that can threaten the stability of payment systems or financial markets. The NPSA defines an operator of a payment system (OPS) as an entity that "provides clearing or settlement services in a payment system, or defines, prescribes, designs, controls or maintains the operational framework for the system".

The Manual of Regulations for Payment Systems (MORPS), the first tranche of which was introduced by the BSP in September 2019, expanded the definition of an OPS and effectively imposed a registration requirement on any entity that: (i) maintains the platform that enables payments or fund transfers within or across institutions; (ii) operates the system or network that enables payments or fund transfers to be made through the use of a payment instrument; (iii) provides a system that processes payments on behalf of any person or the government; or (iv) performs similar activities, as may be determined by the Monetary Board of the BSP.

Because of the wide net cast by the BSP, entities are expected to conduct a self-assessment to determine if their activities fall within the scope of the expanded definition of an OPS. Studying the application of the NPSA as implemented by the MORPS and navigating the multiple registrations required of institutions that are already licensed and supervised by the BSP have become significant concerns for fintech companies and other affected businesses.

More questions may arise with the upcoming issuance of the Payment System Oversight Framework. Based on the draft BSP Circular, [3] the PSOF introduces new classes of payment system participants, imposes reportorial requirements on such participants, provides guiding principles for the BSP's supervision, and fleshes out the procedure and criteria for the designation of payment systems.

In a world that has experienced a pandemic, the Philippine payment services sector may find a silver lining for its business, but if the BSP continues to adopt a broad view in implementing the PSOF, the sector may need to also brace itself for a greater regulatory burden.

Report on CBDCs: Time for an E-Peso?

The implementation of the ECQ as part of the Philippines' effort to manage COVID-19 has resulted in financial institutions temporarily closing down branches and operating those that remain open through a lean skeletal workforce. As a result, access to cash in quarantined areas has been significantly curtailed. As noted in the bulletin on payment services (above), the BSP has not only encouraged the general public to use available digital platforms for their financial transactions; it has also urged all BSP Supervised Financial Institutions (BSFIs) to temporarily suspend all fees and charges for online financial transactions during the pandemic and many BFSIs have voluntarily done so. This notwithstanding, the sight of long lines outside open branches of banks and remittance centers remained common. It appears that the use of digital means to facilitate financial transactions has not yet gained significant traction as a majority of the general public continue to try to access cash using traditional channels and conclude financial transactions via traditional means (i.e., using actual cash). The situation has prompted renewed

[3] BSP, *Draft Payment System Oversight Framework Available for Comments*, March 16, 2020, at http://www.bsp.gov.ph/publications/media.asp?id=5316 (last visited April 16, 2020).

calls for the BSP to consider the roll out of a Central Bank Issued Digital Currency (CBDC) for the Philippines.

Existing infrastructure for digital financial transactions in the Philippines consists of online banking, e-money and payment systems platforms. The operation of online platforms by BSFIs is regulated by the BSP through its Manual of Regulations for Banks and its Manual of Regulations for Non-Bank Financial Institutions and the key thrust of the regulations is on transaction security and anti-money laundering. Online access to cash is generally available for as long as customers have internet access.

In 2017, the BSP adopted a National Retail Payment System (NRPS) Framework for the Philippines with a view to establishing a safe, efficient and reliable online payment system for the Philippines (BSP Circular No. 980, 2017). In October 2018, President Rodrigo Duterte signed the NPSA into law (see bulletin above). The NPSA provides the legal framework for regulating payment systems in the Philippines. The NRPS Framework and the NPSA ushered in (1) the establishment of centralized automated clearing houses for batch electronic fund transfers (PESO NET) and low value instant electronic fund transfers (INSTAPAY) and (2) registration of operators of payment systems in the Philippines. While transactions using digital payments have steadily increased, digital payments are only available for certain transactions and only in bigger retail stores and establishments. Technology for the use of virtual currencies and cryptocurrencies is also available but acceptance and use remains low. Virtual currencies are not recognized as legal tender in the Philippines and only the exchange of virtual currencies to fiat currency is regulated by the BSP.

CBDCs are essentially money in digital form which is intended to be handled electronically from end to end. It differs from electronic money (e-money) since e-money is merely a representation of actual cash stored in an electronic device and which may be used for payment (BSP Circular No. 649, 2009). CBDCs are not intended to be a “mere representation” of money – it is actual electronic cash. CBDCs are similar to virtual currencies and cryptocurrencies as it is also in electronic form. However, CBDCs are issued or backed by a central bank or a central monetary authority and is guaranteed by the state. CBDCs are generally considered as having an advantage over cash as it will be difficult to counterfeit. The regulatory burden in combatting money laundering and other forms of financial fraud will also be lighter since digital transactions would be easier to track. A shift to CBDCs will also eliminate the administrative burden of printing and minting actual cash.

While the COVID-19 pandemic has spurred heightened interests in CBDCs, many economies have been looking at CBDCs even before the pandemic. Venezuela already issued its own CBDC and China is reportedly poised to issue a Bank of China backed CBDC in the very near future. The BSP has also already previously expressed interest in CBDCs. In 2018, the BSP confirmed that it was considering policies in relation to CBDCs with a view of ensuring that Philippine financial institutions are ready and capable of accepting international financial transactions using CBDCs issued by other sovereigns. Back then, the BSP said that it was not keen on issuing a CBDC for the Philippines. Legislation on the creation of a Philippine CBDC or the E-Peso was proposed as early as 2014. Recently, the BSP affirmed that it was looking into all forms of digital

based financial products, including CBDCs, in line with its goals of brining the financial system closer to all Filipinos.

A policy shift towards a CBDC for the Philippines needs to keep in mind that like any technology-based product, the successful integration of CBDCs in the Philippines rests on a robust legal and regulatory framework and a solid financial technology infrastructure. The BSP would need to ensure that a sufficient and responsive legal and regulatory framework is in place and this legal and regulatory framework needs to consider the impact of CBDCs on existing BSFIs that operate and do business based on a cash-deposit model. The NRPS (and the gains of the BSP in implementing the NRPS) shows that the country can establish the required technology to support online financial transactions. However, the BSP needs to ensure a geographically balanced development of digital financial transaction technology across all Philippine economic classes especially those in the unbanked and marginalized sectors. Otherwise, the use of CBDCs will remain just another digital option for the already banked sector of the general public.

This bulletin was prepared by the SyCipLaw TMT Group.

For more information about the legal issuances discussed in this bulletin, please contact any of the following:

Rose Marie M. King-Dominguez
Partner
rmmking@syciplaw.com

Franco Aristotle G. Larcina
Partner
fglarcina@syciplaw.com

John Paul V. de Leon
Partner
jpvdeleon@syciplaw.com

This bulletin contains a summary of the legal issuances discussed above. It was prepared by SyCip Salazar Hernandez & Gatmaitan (SyCipLaw) to update its clients about recent legal developments.

This bulletin is only a guide material and is circulated for information purposes only. SyCipLaw assumes no responsibility for the accuracy, completeness or timeliness of any information provided in this bulletin. It does not constitute legal advice of SyCipLaw or establish any attorney-client relationship between SyCipLaw and the reader. It is not a substitute for legal counsel. Online readers should not act upon the information in this bulletin without seeking professional counsel. For more specific, comprehensive and up-to-date information, or for help regarding particular factual situations, please seek the opinion of legal counsel licensed in your jurisdiction.

SyCipLaw may periodically add, change, improve or update the information in this bulletin without notice.

Please check the official version of the issuances discussed in this bulletin. There may be other relevant legal issuances not mentioned in this bulletin, or there may be amendments or supplements to the legal issuances discussed here which are published after the circulation of this bulletin.

SyCip Salazar Hernandez & Gatmaitan
SyCipLaw Center, 105 Paseo de Roxas
Makati City 1226, The Philippines
t: +632 8982 3500; +632 8982 3600; +632 8982 3700
f: +632 8817 3145; +632 8817 3896
e: sshg@syciplaw.com
www.syciplaw.com