

# FREQUENTLY ASKED QUESTIONS ON DATA PRIVACY

NPC FAQs



NPC FAQs

## IN THE **HEALTH & HOSPITALS SECTOR**

For Personal Information Controllers & Processors  
and Data Subjects



# TABLE OF CONTENTS

<b>I. WIIFM (What's in it for me?)</b>	<b>4</b>	<b>V. COVID-19-Related Questions</b>	<b>46</b>
What is data privacy?	6	What are the guidelines when conducting contact tracing?	48
Why is data privacy important in the health and hospitals sector?	8	Can I share information about COVID-19 patients?	52
How important is data privacy to our clients?	10	Can I publicly disclose the identities of COVID-19 patients?	54
<b>II. THE DATA PRIVACY ACT &amp; ITS COVERAGE</b>	<b>12</b>	<b>VI. RAISING AWARENESS &amp; CAPACITY-BUILDING</b>	<b>56</b>
What is the Data Privacy Act of 2012?	14	What is the DPO ACE Training Program?	58
Who is the National Privacy Commission?	16	What is the DPO Journal?	60
Am I covered by the DPA?	18	Who is a Sector Policy Adviser?	62
<b>III. DATA SECURITY AND COMPLIANCE</b>	<b>20</b>		
Do I need to appoint a Data Protection Officer (DPO)?	22		
What is a Privacy Notice?	26		
What is a Privacy Impact Assessment?	28		
What is a Privacy Management Program?	30		
What is a Privacy Manual?	32		
<b>IV. DATA PROCESSING GUIDELINES</b>	<b>34</b>		
What is the consent of the data subject?	36		
What are the guidelines in collecting and accessing personal data?	40		
What do I need to keep in mind when storing clients' information?	42		
How may personal data be disposed of?	44		



**I. WHAT'S IN**

**IT FOR ME?**



01

## What is data privacy?

The right of an individual to control the collection of, access to, and use of personal information about him or her that are under the control or custody of the government or the private sector.



02

## Why is data privacy important in the Health and Hospitals Sector?



Healthcare services are largely dependent on the free flow of information among all participants – be it the client, the healthcare worker or the health institution.

When clients feel confident that their information are safe and secured at the hands of their healthcare provider, it encourages them to provide complete and accurate data.

A health institution that prioritizes data privacy is an institution that cares for its clients.



03

## How important is data privacy to our clients?



As a healthcare provider, most of the data you process are considered sensitive personal information. Data privacy measures ensure your client that these information are safe and secured. It guarantees them that their data are protected at all times and are not exposed to risks and vulnerabilities like unauthorized access, processing, sharing and disclosure.

**II. DATA**

**PRIVACY ACT &**

**ITS COVERAGE**



04

## What is the Data Privacy Act of 2012?



Republic Act No. 10173 is also known as the Data Privacy Act of 2012 (DPA).

It (1) protects the privacy of individuals while ensuring free flow of information to promote innovation and growth; (2) regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data; and (3) ensures that the Philippines complies with international standards set for data protection through National Privacy Commission.





05

## Who is the National Privacy Commission?

The National Privacy Commission (NPC) is the country's privacy watchdog; an independent body mandated to administer and implement the DPA, and to monitor and ensure compliance of the country with international standards set for data protection.



06

## Am I covered by the DPA?



The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph: Provided, That the requirements of Section 5 are complied with.

**III. DATA**

**PRIVACY & ITS**

**COMPLIANCE**



07

## Do I need to appoint a Data Protection Officer (DPO)?



Appointing a Data Protection Officer (DPO) is a legal requirement for personal information controllers (PICs) and personal information processors (PIPs), under the Data Privacy Act of 2012.

You should assign a DPO if you are a natural or juridical person or any other body in the government or private sector engaged in the processing of personal data of individuals living within and outside the Philippines. An individual PIC or PIP shall be a de facto DPO.

It must be remembered, however, that mere appointment of a DPO is not sufficient compliance to the law. Instead, it must be coupled with the DPO's registration at the NPC.

Note that **Appendix 1 of NPC Circular 17-01** provides that PICs or PIPs that are involved in the processing of personal data that are likely to pose a risk to the rights and freedoms of data subjects and/or those whose processing are not occasional are subject to mandatory registration of their DPOs and data processing systems.



07

## Do I need to appoint a Data Protection Officer (DPO)?

In the healthcare industry, among such PICs or PIPs are the following: **hospitals including primary care facilities, multi-specialty clinics, custodial care facilities, diagnostic or therapeutic facilities, specialized out-patient facilities, and other organizations processing genetic data.**

Meanwhile, **individual health professionals**, acting as an individual PIC, should register as the de facto DPO only if they process sensitive personal information of at least 1000 individuals.

### **Voluntary appointment and registration of a DPO**

is also an option for health providers as doing so could give you a lot of benefits. In this information age, where personal data serve as building blocks of



any organization, assigning a focal person to ensure the protection of your personal data collection and processing is a must. A DPO increases your chance to remain competitive in the dynamic global landscape of data protection. At the same time, it improves your customer service and enhances your responsiveness to growing public awareness and regard for personal data protection.

For more details about the appointment and registration of a DPO, you can refer to NPC Advisory 2017-01: <https://www.privacy.gov.ph/advisories/npc-advisory-no-2017-01-designation-data-protection-officers/>



08

## What is a Privacy Notice?

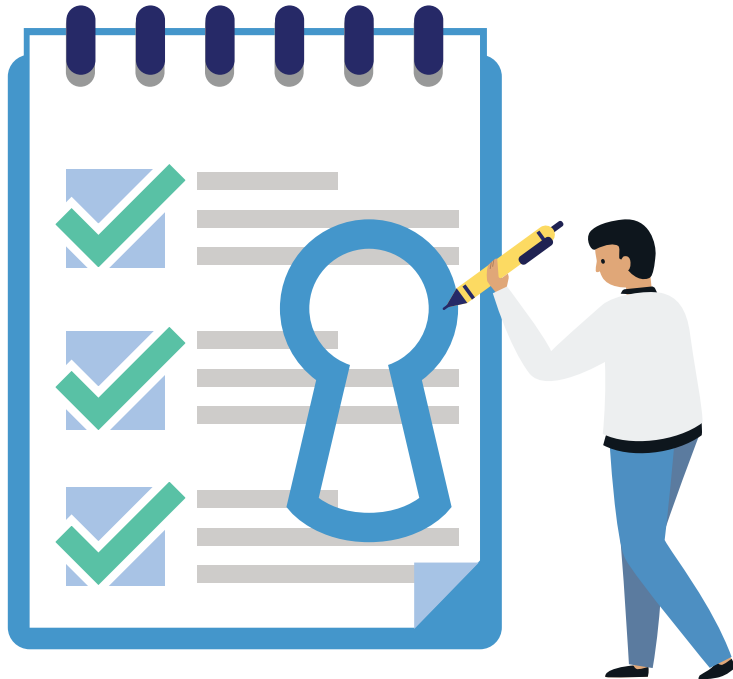


A privacy notice is a statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information. It is sometimes referred to as a privacy statement, a fair processing statement, or privacy policy.

As a privacy notice aims to inform the public, it must be easy-to-read, transparent and compelling.

A Privacy Notice is different from Consent. Health providers must understand that availability and accessibility of a privacy notice is not equivalent to obtaining consent of a data subject. A privacy notice is only meant to inform data subjects of the intended collection and processing by an entity. Meanwhile, a privacy consent is an indication of will, whereby the data subject agrees to the processing of his or her information.

For tips in crafting your privacy notice, you can follow this link: <https://www.privacy.gov.ph/implementing-privacy-and-data-protection-measures/day-to-day/#1>



09

## What is a Privacy Impact Assessment?

Privacy Impact Assessment (PIA) is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a PIC or PIP. It takes into account the nature of the personal data to be protected, the personal data flow, the risks to privacy and security posed by the processing, current data privacy best practices, the cost of security implementation, and, where applicable, the size of the organization, its resources, and the complexity of its operations.

PIA helps a PIC or PIP navigate the process of understanding the personal data flows in the organization. It identifies and provides an assessment of various privacy risks, and proposes measures intended to address them.

For guidelines in the conduct of privacy impact assessments, you can refer to NPC Advisory No. 2017-03: [https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/NPC\\_AdvisoryNo.2017-03.pdf](https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/NPC_AdvisoryNo.2017-03.pdf)



10

## What is a Privacy Management Program?



Privacy Management Program (PMP) refers to a process intended to embed privacy and data protection in the strategic framework and daily operations of a PIC or PIP, maintained through organizational commitment and oversight of coordinated projects and activities.

The PMP puts everyone on the same page. It provides an easier way to explain to the management and staff: why are we doing this, what are the results we expect, what are the benefits of those results, and what do we need to do to get there. With this, you will smoothly get everyone on board.

For more information on how to develop your organization's PMP and other compliance requirements of the DPA, you can download a copy of NPC's Privacy Toolkit at <https://privacy.gov.ph>.





11

## What is a Privacy Manual?

A PIC or PIP is instructed to implement reasonable and appropriate measures to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

To inform its personnel of such measures, each PIC or PIP is expected to produce a Privacy Manual. The Manual serves as a guide or handbook for ensuring the compliance of an organization or entity with the DPA, its Implementing Rules and Regulations (IRR), and other relevant issuances of the National Privacy Commission (NPC). It also encapsulates the privacy and data protection protocols that need to be observed and carried out within the organization for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects.

For guidelines in creating a privacy manual, you can follow this link: <https://www.privacy.gov.ph/creating-a-privacy-manual/#0>



**IV. DATA**

**PROCESSING**

**GUIDELINES**



12

## What is the consent of the data subject?



Under the DPA, the consent of the data subject is defined as any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Note that consent is just one of many other lawful criteria for processing of personal information (Section 12, DPA) and sensitive personal information (Section 13, DPA). When processing information, PICs should determine whether consent is the most appropriate basis for such.

Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.



12

## What is the consent of the data subject?

To protect privacy, the law requires organizations to notify and furnish their data subjects with the following information before they enter personal data into any processing system, or at the next practical opportunity:

1. Description of the personal data to be entered into the system
2. Purposes for which data will be processed (e.g. direct marketing, statistical, scientific etc.)
3. Basis for processing, especially when it is not based on consent (e.g. public health and safety, mandatory reporting of illness, disease surveillance)
4. Scope and method of the personal data processing



5. Recipients to whom data may be disclosed
6. Methods used for automated access by the recipient and the extent to which such access is authorized
7. Identity and contact details of the PIC or its representative
8. The duration for which data will be stored
9. Existence of the rights of the data subjects



13

## What are the guidelines in collecting and accessing personal data?



As consistently urged by the Commission, health providers and those involved in the delivery of health care services must collect only necessary personal details. Recipients must not be burdened 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.

In relation, access to health data must be given only on a “need-to-know” basis which means only those who are in the health team must have minimum and necessary access to enable the performance of their functions.



14

## What do I need to keep in mind when storing clients' information?

The DPA and its IRR provides that personal data shall not be retained longer than necessary:

1. for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
2. for the establishment, exercise or defense of legal claims; or
3. for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.

Likewise, retention of personal data shall be allowed in cases provided by law.

For members of the Health and Hospitals Sector, reference may be made to DOH Memorandum Circular No. 70, series of 1996 for the Revised Disposition Schedule of Medical Records.

In addition, a PIC must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.



15

## How may personal data be disposed of?



Under the IRR, personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects. The DPA penalizes improper disposal of personal information and sensitive personal information.

**V. COVID-19**

**RELATED**

**QUESTIONS**





16

## What are the guidelines when conducting contact tracing?

On 17 April 2020, DOH released Department Memorandum No. 2020 – 0189, or the Updated Guidelines on Contact Tracing of Close Contacts of Confirmed Coronavirus Disease (COVID-19) Cases, which contains provisions on how to properly conduct effective contact tracing while being mindful of data privacy and rights of data subjects.

In line with this, the Commission, through NPC PHE Bulletin No. 13, emphasized that successful contact tracing can only happen when there is 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.



16

## What are the guidelines when conducting contact tracing?

Further, organizations must ensure that processing systems and applications used in the implementation of contact tracing must be designed with data privacy in mind. Functions meant to protect the rights of data subjects must be integral to the system and should not be made as a mere feature. This is called privacy-by-design. And this is also why digital contact tracing systems or applications should undergo thorough Privacy Impact Assessment (PIA) so that risks and vulnerabilities may be identified and resolved at the earliest time possible.



17

## Can I share information about COVID-19 patients?



Following the declaration of health emergency in the country, NPC issued PHE Bulletin No. 6 stating that sharing and disclosure of data related to COVID-19 patients must only be done to the proper authority.

And while there are laws that allow for the sharing of information about COVID-19 patients from one institution to another, PICs must ensure that such is kept to a minimum extent keeping in mind the three general data privacy principles: transparency, legitimate purpose, and proportionality.

It must be noted as well that in instances when a Data Sharing Agreement (DSA) is not mandated by law, PICs and PIPs may still opt to execute it if they have to detail the terms and conditions of the data sharing or to outline security measures.



18

## Can I publicly disclose the identities of COVID-19 patients?



Contact tracing does not require public disclosure of identities of COVID-19 patients. Unbridled disclosure of patients' personal data to the public has been proven to cause actual harm such as physical assault, harassment, and discrimination.

The DPA has never been a hindrance to contact tracing. It does not prevent the processing of personal data when necessary to fulfill their mandates.

**VI. RAISING**

**AWARENESS &**

**CAPACITY-**

**BUILDING**



19

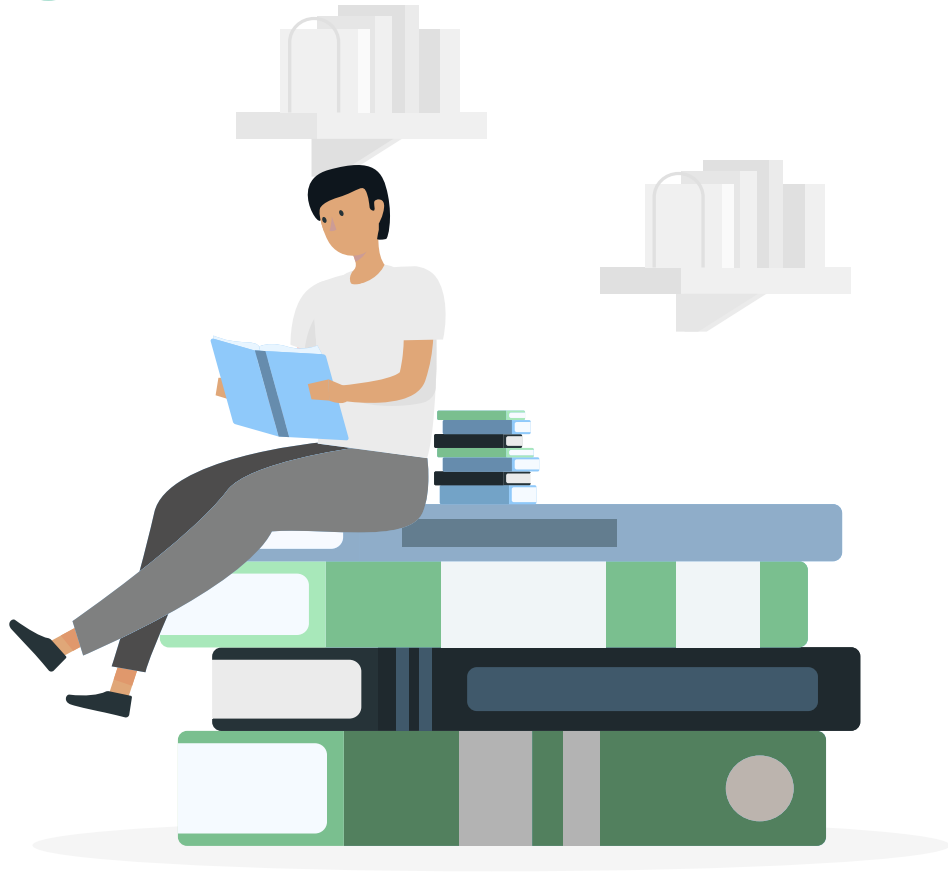
## What is the DPO ACE Training Program?



In 2018, The National Privacy Commission (NPC) launched its DPO Accountability, Compliance, and Ethics (ACE) Program, aimed at establishing a skills benchmark for local privacy professionals, amid the spike in demand for high-quality data privacy trainings in the country.

The DPO ACE Program has three levels and comprises advanced case studies, practical, and written exams. Those who successfully passed will be issued a certificate reflecting their DPO skills level.

At present, this training program is already available publicly. For updates on the schedule, you can send an email to [dpo.ace@privacy.gov.ph](mailto:dpo.ace@privacy.gov.ph).



20

## What is the DPO Journal?



The DPO Journal is the official monthly newsletter of the NPC.

In this publication, you can read various articles on data privacy-related issues. It also contains write-ups which are of interest to the Health and Hospitals Sector.

Get updated with the latest volume of the DPO Journal using this link: <https://dpojournal.privacy.gov.ph/>



21

## Who is a Sector Policy Adviser?



The NPC adapted a sectoral approach which allows for a wider reach and faster implementation of all its projects and programs. Each sector has been assigned a Policy Adviser who acts as the liaison between the Commission and its stakeholders. At present, we have identified more or less 22 sectors which include:

1. Government, including NGAs, GOCCs and LGUs
2. Banks
3. Telecommunications and Internet Service Providers
4. Education
5. Business Process Outsourcing
6. Social Media
- 7. Health and Hospitals**
8. Retail and Direct Marketing
9. Life Insurance
10. Non-Life Insurance and PADPAO
11. Pharmaceutical
12. Utilities
13. Non-Bank Financial Institutions
14. Hotels
15. Manning
16. Transportation and Logistics
17. Real Estate
18. Tourism
19. Health Maintenance Organization
20. Information Society Service

To know more about the Policy Adviser for the Health and Hospitals Sector, you can go to

<https://www.privacy.gov.ph/policy-advisors/>






Para sa dagdag na kaalaman, makipag-ugnayan sa  
**National Privacy Commission (NPC).**

 [info@privacy.gov.ph](mailto:info@privacy.gov.ph)

 [privacy.gov.ph](http://privacy.gov.ph)

 8234 2228