

Data Privacy Act of 2012

ROREN MARIE M. CHIN

CHIEF, PUBLIC INFORMATION AND ASSISTANCE DIVISION

NATIONAL PRIVACY COMMISSION

FOR REFERENCE



PRIVACY

**“The right to be let alone -
the most comprehensive of
rights and the right most
valued by civilized men”**

[Brandeis J, dissenting in *Olmstead v. United States*,
277 U.S. 438 (1928)].

What is

DATA PRIVACY ACT?

FOR REFERENCE

What is Data Privacy Act (DPA)?

**A law protecting
INDIVIDUAL PERSONAL
DATA**

FOR REFERENCE

Data Privacy Act

It is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth.

FOR REFERENCE
National Privacy Commission

Defining the terms

REFERENCE
ROREN MARIE M. CHIN

©

What is PERSONAL INFORMATION?

- Any information from which the identity of an individual is apparent
- Any information that can be put together with other information to reasonably and directly identify an individual
- Includes sensitive personal information such as your health, education, genetic or sexual life
- Includes information that is classified or privileged

Processing

Any operation or set of operation performed upon personal information.

FOR REFERENCE

**To whom this law
applies...**



DATA SUBJECT

**whose personal information is
processed**

FOR REFERENCE



PERSONAL INFORMATION CONTROLLER - person or organization who controls the processing and use of personal information



PERSONAL INFORMATION PROCESSOR - may outsource the processing of personal data pertaining to a data subject

FOR REFERENCE

What are the responsibilities of the PICs and PIPs?

FOR REFERENCE

①

T

L

P

②

**Security
Measures**

③

**Rights of
the Data
Subject**

FOR REFERENCE

T

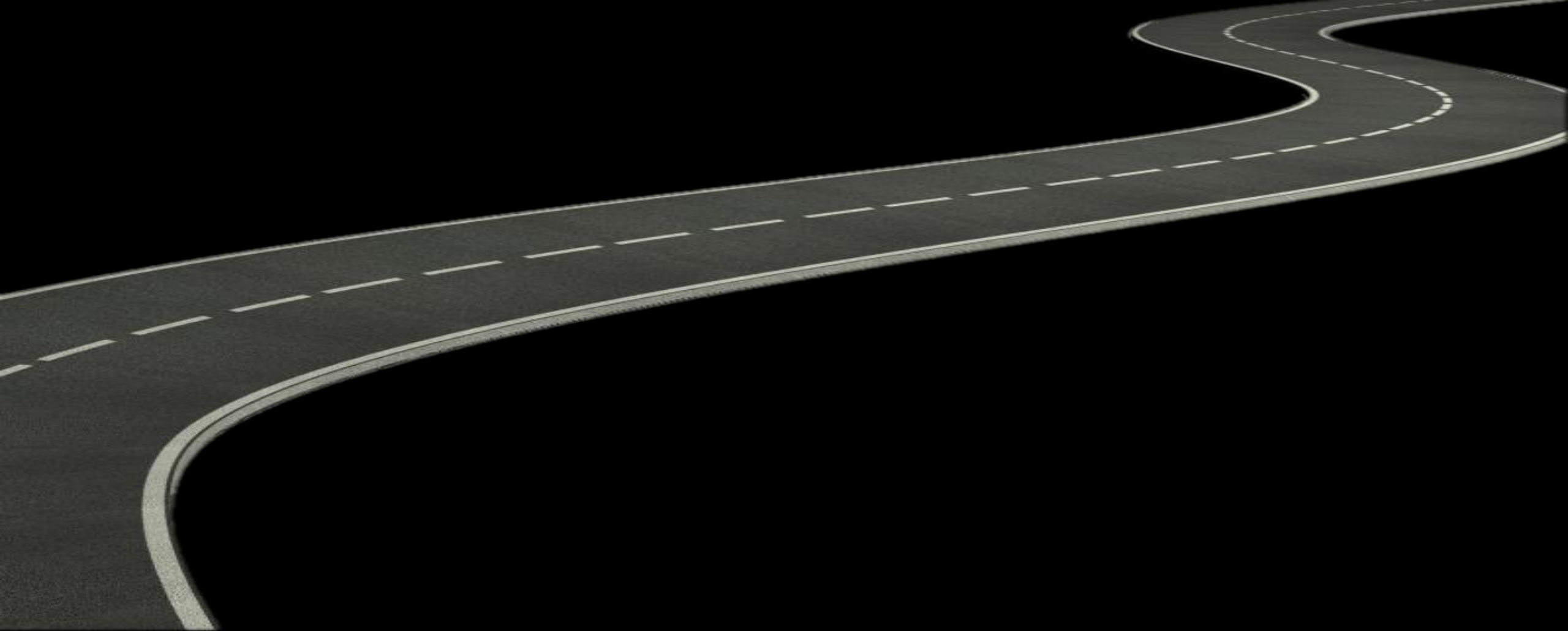
L

P

**Security
Measures**

**Rights of
the Data
Subject**

FOR REFERENCE



GENERAL DATA PRIVACY PRINCIPLES

General Data Privacy Principles

TRANSPARENCY



**LEGITIMATE
PURPOSE**



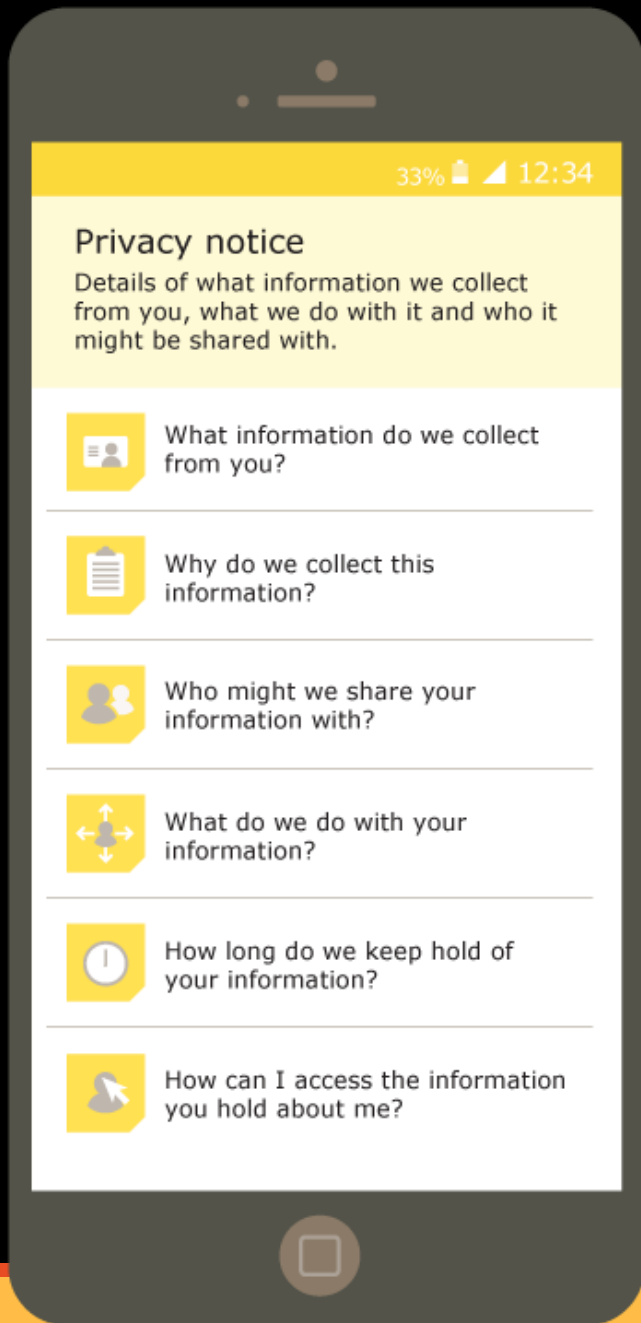
PROPORTIONALITY



Transparency

The data subject must be aware of the nature purpose, and extent of the processing of his or her personal data.

FOR REFERENCE



A **PRIVACY NOTICE** tells you what happens to your personal data.

- who is **collecting** your information
- what it is going to be **used** for
- whether it will be **shared** to other organization

Legitimate purpose

The processing of information shall be compatible with a declared and specified purpose.

Section 12 & 13 Criteria for Lawful Processing



FOR REFERENCE

How about for other purposes, such as...

- marketing
- medical mission
- profiling
- training and compliance to requirement of board exams
- case presentation
- research for public benefit
- and others...



Proportionality

The processing of information shall be adequate, relevant, suitable, necessary, and not excessive.

T

L

P

**Security
Measures**

**Rights of
the Data
Subject**

FOR REFERENCE



IMPLEMENTATION OF SECURITY MEASURES

FOR REFERENCE



organizational



technical



physical

FOR REFERENCE

Organizational Security



Data Protection Officer

Privacy Impact Assessment



FOR REFERENCE



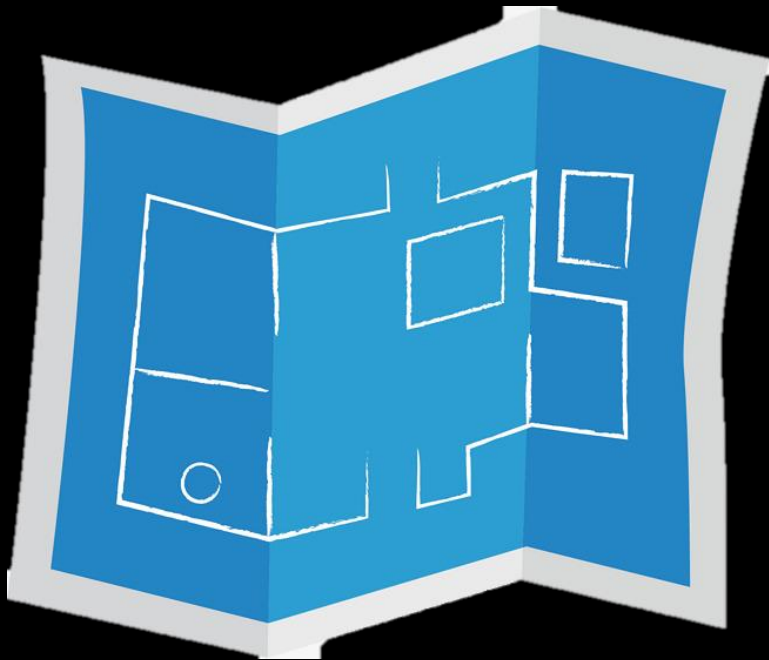
Training and Capacity building

Technical Security



FOR REFERENCE

Physical Security



Design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public

TYPES OF BREACHES

FOR REFERENCE



Confidentiality Breach

**Due to the unauthorized disclosure
of or access to personal data**

FOR REFERENCE

Integrity

Due to alteration of personal data

FOR REFERENCE

A **availability**

**Due to loss, accidental, or unlawful
destruction of personal information**

FOR REFERENCE

Rights of the Data Subject

1. Right to Information
2. Right to Object
3. Right to Access
4. Right to Correct
5. Right to Erase
6. Right to Damages
7. Right to File a Complaint



FOR REFERENCE

Penalties

FOR REFERENCE

RA 10173	if you do	Personal Information		Sensitive Personal Information	
Section	this...	Imprisonment	Fine	Imprisonment	Fine
25	Processed info without authorization (e.g. a doctor accesses a patient record that he's not authorized to view)	one (1) to three (3) years	500,000 to 2,000,000 pesos	three (3) to six (6) years	500,000 to 4,000,000 pesos
26	Provided access to info due to negligence (e.g. the hospital does not have a security measure in place to prevent hacking.)	one (1) to three (3) years	500,000 to 2,000,000 pesos	three (3) to six (6) years	500,000 to 4,000,000 pesos

FOR REFERENCE

RA 10173	if you do	Personal Information		Sensitive Personal Information	
Section	this...	Imprisonment	Fine	Imprisonment	Fine
27	Improper disposal of info (e.g. failing to shred paper records, or failing to ensure that a cloud provider has completely wiped all data)	six (6) months to two (2) years	100,000 to 500,000 pesos	one (1) to three (3) years	100,000 to 1,000,000 pesos
28	Processing of info for unauthorized purposes (e.g. doctor is authorized to use patient data for treatment, but also used it for clinical research)	eighteen (18) months to five (5) years	500,000 to 1,000,000 pesos	two (2) to seven (7) years	500,000 to 2,000,000 pesos

FOR REFERENCE

RA 10173	if you do	Personal Information		Sensitive Personal Information	
Section	this...	Imprisonment	Fine	Imprisonment	Fine
29	Intentional breach of info (e.g. viewing a record using a password stolen from someone else)	one (1) to three (3) years	500,000 to 2,000,000 pesos	one (1) to three (3) years	500,000 to 2,000,000 pesos
30	Concealing security breach (e.g. not informing patients that their sensitive information was exposed/hacked)			eighteen (18) months to five (5) years	500,000 to 1,000,000 pesos

FOR REFERENCE

RA 10173	if you do	Personal Information		Sensitive Personal Information	
Section	this...	Imprisonment	Fine	Imprisonment	Fine
31	Malicious disclosure (e.g. a treatment record is leaked to the press)	eighteen (18) months to five (5) years	500,000 to 1,000,000 pesos	eighteen (18) months to five (5) years	500,000 to 1,000,000 pesos
32	Unauthorized disclosure (other disclosures not covered by "malice", e.g. posting to social media about a patient's case)	one (1) to three (3) years	500,000 to 1,000,000 pesos	three (3) to five (5) years	500,000 to 2,000,000 pesos
33	Combination of series of acts from all of the above	three (3) years to six (6) years	1,000,000 to 5,000,000 pesos	three (3) years to six (6) years	1,000,000 to 5,000,000 pesos

FOR REFERENCE

Thank you!

Visit us at:

<https://privacy.gov.ph/>

Like us at:

<https://www.facebook.com/IvyDPatdu>

<https://www.facebook.com/privacy.gov.ph/>

For more information you may contact us at:

info@privacy.gov.ph

roren.chin@privacy.gov.ph