NATIONAL PRIVACY COMMISSION

NPC COVID-19 BULLETINS

#SiguruhingSigurado

#RightToDataPrivacy

#DataPrivacyIsARight

Volume 1

TABLE OF CONTENTS

NATIONAL
PRIVACY
COMMISSION

privacy.gov.ph privacy.gov.ph privacy.gov.ph privacyPH

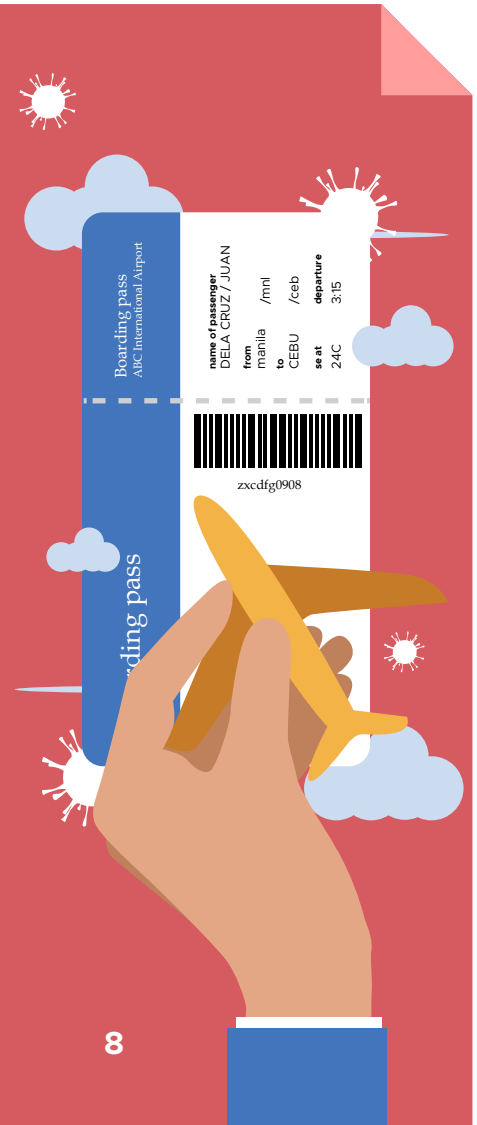
NPC PHE
Bulletin No.
01

Statement of Privacy Commissioner Raymund Enriquez Liboro

on the release of passenger manifest of airlines to government agencies particularly the DOH, in relation to the 2019 nCov response

NPC PHE Bulletin No. 01

Statement of Privacy Commissioner Raymund Enriquez Liboro on the release of passenger manifest of airlines to government agencies particularly the DOH, in relation to the 2019 nCov response



While data privacy is a right, it is not an absolute right. The same should always be harmonized vis-à-vis the requirements of public order and safety, and to protect the life and health of the data subject or another person. (Data Privacy Act of 2012, Sec 12. D and E)

If a government agency pursuant to its constitutional or statutory mandate, requests airlines to release passenger manifest, the same is allowed under the Data Privacy Act of 2012.

In responding to a critical public health issue like nCov, the DOH has the mandate, purpose and the necessity to collect and process personal data to uphold the public welfare. Therefore, nothing should prevent airline companies from releasing relevant passenger data to competent and mandated authorities like the Department of Health.

The Data Privacy Act of 2012 is not meant to prevent the government from processing personal and sensitive personal information when necessary to fulfill their mandates. Rather, it aims to protect the right to data privacy while ensuring free flow of information. What the DPA does is to promote fair, secure, and lawful processing of such information.

We recognize that the passenger manifest to be disclosed with the pertinent government agencies may pose privacy risks to individuals. While the Data Privacy Act of 2012 will not stand as an obstacle to the fulfillment by public authorities of their constitutional and statutorily mandated functions, the DPA nonetheless serves as a reminder of the need for data protection in order to assure that rights of data subjects will be protected.

NPC PHE
Bulletin No.
02

Statement of Privacy Commissioner Raymund Enriquez Liboro

on the Declaration of
Public Health Emergency
in Relation to COVID-19

Data Privacy Vis-à-vis Public Health

Following the President's declaration of a public health emergency (PHE) concerning COVID-19, it is imperative upon the government to strike a balance between individual data privacy vis-à-vis public health interests, including the public's right to know.

We wish to emphasize that the Data Privacy Act does not prevent the government from doing its job. It follows that the DPA should not prevent government, especially public health entities, from processing personal and sensitive personal information when necessary to fulfill their mandates during a public health emergency.

Government Agencies' Access to COVID-19 Information

The proper handling of the health information of Coronavirus patients is crucial in stopping the spread of the virus. Government agencies mandated to address the PHE must have access to the relevant information to accomplish the purpose.

The Department of Health has been cautious in upholding patients' confidentiality. It is releasing only information that is necessary to protect public health during this time of emergency without sacrificing its duty to determine cases and conduct contact-tracing to contain the virus.

The DOH will be walking a fine line in releasing a COVID-19 patient information to the public. Releasing patient information could produce fear and distress but may also make the people adopt the right precautions to stop the spread of the virus. During times of emergency, it is best to adhere to global best practices (as espoused by the General Medical Council, UK.) when assessing what type of patient personal information to disclose. We need to consider:

1. The potential harm or distress to the patient arising from the disclosure.
2. The potential damage to trust in doctors and health institutions in general.

and weigh it versus:

1. The potential harm to the public if the information is not disclosed.
2. The potential benefits to individuals and society arising from the release of information.

The DOH must continue performing its role and make that crucial call on what information is necessary for release to the public.

Safeguarding Patient Information; Upholding Right to Privacy

Revealing the identities to the public or providing information that could accurately identify people who are under investigation or have contracted the disease is counter-productive and could do more harm than good. If people believe that their identities will be released to the public when they come out for testing, they may be discouraged to come out—making it more difficult for the DOH and the rest of the inter-agency task force to identify more COVID-19 cases.

Any unnecessary disclosure of personal information may stunt government efforts to identify and test individuals with confirmed cases effectively and may have serious consequences, which could be far worse than the disease itself.

Responsible Sharing of Verified Information

Only pertinent information necessary in facilitating contact tracing should be collected, such as but not limited to: travel history, and frequented locations. Likewise, the only information required to enable contact tracing shall be disclosed to the public.

We call on the public and the media to be responsible when sharing and publishing information to ensure the health and safety of everyone. It is prudent to confirm with the DOH's official statistics and other information before sharing any pieces of information, especially information that would lead to the identification of an individual.

NPC PHE
Bulletin No.
3A

Collect what is necessary. Disclose only to the proper authority

Data Protection in Times of Emergency

The National Privacy Commission recognizes the extraordinary challenges our nation is facing due to this unfamiliar global pandemic. We all share the same concern and the urgent need to contain the spread of the virus. To win this battle against COVID- 19, trusted and verified information is vital. Thus, during this time, it is not only the "misuse" of data that concerns us but also the "missed" use that could have made a difference in containing the disease.

Data protection and privacy should not hinder the government from collecting, using, and sharing personal information during this time of public health emergency. Neither does the law limit public health authorities from using available technology and databases to stop the spread of the virus. The principles contained in the law allow the use of data to treat patients, prevent imminent threats, and protect the country's public health and still provide the level of protection the citizens expect. The Data Privacy Act of 2012 is an enabler in critical times like this.

We will continue issuing guidance to support our health practitioners and government units to properly and effectively use personal data to ensure the safety and security of everyone. For our frontliners: "To be able to communicate directly with the public, the medical and scientific community, and other government bodies. To coordinate nationally and globally".

The following FAQs have been collated by our NPC staff to answer questions raised by government agencies, private companies, and the public. We will try our best to continue to respond to your queries in the days ahead.

The direction is lawful and straightforward. COLLECT WHAT IS NECESSARY. DISCLOSE ONLY TO THE PROPER AUTHORITY.

The power of data in responding to this global public health emergency cannot be overstated. The NPC is fully ready to help facilitate the safe and rapid flow of data to fight COVID-19

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

FAQs

Questions raised by stakeholders on the processing of personal data concerning the state of public health emergency (PHE) and the COVID-2019 response:

ON MONITORING OF PERSONS ENTERING OFFICES/BUILDINGS

1

Q **Can we collect the details (name, contact details, and travel history) of all persons who will be entering our building through a form as may be required by a Department of Health (DOH) circular?**

A Yes, the building or office administrators may collect such personal data but only as may be necessary with what is required by the DOH.

2

Q **Will the mere filling out and signing of such form amount to the consent required by the Data Privacy Act of 2012 (DPA)?**

A The basis of the processing of data in this scenario is not consent. Its lawfulness rests on the mandate of the Department of Health, given the declaration of the state of public health emergency in response to the COVID-19 pandemic.

It is advisable, though, to provide a privacy notice informing the visitors of the purpose and basis of the collection of such personal data. Once collected, reasonable and appropriate safeguards must ensure the security of the forms and personal data contained therein.

3

Q **What are the specific data elements that we should collect from guests/visitors?**

A The specific data elements to be collected should be coordinated with the DOH as these would depend on what the latter needs to facilitate contact tracing.

Further information is available at the DOH website: https://www.doh.gov.ph/2019-nCov/interim-guidelines, and specifically for contact tracing: https://www.doh.gov.ph/sites/default/files/health-update/DC2020-0048-Reiteration-of-DM2020-0068-Interim-Guidelines-on-Contact-Tracing-for-Confirmed-2019-nCoV-ARD-Cases.pdf

ON EMPLOYEES; COLLECTION OF PERSONAL DATA

4

Q **Can an employer ask its employees to submit declaration forms that provide personal data – for instance, whether they have traveled to or been in close contact with persons who have gone to regions affected by COVID-19, whether they are experiencing symptoms, etc.?**

A Yes, employers may collect such personal data. The National Privacy Commission (NPC) reminds all employers to collect what is only necessary, observing the general data privacy principle of proportionality. Once collected, reasonable and appropriate safeguards should ensure the security of the forms and personal data contained therein.

5

Q **What are the specific data elements that an employer should collect?**

A The specific data elements to be collected should be coordinated with the DOH as these would depend on what the latter needs to facilitate contact tracing.

Further information is available at the DOH website: https://www.doh.gov.ph/2019-nCov/interim-guidelines, and specifically for contact tracing: https://www.doh.gov.ph/sites/default/files/health-update/DC2020-0048-Reiteration-of-DM2020-0068-Interim-Guidelines-on-Contact-Tracing-for-Confirmed-2019-nCoV-ARD-Cases.pdf

6

Q **Can the employer disclose the personal data collected from employees to third parties?**

A Disclosure of employee data in this scenario should be limited to the DOH and other appropriate government agencies and following all existing protocols on the matter.

7

Q **Should we ask our employees to sign a consent form or waiver that their information will be shared with the DOH if needed or requested?**

A Since the basis for the disclosure is not consent, then no consent form is needed. Instead, a privacy notice should be put in place informing employees of the purpose of collection.

ON CONTRACT TRACING; PERSONS UNDER INVESTIGATION

8

Q **Does an employer need to ask for the consent of an employee who is a person under investigation (PUI) for COVID-19 when disclosing the PUI's data to the person/s that such PUI have had contact with during the time of suspected infection?**

A Contact tracing should be done only upon the authority, guidance, and instruction of the DOH.

See the DOH Interim Guidelines on Contact Tracing available here at this link: https://www.doh.gov.ph/sites/default/files/health-update/DC2020-0048-Reiteration-of-DM2020-0068-Interim-Guidelines-on-Contact-Tracing-for-Confirmed-2019-nCoV-ARD-Cases.pdf

9

Q **If a PUI has been proven positive of the COVID-19, can I freely disclose the identity to everyone within the company? The purpose is to inform those who may have had contact with the person so they can be tested and monitored as well**

A The company may make the necessary notices internally without disclosing the identity of the person who is COVID-19 positive. The proper authority that does contact tracing is the DOH. It follows that disclosure of the identity of the patient shall be limited to the DOH personnel only, following the PUM/PUI protocol.

Companies should only disclose such personal information as may be necessary to enable other employees to assess their health and potential exposure. Here, revealing the identity of the COVID-19 patient offers no benefit to the patient nor any advantage to other members of the company in assessing their exposure. If someone in your company tests positive, protocols, and guidelines for PUMs/PUIs would apply and, generally, would cover everyone.

10

Q **Can our company issue a press release or statement relating to our employee, who is a confirmed case for COVID-19?**

A Announcements should come from the DOH or other appropriate government agencies. The government should only make the official announcement regarding COVID-19 cases in the country. Anyone with relevant information should immediately relay it to the DOH for proper handling.

11

Q **Can the DOH release names of PUIs that are purposely evading or escaping mandatory quarantine, as well as those who deliberately lied about their medical and travel history to protect the public and apprise them of the possible threat of contamination?**

A The DOH needs to consider the following factors when assessing the disclosure of patient information to the public:

- The potential harm or distress to the patient arising from the

disclosure

- The potential damage to trust in doctors and health institutions in general and weigh it versus:
- The potential harm to the public if the information is not disclosed.
- The potential benefits to individuals and society arising from the release of information.

Apart from the Data Privacy Act of 2012, there is another law relevant to this matter. RA No. 11332 or the Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act penalizes non-cooperation of the persons identified as having a notifiable disease or affected by the health event of public concern.

The DOH makes the crucial call on what information is necessary for release to the public, taking into consideration the state of public health emergency and the overall strategy to contain the virus as directed by the Inter-Agency Task Force.

12

Q **Can the DOH publicly disclose more detailed information of the frequented locations of the persons positive for COVID-19 to inform the public better and help prevent the transmission of the virus?**

A Yes. The DOH can provide information about the frequented locations of the persons positive for COVID-19 without giving details that would identify individuals.

Personal information controllers are advised to approach any uncertainty as to the collection and disclosure of personal data of PUIs, PUMs, and confirmed cases of COVID-19 in a reasonable manner.

We trust that all shall be socially responsible. False information about COVID-19 may create more problems. Please refrain from sharing unverified reports and fake news to avoid undue stress and worry due to misinformation.

Finally, we emphasize that the DOH is the primary competent authority handling our country's response to the COVID-19. We support our health department, the Inter-Agency Task Force for the Management of Emerging Infectious Disease, health front liners, emergency responders, law enforcement officers, and other persons undertaking our country's response and measures to curtail and eliminate the COVID-19 threat.

For questions or concerns, you may visit our website at **https://www.privacy.gov.ph/** and may reach us at **info@privacy.gov.ph**.

NPC PHE
Bulletin No.
3B

Wastong pangangalaga sa personal na impormasyong pangsugpo sa COVID-19 pandemic

Kinikilala ng National Privacy Commission ang mapaghamong sitwasyong hinaharap ng ating bansa dahil sa pandaigdigang paglaganap ng bagong sakit. Lahat tayo ay nangangamba at umaasa na madaling masusugpo ang virus na tinaguriang COVID-19. Sa panahong ito, napakahalaga ng tama at beripikadong impormasyon. Hindi lamang maling paggamit ng data ang inaalala natin, pati na rin ang mga hindi nasagap na impormasyong sana'y makakatulong sa pagtigil ng sakit na ito.

Hindi dapat maging balakid sa gobyerno ang Data Privacy Act (DPA) of 2012 upang makalap, magamit, at maibahagi ang mga personal na impormasyon na kritikal sa kalusugan ng buong bansa.

Higit pang hindi balakid ang DPA sa mga kawani ng pampublikong pangkalusugan na gumamit ng teknolohiya at mga database ng personal data para mapatigil ang pagkalat ng virus.

Ang mga prinsipyong nakasaad sa batas ay naglalayong pahintulutan ang paggamit ng personal data upang kumalinga sa mga pasyente, pigilan ang mga nakaambang panganib, at protektahan ang kalusugan ng lahat ng Pilipino. Bagama't sa kabila ng lahat ng ito ay makapagbigay pa rin ng seguridad sa personal data tulad ng inaaasahan ng publiko.

Sinisiguro ng DPA ang mabilis at maayos na daloy ng kailangang impormasyon sa mapanganib na panahong gaya nito.

Ipagpapatuloy namin ang gabay at suporta sa ating health practitioners maging ang mga sangay ng gobyerno, upang ang tama at wastong paggamit ng personal data ay magdulot ng kaligtasan at kapanatagan sa ating lahat. Para sa ating Frontliners: "Upang direktang maipabatid sa publiko, sa inyong mga kasamahan na manggagamot, at iba pang ahensya ng gobyerno. Maging pagpapabilis ng pagkilos laban sa COVID-19 sa buong bansa at sa daigdig."

Nakalap ng aming mga kasamahan sa NPC ang FAQs na ito upang masagot ang madalas na tanong mula sa iba't ibang ahensya ng gobyerno, pampribadong kumpanya, at publiko. Gagawin namin, sa abot ng aming makakaya, na masagot nang agaran ang inyong mga katanungan sa mga susunod na araw.

Diretso at naayon sa batas lamang ang ating direksyon. KUNIN LAMANG ANG NARARAPAT. ISIWALAT LAMANG SA WASTONG AWTORIDAD.

Nais naming bigyang-diin ang kahalagahan at kapangyarihan ng tamang datos sa maagap na paglaban at pagsugpo sa pandaigdigang sakunang pangkalusugang ito.

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

NPC PHE Bulletin No. 3B

Wastong Pangangalaga sa Personal na Impormasyong Pangsugpo sa COVID-19 Pandemic

Para sa mga empleyadong papasok sa opisina/gusali:

Maaaring humingi ng impormasyon ang mga namamahala sa mga establisimiyentong hinggil sa direktiba ng Department of Health (DOH) gamit ang declaration form, kung saan idedetalye ang mga personal information gaya ng pangalan, cellphone number, email address, at iba pang contact details para sila ay matunton sakaling magkasakit at maalagaan.

Liban dito, hihingiin din ang mga lugar kung saan sila huling nagtungo upang malaman kung may COVID-19 sa naturang lugar, at pagdeklara kung may sintomas sila ng COVID-19 o wala.

HINDI na kailangang kunin ang consent ng mga empleyado sa paghingi ng personal information sapagkat nasa ilalim tayo ng isang malawakang pagkalat ng sakit sa buong mundo.

Alinsunod sa utos ng Kagawaran ng Kalusugan (Department of Health/ DOH), ipinapayong hingin lamang ang sapat at angkop na impormasyong makatutulong sa DOH sa pagtigil ng COVID-19.

Gumamit ng Privacy Notice alinsunod sa DPA. Ito ay isang nakasulat na abiso na nagpapaliwanag sa mga empleyado na ang mga nakalap na impormasyong pangkalusugan ay gagamitin para sa kaligtasan ng nakararami.

Iparating din na ang kukuning impormasyon ay para sa contact tracing. Ito ay para malinaw sa lahat kung sila ba ay may nakasalamuhang nag-positibo sa COVID-19 sa nakaraang 2 linggo. Maraming matututunan sa contact tracing mula sa

https://www.doh.gov.ph/sites/default/files/health-update/DC2020-0048-Reiteration-of-DM2020-0068-Interim-Guidelines-on-Contact-Tracing-for-Confirmed-2019-nCoV-ARD-Cases.pdf

Ang personal data ng mga empleyado ay maaari lamang isumite sa DOH at iba pang ahensya ng gobyerno na konektado sa pagsugpo sa COVID-19 pandemic.

Para sa Contact Tracing, lalo ng mga Taong Iniimbestigahan kung may COVID-19 (PUI):

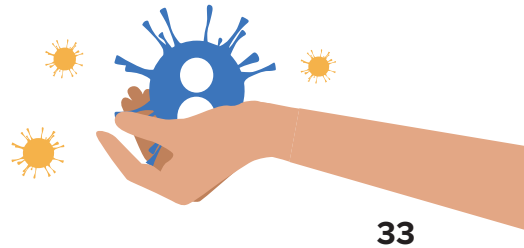
Sakaling may mag-positibo sa COVID-19 sa inyong opisina o tanggapan, ipagbigay alam ito sa inyong mga empleyado sa paraang hindi mabubunyag ang pagkakakilanlan ng may sakit. Tanging sa DOH lamang maaaring ipaalam ang pagkakakilanlan ng nag-positibo sa COVID-19.

Ipagbigay alam agad sa DOH kung mayroon kayong kilalang nagtatago pagkatapos magpositibo sa COVID-19, o kung mayroong namemeke ng papeles ng ospital at lugar na kanilang pinanggalingan kamakailan upang makaiwas sa quarantine.

Umaayon ang DPA sa Republic Act 11332 o mas kilala bilang “Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act”, na nagbibigay ng karampatang parusa sa hindi pag-uulat sa DOH ng mga nagtataglay ng nakahahawang sakit (gaya ng COVID-19).

Maaaring ianunsyo ng DOH ang mga pinanggalingang lugar ng isang pasyenteng nagpositibo sa COVID-19 nang hindi na isiswalaat ang kanyang pagkakakilanlan.

DOH lamang ang may tungkulin na isiwalat ang impormasyon ukol sa COVID-19. Kung may mahalagang balita ang kumpanya ukol sa sakit na ito, dumiretso lamang sa DOH para sa naaakmang pag-uulat nito.



Pinapayuhang maging mapanuri ang mga kumpanya sa pagkuha at pagsiwalat ng personal data ng mga apektado ng CoVID-19 tulad ng mga taong sumasailalim sa imbestigasyon (Persons Under Investigation/PUI), mga taong minamatyagan (Persons Under Monitoring/PUM), at mga taong nagpositibo na.

Hinihikayat namin ang lahat na maging responsible sa pagpoproseso ng anumang impormasyon ukol sa CoVID-19. Ang anumang maling impormasyon na maisasapubliko maaring magdulot ng kapahamakan sa lahat. Lagi nating siguraduhin ang pagkatotoo ng impormasyon at pigilin ang pagkalat nito.

Nais naming ipabatid na ang DOH ang tanging ahensya na maaring magsiwalat ng impormasyon ukol sa CoVID-19 pandemic. Kami ay sumusuporta sa DOH, Inter-Agency Task Force (IATF) for the Management of Emerging Infectious Disease, at frontliners na tumutulong na mapabilis ang pagsugpo sa CoVID-19 sa ating bansa.

Para sa mga katanungan at agam-agam, maaaring puntahan ang aming website sa **https://www.privacy.gov.ph/** at makipag-ugnayan rin sa **info@privacy.gov.ph.**

NPC PHE Bulletin No. 04

Protecting personal data in the time of COVID-19

NPC PHE Bulletin No. 04

Protecting personal data in the time of COVID-19

A growing number of online fraudsters are exploiting the public fear surrounding the COVID-19, using the pandemic to lure people into clicking phishing emails and installing malwares capable of stealing personal data and money.

Our fear during a crisis can expose us to data privacy risks, predisposing us to make hasty or ill-informed choices online, which fraudsters are taking advantage of.

In view of these heightened risks, the National Privacy Commission is appealing to everybody to be very careful online, especially when using online financial services and accessing health-related apps. Be cautious with the sites you visit, enhance your privacy settings, and protect your personal data.

In this period of home quarantine, digital access becomes our main gateway not just for news but also to coordinate tasks with co-workers, make online financial transactions and most importantly, get in touch with loved ones.

Indeed, now is the worst possible time to fall victim to online fraudsters. They can steal your sensitive data, cause you financial and reputational damages, make your device unusable and cut you off from the outside world.

To avoid such scenarios, we need to be vigilant and familiarize ourselves with the warning signs.

The National Privacy Commission encourages everyone to practice the following tips to protect personal data in the time of COVID-19:

Do not give out your personal data in suspicious COVID-themed emails and messages.

Is the email or message unsolicited? Does it urgently encourage you to open the attached file? Is it promising COVID vaccines or cure that you have not heard of at all in the news or credible websites? Do not click them. It is most likely a phishing attack that steals your financial data such as credit card or online banking details.

Make trusted government and other legitimate websites your go-to source for the latest COVID information.

We have a lot of questions about the pandemic. We will not find these answers, however, on some random websites or applications. What we may find on these sites instead are suspicious links, pop-ups and downloadable files, resulting in a ransomware infection that locks us out of our devices. Not only do you protect yourself from ransomware by relying on trusted sources, you also get to avoid misinformation.

Ensure that the charity or crowdfunding campaign you plan to donate to is legitimate.

Research online or through your social media contacts from whom you learned of the charity or crowdfunding campaign. Know where your donations will go. Think twice if the charity rushes or pressures you or makes unrealistic promises just to get you to donate. If you've decided to make the donation, be sure to check your bank statements and see if you've been charged the right amount.

Be mindful of phishing baits from online scammers.

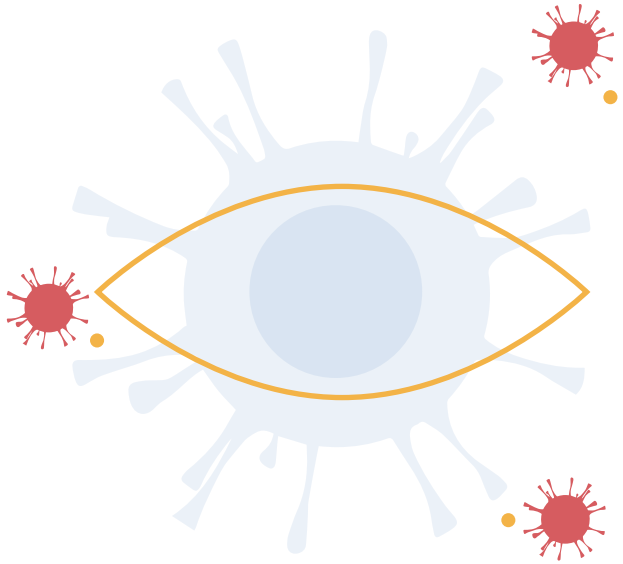
Scammers want you to click on a link or give your password, account number and other personal information. This way they can steal your identity, money and gain access to your computer or cellphone. To do this, they use familiar company names or pretend like someone you know. They pressure you to act now or else.

When you receive such messages, be skeptical. Look up the website or phone number for the company or person contacting you. Call them directly using the company's official number or email. Never give any personal information especially your password and pin number.

Most phishing attempts use bad grammar and spelling. There are some, however, that looks legitimate and very convincing.

During this critical period, all our focus and efforts should go to the fight against the spread of the COVID-19 virus. We should avoid, at all cost, getting sidetracked by these digital pitfalls.

In case you feel that your personal data have been compromised, please feel free to contact our complaints and investigation team. You may email us at **complaints@privacy.gov.ph** and **info@privacy.gov.ph.**



NPC PHE Bulletin No. 05

Statement of Privacy Commissioner Raymund Enriquez Liboro

on "Social Vigilantism" in the time of COVID-19

NPC PHE Bulletin No. 05

Statement of Privacy Commissioner Raymund Enriquez Liboro on "Social Vigilantism" in the time of COVID-19

The National Privacy Commission strongly condemns "social vigilantes" who attack or threaten the safety of health workers amid the COVID-19 pandemic in the misguided belief that such acts of discrimination may serve the public good.

Social vigilantes are those who take it upon themselves to enforce their views of what they consider appropriate beliefs and behavior.

There have been incidents in which vigilantes doused chemicals on health workers, expelled them from boarding houses or refused them lodging and even barred them from taking tricycles on their way to work or home.

The health workers are being attacked as a group, prompting a number of them not to wear uniforms in public for fear of being discriminated against, or worse assaulted.

These acts are unacceptable and their perpetrators must be penalized in accordance with law.

We also denounce people who irresponsibly publicize the personal data of persons under investigation (PUIs) and persons under monitoring (PUMs), thus exposing them to danger even graver than the novel coronavirus itself – that of maltreatment, online bullying and physical violence from individuals who may be driven by desperation and fear.

Our health workers, as well as the PUIs and PUMs under their watch, are not the enemy. They are on the battlefront of the public health emergency, doing their part to contain the crisis and deserving the support and compassion from the rest of us.

Their human rights must be respected in these times of great social and economic distress. They have the right to be left in peace and their personal information protected against being disseminated without their consent.

Once personal information of health workers, PUIs and PUMs is divulged, targeting, doxing and stigmatization are not far behind.

Social vigilantes contribute to the problem by dampening the bayanihan spirit and damaging our collective capacity to respond in an organized and humane way. They must, therefore, be discouraged and stopped.

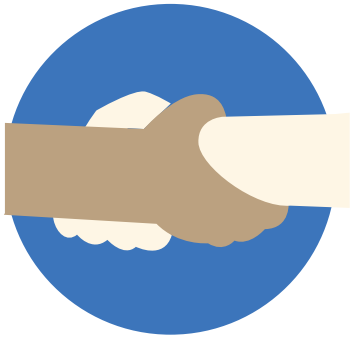
In fulfillment of its twin mandate to protect the fundamental human right of privacy and ensure the free flow of information to promote innovation and growth, the National Privacy Commission is committed to deter all unlawful use of personal data.

NPC PHE Bulletin No. 06

Collect the minimum necessary information in providing financial aid and other relief packages to those affected by the enhanced community quarantine

NPC PHE Bulletin No. 06

Collect the minimum necessary information in providing financial aid and other relief packages to those affected by the enhanced community quarantine



The National Privacy Commission (NPC) supports efforts by the national government to provide much-needed assistance to our people in these extraordinary times.

We remind all government offices, including local government units, to further ease the people's burden by exercising proportionality and collecting less of their data to facilitate such assistance.

Collect only necessary personal details, such as those required according to usual accounting, auditing, and budgeting rules and regulations when disbursing public funds, as well as other applicable laws and regulations.

Avoid burdening recipients with personal data requirements that are beyond the minimum necessary, which would only impede the speedy flow of aid distribution in this time of urgency.

All collected personal data must be safeguarded to prevent any unauthorized access and use. Appropriate retention and disposal policies should also be in place. Collect to meet present objectives and discard any notion of possible future use of the data.

On the part of the employers, the need to obtain consent from concerned affected workers is not required under the present emergency when submitting requirements to government regulatory agencies mandated to distribute aid to these workers.

It is during these trying times that the data protection officers of companies are needed to provide timely and sensible advice to their management, considering all attendant circumstances and mindful of the rights and interests of the affected workers.

NPC remains committed to working with all agencies tasked in distributing aid to provide additional guidance and inputs, as may be necessary and appropriate.

For further guidance, we may be reached at **info@privacy.gov.ph.**

NPC PHE Bulletin No. 07

Official Statement of the National Privacy Commission on Calls for Patients to Waive Privacy Rights, Publicly Disclose Health Status

NPC PHE Bulletin No. 07

Official Statement of the National Privacy Commission on Calls for Patients to Waive Privacy Rights, Publicly Disclose Health Status

Amid the public health crisis, we have been hearing calls from certain quarters for patients to temporarily set aside their data privacy rights, as though doing so makes for a robust weapon in overcoming this pandemic. In this war that is testing our humanity and values, it should be emphasized that protecting privacy rights is tantamount to protecting lives.

The Data Privacy Act of 2012 (DPA) is not a hindrance to the COVID-19 response. There are enough provisions in the law to allow contact tracing, treating patients, and addressing threats while guaranteeing the privacy that COVID-19 positive patients, persons under investigation (PUIs), and persons under monitoring (PUMs) expect.

Republic Act No. 11332 (An Act Providing Policies and Prescribing Procedures on Surveillance and Response to Notifiable Diseases, Epidemics, and Health Events of Public Health Concern) mandates patients, PUIs, and PUMs to be fully transparent and truthful to the Department of Health (DOH), our hospitals, and other pertinent public authority on the personal data (travel and medical history, etc.) requested from them. Such information will be material for health and local institutions to treat them and/or properly contain the spread of the infectious disease in a timely manner.

Where they may falter in cooperation, as when they refuse to provide details or conceal required information, patients can be penalized with imprisonment and hefty fines under RA 11332.

In addition, the DOH has set management protocols requiring every health institution to triage patients in emergency rooms according to their conditions. These protocols are in place and designed to keep our health workers safe.

On sharing with other authorized public authorities, the DOH may do so subject to the limitations that the sharing is (a) pursuant to a public function or a public service, (b) based on the constitutional or statutory mandate of the DOH and/or the other public authorities, (c) strictly following set protocols and processes, (d) ensuring the security of such shared information, and (e) upholding data subjects' rights.

With respect to sharing medical information of individuals to private health institutions, the Health department would be in the best position to determine if such is consistent with the provisions of RA 11332 and other applicable protocols in a pandemic.

The joint plea of the Integrated Bar of the Philippines, Philippine Medical Association and Philippine College of Surgeons quoted a recent bulletin of the National Privacy Commission (NPC). We clarify that the statement was made in connection with our appeal for the release only of "trusted and verified information," especially during an "unfamiliar global pandemic." It was never meant to support any request for the voluntary waiver by COVID-19 patients, PUIs and PUMs of the confidentiality of their medical condition.

We remain firm in our stand that authorities and institutions should collect only what is necessary and share information only to the proper authority.

On the call for patients, PUIs and PUMs to share or consent to the sharing of personal data to the general public for contact tracing, we affirm our stand that doing so may not be as helpful to contact tracing interventions as this can only induce fear among these individuals given the multiple reports now on physical assaults, harassments, and discrimination endured by patients, PUIs, PUMs, and even health workers. These threats to their safety and security may discourage them to report their symptoms to public authorities, take confirmatory tests, and submit to treatments.

If a patient, PUI, or PUM himself or herself would want to disclose such information, as what some public figures have done, that is their personal choice.

On seeking consent, the DPA requires consent to be freely given, specific, and an informed indication of will that they indeed agree to the public disclosure. Informed consent requires that these patients, PUIs, or PUMs have been made aware of the risks that may arise from the disclosure, including the risk of being subjected to violent physical attacks as some COVID positive patients and their family members have experienced according to news reports.

To conclude, we want to reiterate that even in times of calamity or a state of a public health emergency, rules on patient privacy, the confidentiality of health records, medical ethics, and data subjects' rights remain in effect and upholding them equate to protecting lives.

NPC PHE Bulletin No. 08

On COVID-19 -related apps, digital tools and solutions in this time of pandemic

NPC PHE Bulletin No. 08

On COVID-19- related apps, digital tools and solutions in this time of pandemic

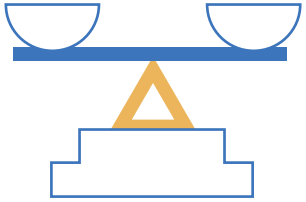
The National Privacy Commission (NPC) supports the successful use of digital technologies and the processing of personal data to enable health authorities contain the COVID-19 pandemic, in a manner that is effective and preserves and protects the data privacy rights of individuals.

For COVID-19 related apps to be successful, these must be inclusive and trusted. Therefore, efforts should be geared not only towards its rapid deployment but also in ensuring that the widest segment of the population with their devices can avail of these apps and that data quality is achieved. To be effective, such solutions must be trustworthy and acceptable for individual users to use with confidence so that users will share information without fear of misuse or discrimination.

COVID-19 related apps can only achieve the desired level of uptake if it is clear about its legitimate purpose, is transparent on how it uses personal data and proportional in its collection. The App must not over-collect personal information from users and collect only what is necessary for the purpose.

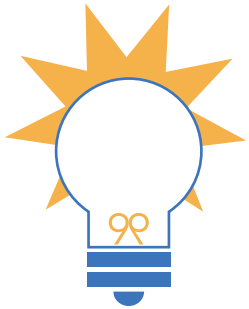
From the design stage, personal information controllers (PICs) must make sure that the app is solidly built on a legitimate purpose – making sure that it is limited to and consistent with the objective of helping defeat the COVID-19 pandemic. Thus, the app's design, functionalities, personal data collection and extent of processing must never deviate from this purpose. Once the purpose is achieved, personal data processing must stop, while the collected and generated personal data must be disposed or discarded in a secure manner to prevent any further use. In doing so, breach-related privacy risks are minimized, thus enabling user trust and adoption by the general public.

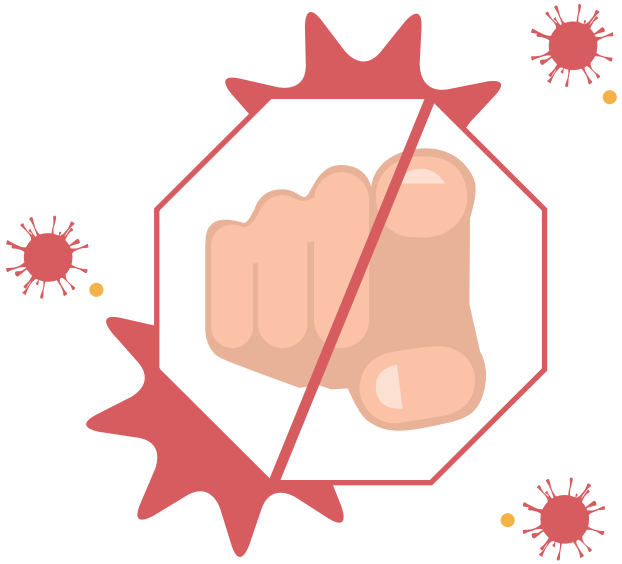
The personal data to be collected and the manner of processing must be moderated with the principle of proportionality. This means PICs must collect only the minimum data necessary to achieve the declared and specific purpose, using the least intrusive method.



PICs must also ensure transparency by telling individual users, through an easy-to-understand privacy notice, how the app or digital solution will collect, use, store, and dispose their personal data. Users must also be made aware to whom, if any, shall their personal data be disclosed incidental to the processing.

Considering the inherent vulnerability of personal data processing over the internet and in anticipation of the latest cyber threats, PICs must also ensure that appropriate security measures are identified and implemented. PICs are also expected to inform users of their data subject rights and incorporate mechanisms to easily exercise them.



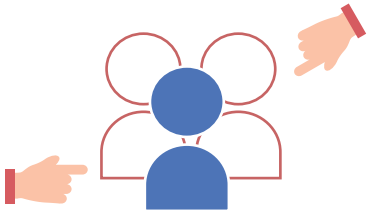


NPC PHE Bulletin No. 09

NPC supports DILG's bid vs discrimination of COVID-19 frontliners

The National Privacy Commission supports the call of the Department of the Interior and Local Government on local government units to enact ordinances to safeguard COVID-19 frontline workers against acts of discrimination.

Being a communicable disease, COVID-19 carries with it a stigma that brings out the worst in others. This stigma affects not just patients but also frontliners — health professions and hospital workers, police, military, and essential services personnel — people who have put so much of themselves in the nation's fight to contain the pandemic. COVID-19 related apps can only achieve the desired level of uptake if it is clear about its legitimate purpose, is transparent on how it uses personal data and proportional in its collection. The App must not over-collect personal information from users and collect only what is necessary for the purpose.



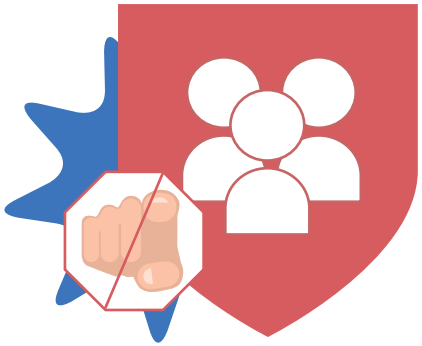
Despite the services and sacrifices frontliners contributed to defend the rest of us against the pandemic, they often find themselves battling harassment, discrimination, and even violence from people who may be acting misguidedly out of dread or distress.

Some frontliners even had their personal data shared in public, without their consent, thus exposing them to potential cyber-bullying, and causing them added stress and mental strain.

Any form of discrimination against frontliners are downright wrong and must be penalized.

Such discriminatory acts only disrupt the delivery of the most critical and valuable services our country needs right now

We need to act immediately to defend frontliners against discrimination, or risk losing the gains we achieved in this collective fight to beat the COVID-19 crisis.



NPC PHE Bulletin No. 10A

Protecting patient data from unauthorized disclosure

NPC PHE Bulletin No. 10A

Protecting patient data from unauthorized disclosure

In recent weeks, the National Privacy Commission (NPC) has received several breach notifications which involve the possible unauthorized disclosure of sensitive personal information of suspect, probable and confirmed COVID-19 patients. The NPC is now looking into said breach incidents, in accordance with our internal procedures and in collaboration with concerned Personal Information Controllers (PICs), for remediation and other purposes within the bounds of the Data Privacy Act of 2012.

With a view to preventing unauthorized disclosure from happening, we call on health institutions and their Data Protection Officers (DPOs) to strengthen the protection of patient data. After all, fostering mutual trust and protection between patients, health institutions and authorities is crucial in dealing with the COVID-19 pandemic.

Patients will only fully and truthfully disclose the needed information to authorities if they feel assured that the information will be properly used for treatment, disease surveillance and response, and will be protected against any type of misuse, such as unauthorized disclosure, which has proven to result in stigma-driven physical assaults, harassments, and acts of discrimination.

Below are some of the organizational, physical and technical security measures that health institutions and their staff may enforce to protect patient data against unauthorized disclosure:

- **Regularly remind officials and employees of their ethical and legal duty to protect patient data.** This reminder may come in the form of strategically

located posters or print outs informing every one of their responsibility to protect the confidentiality, integrity and availability of patient data, which they have been entrusted with. Health institutions may want to emphasize that unauthorized disclosure is a prohibited act, both under Republic Act No. 11332 or the Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act, and the Data Privacy Act of 2012. They should ensure that non-disclosure agreements and related contracts are in place and enforced.

Establish access control for patient data based on least privileges. Only provide access on a "need-to-know" basis. This means that health personnel are allowed only the minimum and necessary access to enable the performance of their functions.

Equip facilities with physical access controls. Protect physical access to facilities through locks and alarms. This is to ensure that only authorized personnel have access to facilities that house the systems and the data. At the same time, keep documents containing patient data in locked cabinets or secure rooms when not in use.

Only disclose patient data to proper authorities and in appropriate areas. Refrain from discussing patient data in public areas where unauthorized parties may pick up personal data, unless when providing treatment under compelling circumstances. In addition, when discussing over the phone, confirm the identity of the person first and check whether he or she is authorized to receive such information.

Protect the computer display from unauthorized or accidental viewing. Prevent the accidental viewing and disclosure of data through the use of privacy screens. If a privacy screen is not readily available or practical, place computer monitors inside secluded cubicles or angle them in such way that minimizes the chance of any unauthorized or accidental viewing by unauthorized individuals. Computers must be locked with a password whenever the authorized user leaves the workstation.

Lock storage media away when not in use. If the use of portable storage media (such as USB flash drives or external hard drives), to store patient data is unavoidable, ensure that the files are encrypted and password protected. Also, make sure they are kept secure in your person when working in public places and not left absentmindedly on desks, counters, in conference rooms, and other common areas where it may be accessed by unauthorized individuals.

Ensure that patient data are encrypted, both in-transit and at rest. Electronic copies of patient data must be protected in the same extent that physical files and storage media containing patient data are secured. Encrypting patient data both in-transit and at rest ensures that the files are locked and only accessible to authorized persons.

Communicate securely. Choose a secure platform for care team collaboration and patient communication. For further protection, ensure that the documents are encrypted with a password of sufficient strength. The password must be sent via a separate channel like SMS/text. It is likewise advised that apart from setting a strong password, a second-factor authenticator may be used whenever logging into accounts.

NPC PHE Bulletin No. 10B

Proteksyon laban sa hindi awtorisadong pagbunyag sa datos ng pasyente

Sa mga nagdaang linggo, ang National Privacy Commission (NPC) ay nakatanggap ng *breach notifications* ukol sa posibleng *unauthorized diclosure* o hindi awtorisadong pagsiwalat ng sensitibong personal na impormasyon ng *suspect, probable* at *confirmed* na mga pasyenteng may COVID-19. Kasalukuyang sinisiyasat na ng NPC ang mga nasabing insidente, alinsunod sa Data Privacy Act.

Upang maiwasan ang paglanap ng insidente ng unauthorized processing, nananawagan ang NPC sa mga institusyon na nagbibigay ng serbisyong pangkalusugan, at sa kanilang Data Protection Officers, na pagtibayin ang pangangalaga sa personal na datos ng mga pasyente. Tandaan natin, ang tiwala sa pagitan ng mga pasyente, institusyong pangkalusugan, at gobyerno ay importante sa pagsugpo sa COVID-19 pandemic.

Ang mga pasyente ay magbibigay ng totoo at kumpletong mga detalye na kailangan ng mga awtoridad kung panatag ang kanilang loob na ang kanilang sensitibong datos ay gagamitin lamang sa paggamot, pagmamatyag, at pagresponde sa COVID-19 pandemic — at gagamitin lamang na may buong pag-iingat, upang 'di ito mabunyag sa iba o magamit sa paraan na magdudulot lamang ng stigma, gaya ng diskriminasyon, panliligalig, at pisikal na pananakit.

Narito ang mga hakbang upang mapagtibay ang organisasyonal, pisikal, at teknikal na mga seguridad sa pangangalaga ng datos ng inyong pasyente upang makaiwas sa *unauthorized disclosure:*

Laging ipaalala sa inyong mga opisyal at empleyado na isang legal at moral na responsibilidad ang pagprotekta sa personal na datos ng mga pasyente. Gumamit ng praktikal na pamamaraan, gaya ng pagdikit ng posters o pamimigay ng print outs. Ipaalala na bilang katiwala ng datos, obligasyon nilang siguruhin ang *confidentiality, integrity* at *availability* nito.

Bigyang-diin na ang *unauthorized disclosure* ng datos ay ipinagbabawal ng batas, partikular sa Republic Act No. 11332 o the Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act, at DPA. Ipaalala din na may nilagdaan silang *non-disclosure agreement* kaugnay dito.

Magtalaga ng "access control" para sa datos ng pasyente, base sa "least privileges". Limitahan ang pwedeng maka-access sa datos ng pasyente, ayon sa pangangailangan. Ibig sabihin, bigyan lamang ng sapat na access ang isang empleyado upang gampanan ang kanyang tungkulin, sa panahon na ito ay kailangan.

Maglagay ng kandado, alarma, at iba pang pisikal na kagamitan pang-seguridad. Siguraduhing ang inyong pasilidad ay hindi basta mapapasok ng hindi awtorisadong indibidwal. Kapag hindi ginagamit, ang mga dokumentong naglalaman ng datos ng pasyente, dapat nakakandado ang mga ito sa isang cabinet o silid.

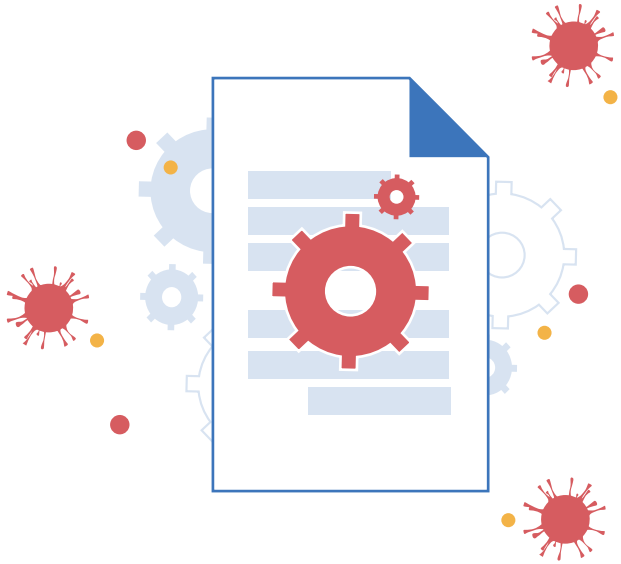
Sa tamang awtoridad lamang ibigay ang datos ng pasyente, at sa pribadong lugar lamang ito talakayin. Iwasang pag-usapan ang personal na detalye ng isang pasyente sa publikong lugar, maliban na lang kung bunsod ng *emergency*. Kung makikipag-usap gamit ang telepono, kumpirmahin muna ang identity ng nasa kabilang linya at kung awtorisado ba siya na tumanggap ng impormasyon patungkol sa pasyente.

Lagyan ng *privacy screens* ang inyong computer upang 'di masilip ng 'di awtorisadong indibidwal ang impormasyon sa screen. Kung walang privacy screen, ipwesto ang *computer monitors* sa tagong cubicle o ianggulo ito sa paraang hindi agad mahahagip ng mata. Tiyakin din na may password ang computers o laptops.

Siguraduhin na encrypted at may password ang inyong portable storage media ('gaya ng USB flash drives at external hard drives) na naglalaman ng patient data. Itago ito sa isang locked cabinet kung hindi ginagamit, at tiyakin na hindi pakalat-kalat lamang sa desk, counters, conference rooms, at iba pang common areas.

- **Tiyakin na may encryption ang electronic file o digital copies ng patient data.**

- **Siguraduhin na secure ang digital platform na gagamitin sa pakikipag-usap sa inyong team o pasyente.** Lagyan ng encryption ang dokumento o files na ipapadala sa pamamagitan ng internet. Gumamit ng passwords na mahirap hulaan, at gumamit din ng second-factor authentication kapag nagla-login sa accounts.



NPC PHE Bulletin No. 11

Joint Statement of the Department of Health (DOH) and National Privacy Commission (NPC) on Processing and Disclosure of COVID-19 Related Data

NPC PHE Bulletin No. 11

Joint Statement of the Department of Health (DOH) and National Privacy Commission (NPC) on Processing and Disclosure of COVID-19 Related Data

This joint statement is issued by the Department of Health and the National Privacy Commission in response to concerns raised by various stakeholders on the processing and disclosure of COVID-19 patient data, including those of COVID-19 suspect, probable, or confirmed patients.

We uphold the Republic Act No. 11332 or the Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act and the Data Privacy Act of 2012 in processing COVID-19 patient data in pursuit of disease surveillance and response.

As we call on all COVID-19 patients to truthfully and accurately disclose their personal data to proper authorities to help fight this pandemic, the DOH guarantees that the data privacy rights of these patients are protected. The DOH and NPC stand firm against any form of unbridled disclosure of patients' personal data to the public that has been proven to cause a real risk of severe harm to patients.

We reiterate our appeal to all COVID-19 suspect, probable, and confirmed patients. Your honesty and cooperation will allow our frontliners to adopt appropriate measures to protect themselves.

Rest assured that the DOH only discloses these data to public health authorities and concerned health care providers for purposes of contact tracing and management of the disease. These personally-identifiable data may also be disclosed to other government entities authorized based on DOH guidelines.

In these instances, public health authorities, concerned health care providers, and other government entities who are custodians of patients' personal data have the legal obligation to protect the data privacy rights of these patients and ensure the confidentiality, integrity, and availability of their personal data.

We also remind public health authorities, concerned health care providers, and other government entities to ensure and protect the privacy of COVID-19 patient data and the data privacy rights of the patients. This way, we can help allay the fears of patients on COVID-related physical assaults, harassments, and discrimination, and encourage them to report their symptoms, take confirmatory tests, and submit themselves to treatments by proper authorities.

Fostering mutual trust and protection between patients and authorities is an indispensable part of our fight to defeat the COVID-19 pandemic.

NPC PHE Bulletin No. 12

Protecting personal data in a work from home arrangement

As the Philippines was placed under varying levels of community quarantine to address the COVID-19 pandemic, organizations in the government and private sector implemented a work from home (WFH) setup, which is a type of telecommuting. Republic Act 11165 or the Telecommuting Act defines telecommuting as a "work arrangement that allows an employee in the private sector to work from an alternative workplace with the use of telecommunications and/or computer technologies."

Given the public health emergency that the country faces, the National Privacy Commission (NPC) supports the adoption of the WFH set up as a viable strategy to balance the need to preserve the health and well-being of an organization's workforce with the need to continuously operate and provide services to the public.

WFH and other telecommuting modes, is a management option determined by the organization as part of its Business Continuity Plan to facilitate organizational operations to continuously deliver work in the face of events such as typhoons, public safety or public health emergencies.

This setup, however, is not risk-free. Unauthorized access to and improper disposal of documents containing personal data due to unprotected home devices and physical files are just some of the potential dangers that come with it.

Thus, the NPC advises organizations operating under a WFH setup and other modes of telecommuting, to consider the following measures to ensure that the data privacy of data subjects remain protected.

These guidelines cover general security measures that organizations and individuals working on their own can take, not only during the pandemic but whenever a telecommuting arrangement is implemented.

GUIDELINES

Authorized Information Communication Technology (ICT) Assets.

Organizations are responsible for making sure telecommuting employees are provided the proper ICT assets. In return, employees are accountable and responsible for the physical care of those assets.

Computers and other

1. **ICT peripherals.** Employers should issue their staff with appropriate ICT resources to adequately perform their duties.

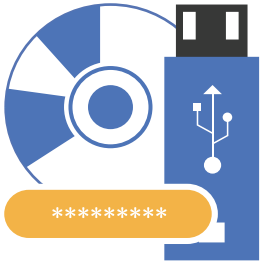
   Personal devices may be used

if provision of organization-owned ICT resources is impractical. Such practice, however, must be governed by the organization's Bring Your Own Devices (BYOD) policy.

Removable Devices.

2. Personnel are encouraged to only use organization-issued ICT peripherals (such as USB flash drives,

USB mouse, USB keyboard, etc.) When using portable media, (such as disks or USB flash drives) to store or transfer data, the use of data encryption must be ensured.



3 **Software.** Only softwares authorized by the organization must be used and only for official purposes. Avoid storing the organization's digital files, including those with personal data, on external services and softwares.

4 **Proper configuration and security updates.** Install security patches prior to and while WFH is enforced to prevent cyber security exploits and malicious damage, including the following:

- Automatic update & installation of operating system security patches
- Periodic scheduling & scanning of authorized antivirus software
- Automatic update, installation & configuration of web browser and its preferences
- Automatic update & installation of personal productivity softwares (i.e., word processor, spreadsheet processor, presentation software, etc.)
- Update and configuration of video conferencing software / platform

5 **Web Browser Hardening.** Ensure that your browser is up to date & properly configured.

Below are the configurations for popular browsers.

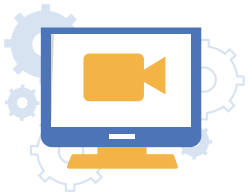
Measures	Chrome Configuration	Firefox configuration	Edge configuration
Browse in private	Use Incognito Window and delete private data when exiting browser	Use Private Window and delete private data when exiting browser	Use InPrivate Window and delete private data when exiting browser
Disable autofill of passwords and information	In Settings, disable Autofill Passwords, Payment methods, Addresses and more	In the Privacy and Security tab, disable Ask to save login and passwords; Enable Suggest and generate strong passwords;	In Profiles, disable offer to save passwords and save and fill information
Prevent tracking	Enable "Do Not Track" request with your browsing traffic	Set to "Always" send websites a "Do Not Track" signal that you don't want to be tracked	Enable Strict Tracking Prevention
Check password exposure in breaches	Warn you if passwords are exposed in a data breach	Show alerts about passwords for breached websites	Not applicable
Control permissions	Set all to "Ask before accessing"	Set all permissions to "Block" by default Set all to "Ask first"	Set all to "Ask first"

Video conferencing. If available, only use video conferencing platforms contracted by your organization, which should pass its privacy and security standards.

When availing of free platforms, use only an up-to-date version, one that offers adequate privacy & security features, and is properly configured:

6

- Set your meeting 'private' by default. Do not reveal meeting IDs in public domains
- Require meeting participants a password upon joining
- Make sure the meeting host is notified when people join and verifies identity of each
- Carefully control screen sharing & recording
- Keep cameras & microphones turned off, unless when speaking
- Avoid transferring files



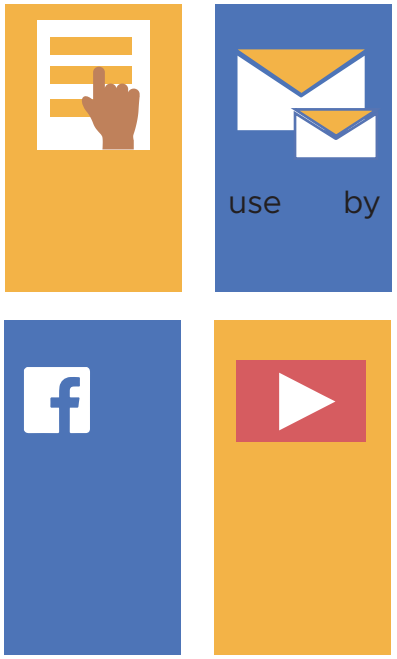
Acceptable Use.

Organizations must have an Acceptable Use Policy (AUP) that defines allowable personal uses of ICT assets. This may include:

Browsing of news and articles

Video streaming

While organization ICT assets should only be used for authorized purposes, the AUP must acknowledge that occasional personal use by employees may occur without adverse effect to the organization's interests.



The AUP should also define unacceptable and unauthorized uses, which may include:

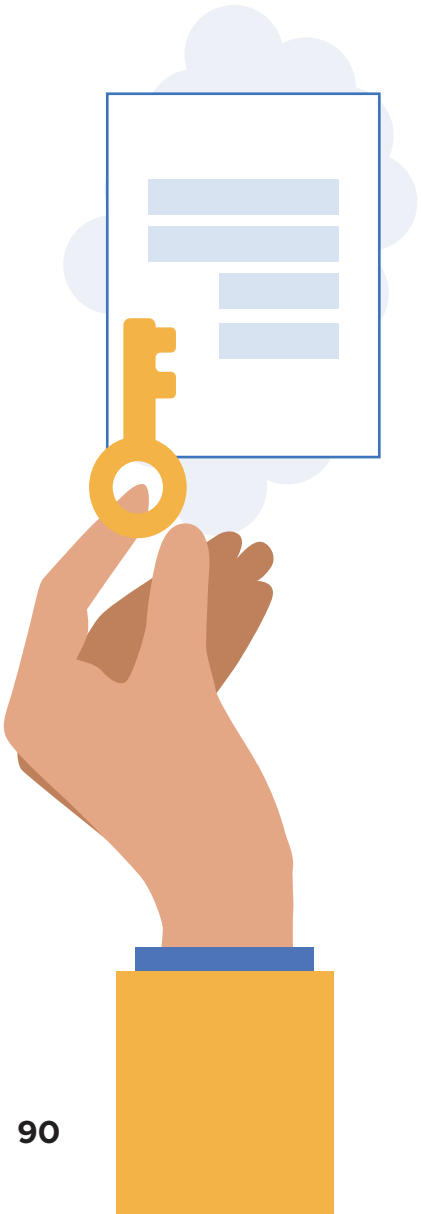
- Uses contrary to laws, customs, mores & ethical behavior
- Uses for personal benefit, entertainment, profit-oriented, partisan, or hostile activities.
- Uses that damage the integrity, reliability, confidentiality and efficiency of ICT resources
- Uses that violate the rights of other users

Access Control. Personnel access to organization data must only be on a "need-to-know-basis", anchored on pre-defined user profiles and controlled via a systems management tool.

User Authentication. Require strong passwords to access personnel credentials and accounts. Passwords must be at least eight (8) characters long, comprising of upper- and lower-case letters, numbers and symbols. Prohibit sharing of passwords. Set up multifactor authentication for all accounts to deny threat actors immediate control of an account with a compromised password.

Network Security. When organization ICT assets are connected to personal hotspots and/or home Wi-Fis, observe the following:

- Don't visit malicious webpages. Always look for the "https" prefix on the URL to ensure it is encrypted. Also, inspect the site's certificate manually to validate owner identity.
- As much as possible, ensure high availability and reliability of internet connection.
- Configure the WiFi Modem or Router. Review and configure the following:
  - Current devices connected;
  - Encryption/ Security: Wi-Fi Protected Access 2 (WPA2) Advanced Encryption Standard (AES) with a strong password.
- Avoid connecting office computers to public networks, such as coffee shop Wi-Fis. If left with no choice, use a reliable Virtual Private Network (VPN) when connecting.



Records and File Security. Set up policies to ensure sensitive data is processed in a protected and confidential manner to prevent unauthorized access, including:

- A records management policy
- A policy against posting sensitive documents in unauthorized channels, such as social media sites
- A policy imposing the use of a file's digital version instead of physical records, whenever possible
- A retention policy for processing sensitive data in personal devices.

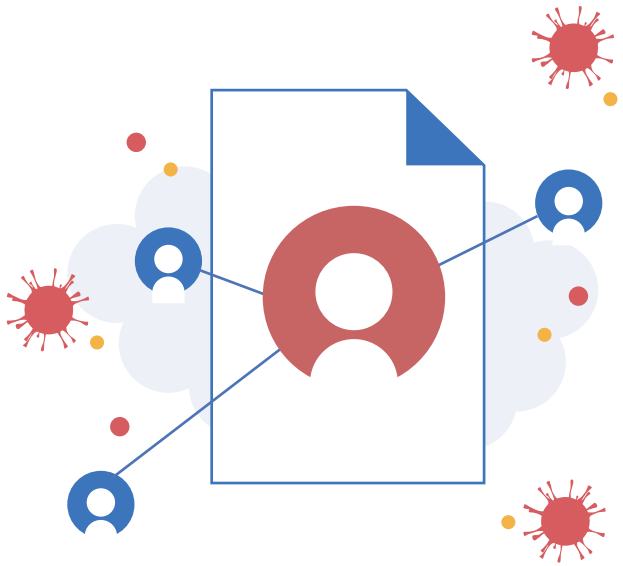
Emails. When transferring sensitive data via email, encryption of files and attachments should be done. Also, ensure that personnel always use the proper "TO, CC and BCC" fields to avoid sending to wrong recipients or needlessly expose other people's email addresses to all recipients.

Physical security. Create workspaces in private areas of the home, or angle work computers in a way that minimizes unauthorized or accidental viewing by others.

- Lock away work devices and physical files in secure storage when not in use. Should there be a need to print documents, the personnel must ensure that physical and digital documents are properly handled and disposed of – in accordance with office policy.
- Never leave physical documents with sensitive data just lying around, nor use them as a "scratch paper".

Security Incident Management. Personnel must immediately notify his or her immediate supervisor in case of a potential or actual personal data breach while working from home. The organization's Data Protection Officer and/ or Data Breach Response Team should immediately be alerted.

For further guidance, please review the NPC Circular on Personal Data Breach Management (https://www.privacy.gov.ph/memorandum-circulars/npc-circular-16-03-personal-data-breach-management/)



NPC PHE Bulletin No. 13

Press Statement of Privacy Commissioner Raymund Enriquez Liboro on the collection of personal data to aid in contact tracing relevant to the COVID-19 response

NPC PHE Bulletin No. 13

Press Statement of Privacy Commissioner Raymund Enriquez Liboro on the collection of personal data to aid in contact tracing relevant to the COVID-19 response

The National Privacy Commission (NPC) recognizes the importance of effective contact tracing and a whole of government approach as a main public health intervention and strategy against COVID-19.

Thus, the Commission is closely coordinating with the Department of Health (DOH) to ensure that its guidelines are consistent with the Data Privacy Act of 2012, the law's implementing rules and regulations and other related NPC issuances.

DOH guidelines of tracing

The DOH released on April 17 Department Memorandum No. 2020 – 0189: Updated Guidelines on Contact Tracing of Close Contacts of Confirmed Coronavirus Disease (COVID-19) Cases.

The memorandum contains provisions on how to properly conduct effective contact tracing while being mindful of data privacy and rights of data subjects. It also establishes the Department of Health through its Epidemiological Bureau as oversight to all contact –tracing activities. (Sec IIIA.1)

Everyone is expected to be guided by this memorandum when collecting personal data. The DOH memorandum also applies to other government agencies.

NPC issuances

The NPC has issued guidelines on the collection, use and disclosure of personal information during the pandemic. Collect what is necessary but disclose only to proper authorities. Likewise, companies and government agencies are mandated to implement appropriate and reasonable security measures always.

Data quality is vital to effective contact tracing. Inaccurate information undermines the over-all aims to trace, misdirect government efforts and put human and other scarce resources to waste.

We believe successful contact tracing can only happen when there's mutual trust between public health authorities and the citizenry. The public must give accurate information for contact tracing to be effective. But for the public to respond, they must rely on authorities to balance the risks to their rights and security and the promised benefits to public health, with the assurance that their data is processed fairly, lawfully, and securely.

Rest assured that the NPC is closely coordinating with concerned agencies on matters concerning data privacy.

NPC PHE
Bulletin No.

14A

Updated Frequently Asked Questions (FAQs)

NPC PHE Bulletin No. 14A

Updated Frequently Asked Questions

We issue the following guidance and response to the updated FAQs raised by stakeholders' concerns on returning-to-work and current work-from-home arrangements.

We expect employers, whether in the government or the private sector, to process personal data responsibly and with accountability in order to address existing health threats brought by COVID-19. We also expect employees to cooperate to reasonable and appropriate collection of their information to mitigate COVID-19 related risks and keep their co-workers and visitors safe. Overall, our guidelines are intended to produce best practices in the workplace that now extend to the homes of employees working remotely.

The National Privacy Commission (NPC) remains steadfast that in this extraordinary time, public health remains our primary concern and that the Data Privacy Act is not a hindrance to beating COVID-19. It is our view that the effective use of personal data is crucial in winning this battle and recovering in its aftermath. And we must remain vigilant in this fight by being mindful of our own health and the health and safety of others.

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ON RETURNING-TO-WORK:

Q **What type/s of personal data can employers collect from employees? Can employers collect health information? How can this be done with the best consideration for privacy?**

A There is legitimate basis for employers to collect additional personal data that includes health information from employees during the pandemic. Employers may collect personal data that are necessary for a specified and legitimate purpose to help control the spread of the virus and keep their workers and visitors safe. Parallel guidelines have been issued by concerned government agencies in this regard: i.e. contact tracing rules of the Department of Health (DOH), guidelines on COVID-19 prevention in the workplace of the Department of Trade and Industry (DTI) and the Department of Labor and Employment (DOLE), or guidelines on alternative work arrangements of the Civil Service Commission (CSC), among others. Employers should refer to these guidelines in coming up with their COVID-19 related policies.

In collecting and processing data from the employees, which shall inevitably include health data, all employers are enjoined to adhere to data privacy principles of: transparency, legitimate purpose and proportionality. Keep collection to the minimum information necessary and use

appropriate means to achieve the purpose. It is essential for employers to be transparent with their employees during this time.

Once collected, reasonable and appropriate safeguards should be in place to ensure the security of the physical or electronic forms used, i.e., health symptoms questionnaires or health status survey forms, under the custody of the employer.

Set a health information policy within the company considering the following, among others: determination of who is authorized to gather the information, who should know the results, how to secure the information, and how to disclose it to authorities when necessary.

Q **How long can employers retain the personal data that they have collected?**

A Employers may retain the personal data from employees as necessary to fulfill the purpose for which these were collected, pursuant to the protocols of the relevant public authorities. After the fulfillment of such purpose/s, personal data shall be disposed in a secure manner that would prevent any unauthorized processing.

Q **In keeping with implementing the minimum health standards, can employers regularly check the temperature of employees returning to work? Can employees refuse to have such temperature checks?**

A Yes. Employers may regularly check the temperature of employees returning to work.

According to the DOH Department Memorandum No. 2020-0220, employees physically reporting to their workplaces shall be screened for COVID-19 symptoms, including fever, cough, colds, and other respiratory symptoms. Daily temperature and symptom monitoring and recording of all staff who will report for work are part of prevention and control measures.

Hence, it is necessary to conduct temperature checks under existing issuances of the various public authorities. Employees should find it reasonable to be screened and must cooperate with their employers to ensure the safety of all returning employees. Employers are expected to use reasonable measures to ensure privacy when doing the collection, like instructing security guards or other personnel to refrain from publicly announcing a person's temperature results and putting in place protocols to implement minimum health standards mindful of the rights and freedoms of data subjects.

Q **Can employers continue checking for travel history and data?**

A Yes. Travel history is now included in usual medical assessments. Employers may collect such data in compliance with the DOH requirements.

Q **Can employers disclose to other parties the health information collected from employees? Can it be used for other purposes? Can they reveal these data to health authorities?**

A Any disclosures of employee health data related to COVID-19 must be limited to the 1) DOH, 2) entities authorized by the DOH, and 3) entities authorized by law, following all existing protocols on the matter. Use of collected employee data shall solely be for the specified and declared purpose/s only.

Q **Can employers retain information collected about employees' temperature checks, results of antibody testing, and/or COVID-19 diagnosis? How long can they retain such information?**

A Yes. Temperature checks, results of antibody testing, and/or COVID-19 diagnosis may be retained as necessary to fulfill the purpose for which these were collected, pursuant to the protocols of the relevant public authorities. Retention requires that appropriate security measures (i.e. organizational, physical, and technical) are implemented in order to prevent unlawful processing or unauthorized access by other employees or third parties.

ON WORK FROM HOME (WFH):

Q **Can employers monitor employees during WFH through the installation of monitoring software in company-issued devices?**

A Yes, employers in exercising their legitimate interest may monitor employees during WFH but should balance it with the rights and freedoms of their employees and adherence to the general data privacy principles. We reiterate the discussions in NPC Advisory Opinion No. 2018-084: monitoring employee activities when he or she is using an office-issued computer may be allowed under the DPA, provided the processing falls under any of the criteria for lawful processing under Sections 12 and/or 13 of the law.

Employers must be transparent to the employees and notify them that they are being monitored. There should be an assessment of the necessity and proportionality of the monitoring (i.e. the method of monitoring) vis-à-vis the objective of the same (i.e. ensuring productivity while under WFH). It is also recommended for the employers to conduct a privacy impact assessment (PIA) of the monitoring software to determine risks and how to mitigate them. Employers should likewise implement clear policies with regard to its monitoring procedures.

Further, less privacy intrusive means of monitoring should be considered rather than excessive and disproportionate mechanism in monitoring such as the use of tracking mouse movements, recording keystrokes, taking random photos of the computer screen, enabling webcams to take a picture of the employee, etc.,

Q **Can employers require employees to stay on video during business hours or even beyond as when they render overtime work, as proof of work done during the day?**

A No. The proportionality principle dictates that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. Employers should avoid extreme privacy intrusive means of managing employees as there are other available means of ensuring that employees are doing their assigned tasks.

Q **How can employers ensure that personal data processing systems being used during WFH are secured?**

A Employers can secure personal data processing systems being used during WFH by providing proper ICT equipment and support facilities and mechanisms to the employees. More importantly, data protection and privacy policies should be in place to guide the staff.

Specifically, for the government, the heads of agencies shall ensure that employees have access to or is provided with communication equipment or facilities (laptop, computer, internet, telephone, mobile phone, etc.) to carry out their functions.

You may refer to our previous bulletin on WFH: NPC PHE Bulletin No. 12 on Protecting Personal Data in a Work From Home Arrangement (https://www.privacy.gov.ph/2020/05/npc-phe-bulletin-no-12-protecting-personal-data-in-a-work-from-home-arrangement/).

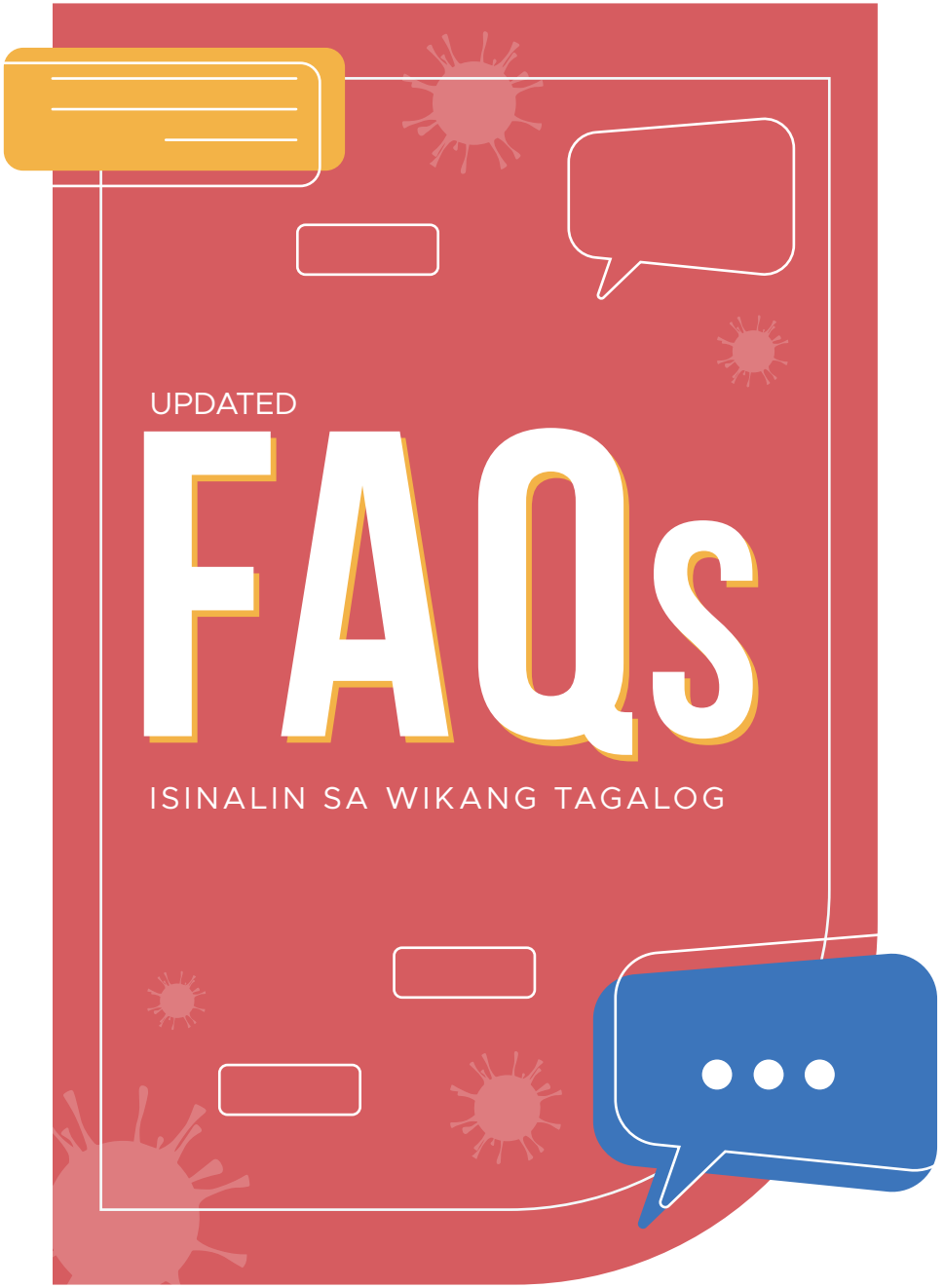
For more information, please refer to the following related issuances:

- National Privacy Commission COVID-19 Bulletins: https://www.privacy.gov.ph/list-of-npc-issuances-related-to-covid-19/
- DOH Memorandum No. 2020-0220 https://www.doh.gov.ph/sites/default/files/health-update/dm2020-0220.pdf
- DOH Department Memorandum No. 2020-0151 https://www.doh.gov.ph/sites/default/files/health-update/dc2020-0174.pdf
- DTI and DOLE Interim Guidelines on Workplace Prevention and Control of COVID-19 https://www.dole.gov.ph/php_assets/uploads/2020/05/DTI_and_DOLE_InterimGuidelinesonWorkplacePreventionandControlofCOVID19_3.pdf
- CSC MC No. 10, s. 2020 http://www.csc.gov.ph/phocadownload/MC2020/MC%20No.%2010,%20s.%202020.pdf
- IATF Omnibus Guidelines on the Implementation of Community Quarantine in the Philippines https://www.officialgazette.gov.ph/downloads/2020/05may/20200515-omnibus-guidelines-on-the-implementation-of-community-quarantine-in-the-philippines.pdf

NPC PHE Bulletin No. 14B

Updated Frequently Asked Questions (FAQs)

ISINALIN SA WIKANG TAGALOG



NPC PHE Bulletin No. 14B

Updated Frequently Asked Questions
Isinalin sa Wikang Tagalog

Inilalabas namin ang *updated FAQs* na ito bilang tugon sa mga isinangguni sa amin ng mga stakeholders ukol sa pag-iingat ng datos sa ilalim ng *return-to-work at work-from-home* na mga *setup* sa pagtatrabaho.

Inaasahan na ang mga employer, nasa gobyerno man o pribadong sektor, ay responsable at may buong pananagutan sa pag-proseso ng personal na datos, upang matugunan ang peligro sa pampublikong kalusugan na dulot ng COVID-19. Gayundin, ang mga empleyado nama'y inaasahang makipagtulungan sa makatwiran at marapat na pangongolekta ng kanilang datos upang maibsan ang pagkalat ng COVID-19 at mapanatiling ligtas ang kanilang mga kasamahan sa trabaho, at mga bisita. Sa pangkalahatan, ang aming *guidelines* ay naglalayon na magtaguyod ng *best practices* sa ating lugar ng trabaho, na sa ngayon ay sakop na rin ang tahanan ng mga empleyadong *work-from-home*.

Ang National Privacy Commission ay patuloy na naninindigan na, sa gitna ng hindi pangkaraniwang panahon na ito, ang kalusugan ng lahat ay prayoridad at ang Data Privacy Act ay hindi balakid sa pagsugpo sa COVID-19. Naniniwala kami na ang epektibong gamit nasa personal na datos ay susi sa tagumpay natin sa digmaan na ito. Kailangan tayong manatiling mapag-matyag sa labang ito, maingat sa sariling kalusugan, pati na rin sa kalusugan at kaligtasan ng lahat.

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

SA PAGBALIK SA TRABAHO:

Q **Anong mga uri ng personal na datos ang pwedeng kunin ng employer sa mga empleyado nito? Maaari bang kumuha sila ng *health information?* Paano ito magagawa na may pagsasa-alang-alang sa *privacy?***

A May lehitimong batayan ang mga employer sa pangongolekta ng karagdagang personal na datos, kabilang ang *health information* ng mga empleyado habang may pandemya. Ang mga employer ay maaaring kumolekta ng personal na datos na kinakailangan para sa itinakda at lehitimong layunin na makatulong kontrolin ang pagkalat ng *virus* at mapanatiling ligtas ang mga manggagawa at bibisita sa tanggapan nila. Kahalintulad na mga gabay ay nailabas na rin ng mga kaagapay na sangay ng gobyerno ukol rito: gaya na lamang ng *contact tracing rules* ng Department of Health, gabay sa pagpapanatiling walang COVID-19 sa mga lugar ng paggawa ng Department of Trade and Industry (DTI) at Department of Labor and Employment (DOLE), maging ang gabay sa alternatibong paraan upang makapagtrabaho ng Civil Service Commission (CSC), ang ilan sa mga ito. Ang mga employer ay nararapat na sumangguni sa mga gabay na ito sa paggawa ng kanilang mga polisiya kontra-COVID-19.

Sa pangongolekta at pagproseso ng *employee data*, kung saan ay kabilang na rin ang *health data,* ang mga employer ay hinihimok na sundin ang *data privacy principles* na: t*ransparency, legitimate purpose*, at *proportionality*. Kolektahin lamang ang nararapat ayon sa kailangan upang makamit ang deklaradong layunin nito. Nararapat lang na ang mga employer ay transparent sa kanilang mga empleyado, lalo na sa panahong ito.

Matapos ang koleksyon, dapat pangalagaan mabuti ng mga employer ang seguridad ng mga datos na nakasaad sa pisikal at digital na mga dokumento gaya ng *electronic forms, questionnaire* sa sintomas at mga *survey form* para sa lagay ng kalusugan ng mga empleyado.

Magtakda ng *health information policy* sa loob ng kumpanya na tumutukoy sa mga sumusunod: pag-alam kung sino ang nararapat magkalap ng impormasyon, sinong makakaalam ng resulta ng *health tests*, papaano pangangalagaan ang impormasyon, at papaano ipagbibigay-alam ito sa mga awtoridad kung kinakailangan.

Q **Gaano katagal maaaring itabi ng mga employer ang nakolektang personal na datos?**

A Maaaring manatili sa pag-iingat ng mga employer ang nakolektang personal na datos ng kanilang mga empleyado hanggang sa panahon na ang layunin sa pagkolekta ay nakamit na, alinsunod na rin sa mga protocols ng mga ahensya ng gobyerno na gagamit sa datos. Matapos makamit ang layunin, ang mga personal datos ay dapat burahin o sirain sa paraan na hindi na muli ito magagamit ng iba, lalo na ng mga di-awtorisado.

Q **Bilang pagpapatupad ng minimum health standards, pwede bang tingnan ng mga employer ang temperatura ng mga empleyado na babalik sa trabaho? Pwede ba tumanggi ang mga empleyado sa ganito?**

A Oo. Pwede tingnan ng mga employer ang temperatura ng nga empleyadong babalik sa trabaho.

Ayon sa DOH Department Memorandum No. 2020-0220, ang mga empleyado na babalik sa lugar ng kanilang trabaho ay susuriin para sa sintomas ng COVID-19, gaya ng lagnat, ubo, sipon, at iba pang sintomas na may kinalaman sa sakit sa baga. Araw-araw na pagtingin sa temperatura at pagkakaroon ng sintomas para sa lahat ng tauhan na papasok sa trabaho ay bahagi ng pag-iwas at pagpigil sa sakit na ito.

Kung kaya, nararapat na matingnan ang temperatura ng mga empleyadong papasok, alinsunod sa nailabas nang mga tagubilin ng iba't ibang sangay ng gobyerno. Ang mga empleyado ay dapat makipagtulungan sa kanilang employer upang masiguro ang kaligtasan ng lahat ng babalik sa trabaho. Ang mga employer naman ay inaasahang gumamit ng mga makatwiran na pamamaraan sa pagkolekta ng datos para masiguro ang data privacy, gaya ng pagtuturo sa mga security guard at iba pang tauhan, na huwag isapubliko ang temperatura ng sinoman, at maglagay na rin ng protocol sa pagpapatupad ng minimum health standards na nagbibigay puwang rin naman ang karapatan at kalayaan ng mga indibidwal.

Q **Maaari bang tingnan ng mga employer ang travel history at datos na kasama nito?**

A Oo. Ang *travel history* ay kasama na sa regular na *medical assessment* ukol sa COVID-19. Ang mga employer ay maaaring kumolekta ng *data* ukol rito alinsunod sa pangangailangan at patakaran ng DOH.

Q **Maaari bang ang mga employer ay magbahagi sa iba ng health information na makokolekta sa mga empleyado? Maaari ba itong gamitin sa ibang layunin? Dapat ba na ipagbigay-alam ang mga impormasyong ito sa mga awtoridad pangkalusugan?**

A Ang *health data* ng mga empleyado ukol sa COVID-19 ay pwede lamang ilahad ng employer sa: 1) DOH, 2) mga opisinang awtorisado ng DOH, at 3) mga opisinang awtorisado ng batas; alinsunod sa mga patakaran ukol sa bagay na ito. Ang paggamit ng nakuhang personal na datos ay pwede lamang gamitin sa mga layunin na dineklara sa mga empleyado.

Q **Pwede bang magtabi ang employer ng kopya ng mga health data na nakalap sa mga empleyado, gaya ng temperatura ng katawan, resulta ng antibody tests, o kaya'y maging ang COVID-19 diagnosis? Gaano katagal naman nila pwede itabi ang mga ito?**

A Oo. Ang mga kopya ng *health data* ng empleyado, gaya ng temperature ng katawan, resulta ng pagsusuri sa antibodies, pati na ang COVID-19 diagnosis, ay maaaring itabi ng employer pansamantala hanggang sa makamit ang layunin sa kanilang koleksyon. Sa panahon na ang mga ito ay nasa pag-iingat ng employer, nararapat na mayroong *security measures* (*organizational, physical,* at *technical*) na ipinatupad ukol dito, upang maiwasan ang di awtorisadong paggamit.

SA NAKA-*WORK FROM HOME* (WFH) SETUP:

Q **Pwede bang i-monitor ng employer ang mga empleyado na gumagamit ng mga *company-issued devices* habang sila ay naka-WFH, sa pamamagitan ng mga monitoring software?**

A Oo, bilang pagtaguyod sa *legitimate interests* ng mga employer, pwede silang magmonitor sa mga empleyado na naka-WFH, subalit sa paraan lamang na balanse, na walang nalalabag na mga karapatan at kalayaan, at alinsunod na rin sa *data privacy principles*.

Iginigiit namin ang mga tinalakay sa NPC Advisory Opinion No. 2018-084: Ang pag-monitor ng mga aktibidad ng empleyado habang gamit niya ang isang computer na pag-aari ng opisina ay pinapayagan sa ilalim ng DPA, datapwat ang pag-momonitor na ito ay sakop ng isa sa mga *criteria* ng *lawful processing* sa ilalim ng Section 12 at/o kaya'y 13 ng batas na ito.

Dapat *transparent* ang mga employer at abisuhan ang kanilang mga empleyado na napapasailalim sila sa *monitoring*. Dapat magkaroon ng pagsusuri kung talaga bang kailangan ang ganitong monitoring, hanggang saan ang sakop nito (paraan ng pag monitor), at kung nakakamit ba ang layunin sa likod nito (halimbawa, para matiyak na produktibo ang

mga empleyado). Ipinapayo rin sa mga employer na mag-*privacy impact assessment* (PIA) sa mga monitoring software na gagamitin para alamin ang peligro sa paggamit nito, at gawan ng paraan na ito'y mapigilan o mabawasan. Dapat magpatupad ang mga employer ng malinaw na mga polisiya na pagbabatayan ng *procedures* sa pag-monitor.

At isa pa, dapat ikonsidera ng mga employer na may mga pamamaraan ng pagmonitor na hindi gaanong nakakapanghimasok sa *privacy* ng mga empleyado, at piliin ang mga ito kaysa sa mga paraan na sobra-sobrang datos na di kailangan ang nakakalap, gaya ng pag-rekord sa galaw ng *mouse* ng *computer*, pagpindot sa *keyboard*, random na pagkuha ng *screenshots*, pag bukas ng *webcam* para makunan ang empleyado, atbp.

Q **Maaari bang i-require ng mga employer na naka-video ang mga empleyado habang nasa oras ng paggawa, o lampas pa rito kung sila ay naka-overtime, bilang katibayan ng trabaho sa araw na iyon?**

A Hindi. Idinidikta ng prinsipyo ng *proportionality* na dapat ang pagproseso ng impormasyon ay sapat, makabuluhan, naaayon sa sitwasyon, kinakailangan, at hindi labis. Ang pagproseso sa personal na datos ay gagawin lamang kung ang layunin ng pagprosesong ito ay 'di makakamit sa ibang paraan.

Dapat umiwas ang employer sa mga paraan ng pamamahala sa empleyado na sukdulang mapanghimasok sa *privacy*, lalo pa't may iba namang paraan upang masiguro na ginagawa nila ang kanilang trabaho.

Q **Paano masisiguro ng mga employer na ligtas gamitin ang *personal data processing systems* habang naka-WFH?**

A Masisiguro ng mga employer na ligtas gamitin ang kanilang *personal data processing systems* habang nagapapatupad ng WFH setup sa pamamagitan ng pagbibigay sa mga empleyado ng tamang *ICT equipment* at karampatang gabay o alalay sa paggamit ng mga ito. Napakahalaga din na ang mga polisiya ng opisina ukol sa proteksyon at privacy ng datos na maayos na ibinabahagi sa mga empleyado.

Partikular sa gobyerno, dapat siguruhin ng mga pinuno ng mga ahensya na ang mga empleyado ay may access o nabigyan ng mga gamit sa komyunikasyon *(laptop, computer, internet, telephone, mobile phone, atbp.)* upang makapagtrabaho nang maayos.

Maaaring sumangguni sa aming naunang bulletin ukol sa WFH: NPC PHE Bulletin No. 12 na tinalakay ang Protecting Personal Data in a Work From Home Arrangement (https://www.privacy.gov.ph/2020/05/npc-phe-bulletin-no-12-protecting-personal-data-in-a-work-from-home-arrangement/).

Para sa karagdagang impormasyon, maaaring tingnan ang mga sumusunod na issuances:

- National Privacy Commission COVID-19 Bulletins: https://www.privacy.gov.ph/list-of-npc-issuances-related-to-covid-19/

- DOH Memorandum No. 2020-0220 https://www.doh.gov.ph/sites/default/files/health-update/dm2020-0220.pdf

- DOH Department Memorandum No. 2020-0151 https://www.doh.gov.ph/sites/default/files/health-update/dc2020-0174.pdf

- DTI and DOLE Interim Guidelines on Workplace Prevention and Control of COVID-19 https://www.dole.gov.ph/php_assets/uploads/2020/05/DTI_and_DOLE_InterimGuidelinesonWorkplacePreventionandControlofCOVID19__3.pdf

- CSC MC No. 10, s. 2020 http://www.csc.gov.ph/phocadownload/MC2020/MC%20No.%2010,%20s.%202020.pdf

- IATF Omnibus Guidelines on the Implementation of Community Quarantine in the Philippines https://www.officialgazette.gov.ph/downloads/2020/05may/20200515-omnibus-guidelines-on-the-implementation-of-community-quarantine-in-the-philippines.pdf

NATIONAL PRIVACY COMMISSION

NPC PHE Bulletin No. 15: Guidelines for Establishments on the Proper Handling of Customer and Visitor Information for Contact Tracing

July 8, 2020 | 3:16 PM GMT+0800 Last Edit: July 8, 2020

Pursuant to DTI Memorandum Circular 20-28, s. 2020 (Guidelines to Follow on Minimum Health Protocols for Barbershops and Salons) and DTI Memorandum Circular 20-37, s. 2020 (Guidelines to Follow on Minimum Health Protocols for Dine-in Restaurants and Fastfood Establishments), establishments are required to implement contact tracing measures as one of the mandatory minimum

NATIONAL PRIVACY COMMISSION

Collect only what is necessary

Establishments should ensure that the processing of personal data is proportional to the purpose of contact tracing. Collect only such information as required under existing government issuances. Establishments may adopt sample health checklist forms issued by government agencies but should not collect beyond what is required and necessary.

Be transparent

Establishments should inform their customers and visitors of the collection of their personal data and the reasons for such collection. This can be done by posting a privacy notice which is readily visible within the establishment's premises, such as points of entry, and other conspicuous areas. If the establishment opts to use electronic means, the notice must be posted in the platform prior to collection.

For further information on the processing activity, establishments may direct their customers and visitors to their official websites or social media pages, as well as official websites of pertinent government agencies to provide them with information on the possible uses of their personal data for contact-tracing purposes.

Establishments must ensure that the privacy notice is easy to access, understandable, and uses clear and plain language.

Use information only for the declared purpose

All establishments should use only the personal data collected through health checklists or other similar forms for the purpose of contact-tracing measures. Repurposing the use of data other than contact tracing and storing data for speculative use is not allowed.

Establishments are responsible for reminding their employees and third-party service providers, such as security personnel, that using the collected personal data of customers or visitors for any other purpose is punishable under the Data Privacy Act of 2012 (DPA).

Implement security measures

or unlawful processing, alteration, disclosure, and destruction.

Keep the data only for a limited period

All personal data collected for the purpose of contact tracing shall be retained only for a period allowed by existing government issuances. After which, all personal data should be disposed of in a secure manner that would prevent further processing and/or unauthorized access or disclosure.

For further information, we may be reached at info@privacy.gov.ph.

# # #

Share this:

Related

Privacy Commission Pushes Restaurants, Barbershops, and Salons to Adopt Data Privacy Measures in Contact Tracing
July 9, 2020
In "Press Releases"

DATA PRIVACY ACT is not a hindrance in contact tracing
August 11, 2020
In "Press Releases"

NPC PHE Bulletin No. 13: Press Statement of Privacy Commissioner Raymund Eriquez Liboro on the collection of personal data to aid in contact tracing relevant to the COVID-19 response
May 21, 2020
Similar post