Understanding Data Privacy Act in the Context of Health Research

ROREN MARIE M. CHIN

Development Management Officer IV

Privacy Policy Office, NPC

RIGHT TO PRIVACY

"The right to be let alone - the most comprehensive of rights & the right most valued by civilized men"

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

RORENMARIE M. CHIN, National Privacy Commission

CONFIDENTIALITY

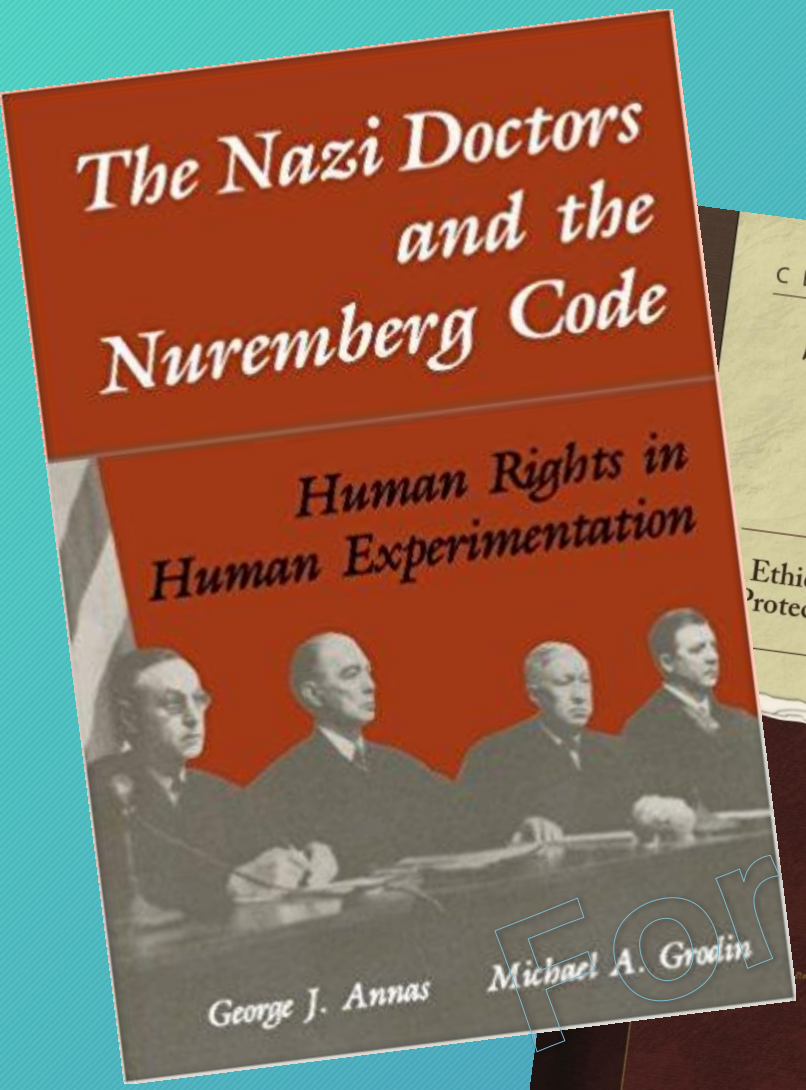
"The obligations of those who receive information in the context of an intimate relationship to respect the privacy interests of those to whom the data relate and to safeguard that information"

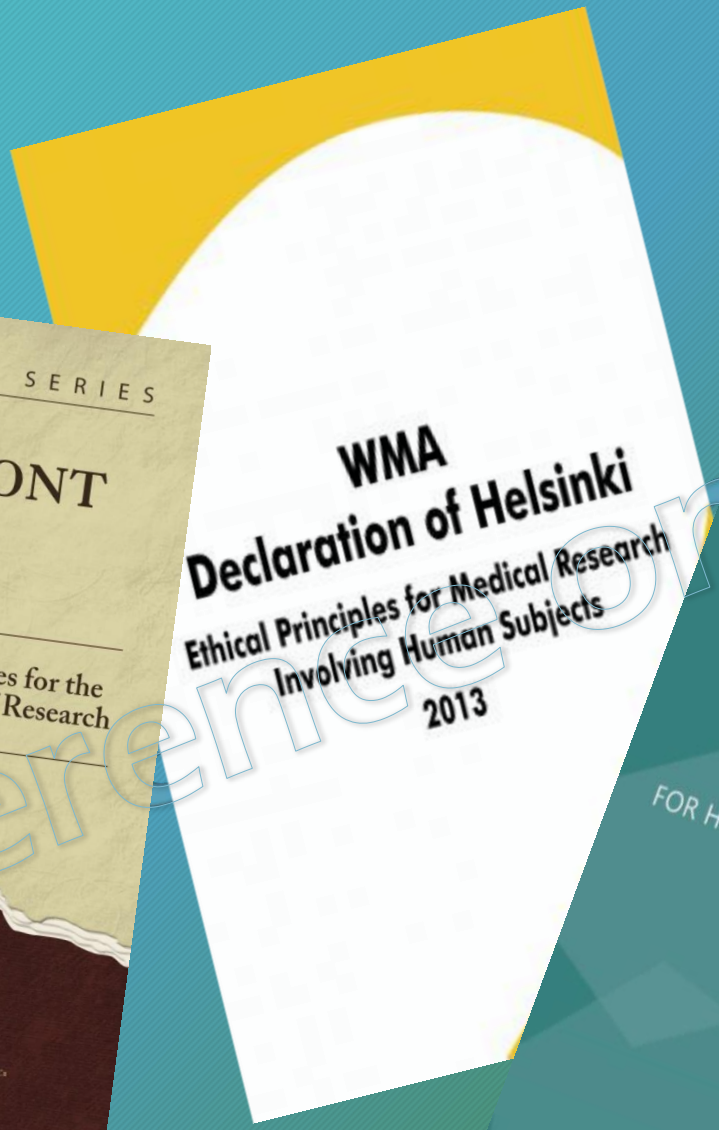
Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research http://www.nap.edu/catalog/12458.html

SECURITY

"The procedural and technical measures required to (a) prevent unauthorized access, modification, use, and dissemination of data stored or processed in a computer system, (b) prevent any deliberate denial of service, and (c) to protect the system in its entirety from physical harm."

Turn, R., and W. H. Ware. 1976. Privacy and security issues in information systems. *The Rand Paper Series.* Santa Monica, CA: The Rand Corporation.





CULTURE

Researchers intentionally leak details of 70,000 OkCupid profiles

BY MEREDITH PLACKO 05.16.2016 :: 1:44PM EDT MPLACKO

Users of OkCupid waived their rights away to their personal statistics such as their age, sexual preferences, and religious beliefs when they signed up for the website, but that information belongs to Match, the parents company of OkCupid. It's Match — and only Match — that can decide who sells that data, and to whom. Kirkegaard and his fellows publishing it online violated the privacy of the service's users.

https://www.geek.com/culture/okcupid-data-leak-releases-70000-profiles-1655161/

nhs it, records and data

04.07.18

Major NHS breach means 150,000 patients had confidential data used without consent

Just one month after the roll-out of GDPR, it has been revealed that a staggering 150,000 patients have been affected by an NHS data breach where confidential information only requested to be used to provide them with care was also exploited for clinical research purposes without their consent or knowledge.

The mistake is said to have been linked to a coding error in the software used by GPs to record objections to patient data being used for research purposes, which meant the application never passed on the request to NHS England's IT provider.

Source: http://www.nationalhealthexecutive.com/Health-Care-News/major-nhs-breach-means-150000-patients-had-confidential-data-used-without-consent

What is DATA PRIVACY ACT?

RORENMARIE M. CHIN, National Privacy Commission

What is Data Privacy Act (DPA)?

A law protecting INDIVIDUAL PERSONAL DATA

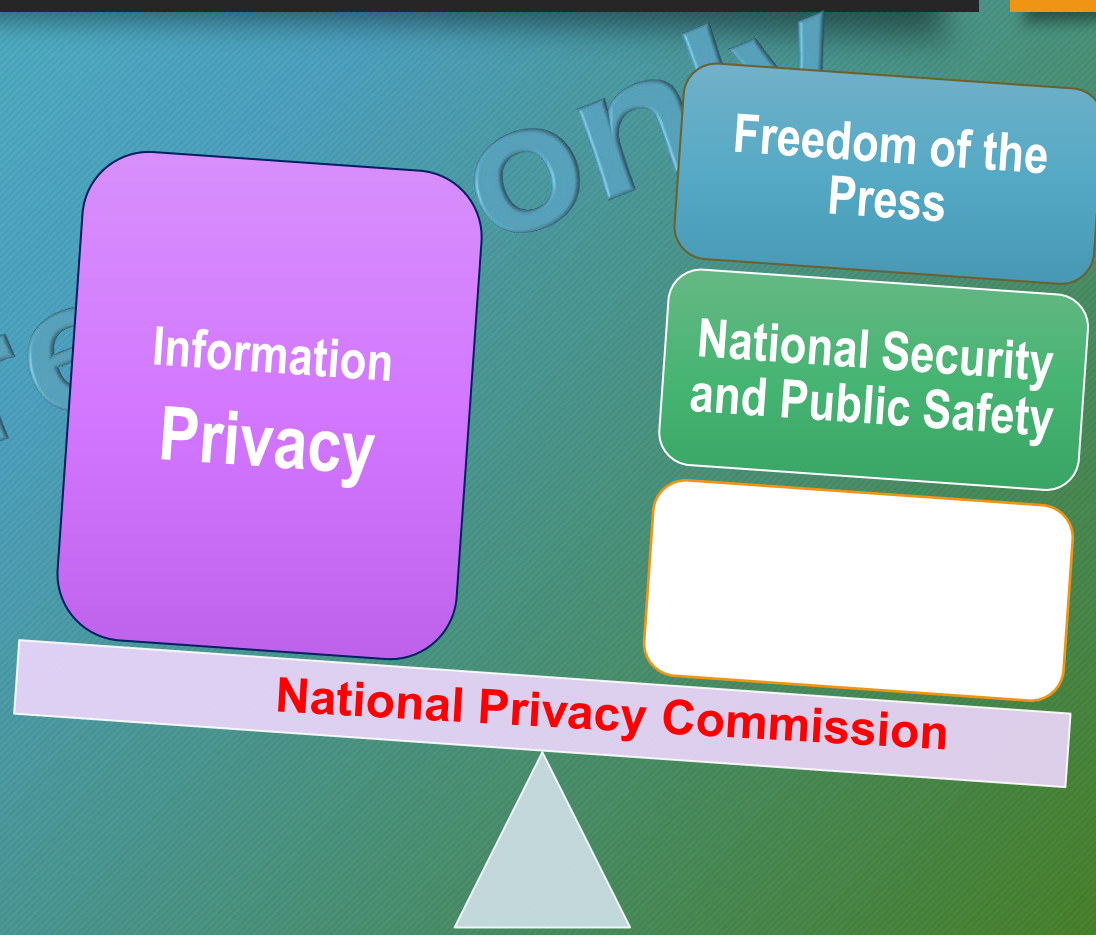
RORENMARIE M. CHIN, National Privacy Commission

Data Privacy Act

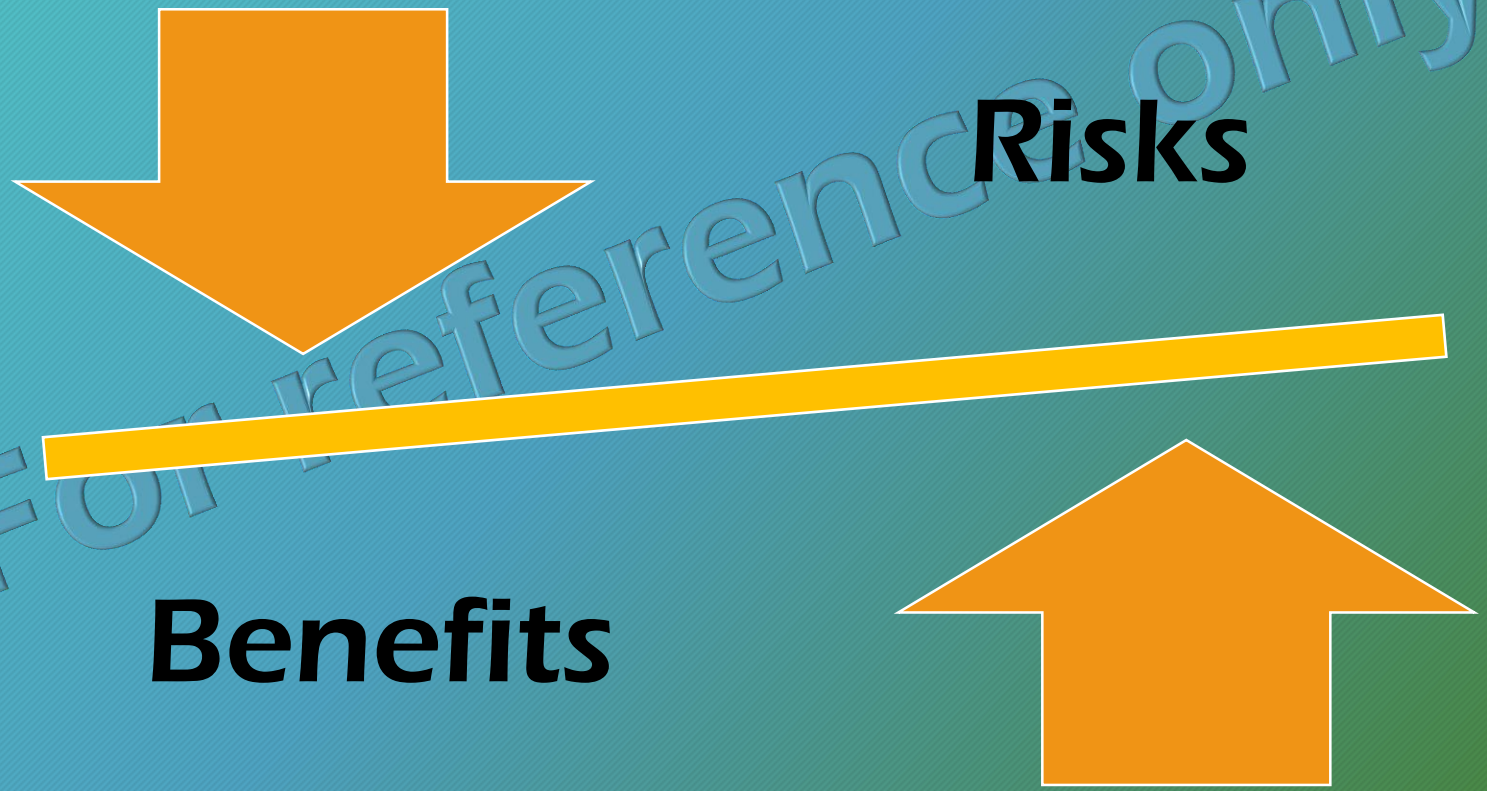
Data Privacy

Free Flow

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.



Research



RORENMARIE M. CHIN, National Privacy Commission

Scope of the Data Privacy Act

Processing of personal data

RORENMARIE M. CHIN, National Privacy Commission

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

What is PROCESSING?

to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data

Special cases under the Data Privacy Act and its IRR

RORENMARIE M. CHIN, National Privacy Commission

Research

RESEARCH shall refer to the development of knowledge with the aim of understanding health challenges and mounting an improved response to them.

This covers the full spectrum of research in five (5) generic areas of activity:

1) measuring the problem;
2) understanding its cause(s);
3) elaborating solutions;
4) translating the solutions or evidence into policy, practice and products; and
5) evaluating the effectiveness of solutions. (Philippine National Health Research System Act of 2013, Sec. 3h)

Special cases [IRR, Sec. 5(c)]

The Act and these Rules shall not apply to the following specified information, only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned:

- Personal information that will be **processed for research purpose** intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards [IRR, Sec. 5(c)]

Data Privacy Act is NOT APPLICABLE

From the slides of Atty. IVY D. Patdu, MD

When the identity of the individual

1. Is not apparent; or
2. Can not be reasonably and directly ascertained by the entity holding the information or when put together with other information, still would not directly and certainly identify an individual.

- *If personal data can be anonymized, then data is not covered by the Data Privacy Act. Aggregate data also not covered.*

The HIPAA Safe Harbor Method

RORENMARIE M. CHIN, National Privacy Commission

18 Key identifiers

- Name
- All geographic subdivisions smaller than a state, including street address, city
- All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

18 Key identifiers

- Telephone numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Fax numbers
- Device identifiers and serial numbers

18 Key identifiers

- Email addresses
- Web Universal Resource Locators (URLs)
- Social security numbers
- Internet Protocol (IP) addresses

18 Key identifiers

- Medical record numbers
- Biometric identifiers, including finger and voice prints
- Health plan beneficiary number
- Full-face photographs and any comparable images

18 Key identifiers

- Account numbers
- Any other unique identifying number, characteristic, or code
- Certificate/license numbers

Source: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

Obligations of the Researcher under the Data Privacy Act

RORENMARIE M. CHIN, National Privacy Commission

The Researcher shall

- Adhere to the Data Privacy Principles
- Implement Security Measures
- Uphold the Rights of the Data Subjects

ROREN MARIE M. CHIN, National Privacy Commission

GENERAL DATA PRIVACY PRINCIPLES

RORENMARIE M. CHIN, National Privacy Commission

General Data Privacy Principles

TRANSPARENCY

LEGITIMATE PURPOSE

PROPORTIONALITY

General Data Privacy Principles

Transparency –

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

General Data Privacy Principles

Legitimate purpose –

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

Section 12 & 13
Criteria for Lawful Processing

RORENMARIE M. CHIN, National Privacy Commission

Consent

From the slides of Atty. IVY D. Patdu, MD

Any freely given, specific, informed indication of will.

CONSENT FORMS

- Waiver of all rights under the Data Privacy Act
- Bundle Consent
- Opt-out

Consent

If data subject is incapable…

If data subject is minor….

Consent may be waived

- Subject to legal and ethical grounds
- Must be approved by an REB/IRB

General Data Privacy Principles

Proportionality –

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

Patient Chart Form

Please print in block capital letters.
*required field

⬡ New Patient ⬡ Flawless Transferee
Branch: _____

*Name: _____ *Sex: _____ Civil Status: _____
(Last) (First) (Middle)

Referred by: _____ Citizenship/Nationality: _____

*Birthday: ⬡⬡/⬡⬡/⬡⬡ *Age: _____ Occupation: _____

Height (ft/in): _____ Weight (lb/kg): _____ Company: _____

Please indicate:

⬡ Filipino Resident ⬡ Balikbayan ⬡ Foreign Resident ⬡ Foreign Visitor

*Address:

(No./ Street): _____

(Brgy./ Subdivision): _____

(City/ Town): _____

(Tel. no.): _____

(Fax no.): _____

(Mobile no.): _____

*E-mail Address : _____

⬡ Check here if you not wish to receive news, promos, and event updates from flawless

SECURITY MEASURES

Sec. 20.

...implement reasonable and appropriate organizational, physical and technical measures.

SECURITY MEASURES

Organizational
Physical
Technical

Confidentiality
Integrity
Availability

Organizational Security

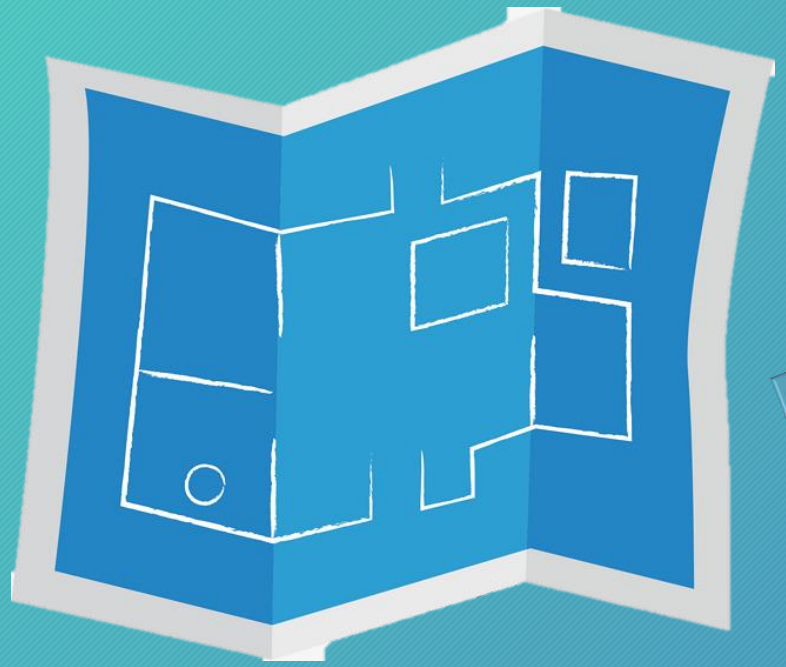
Review of ethical guidelines

Protocols and policies

Training and Capacity building

RORENMARIE M. CHIN, National Privacy Commission

Physical Security



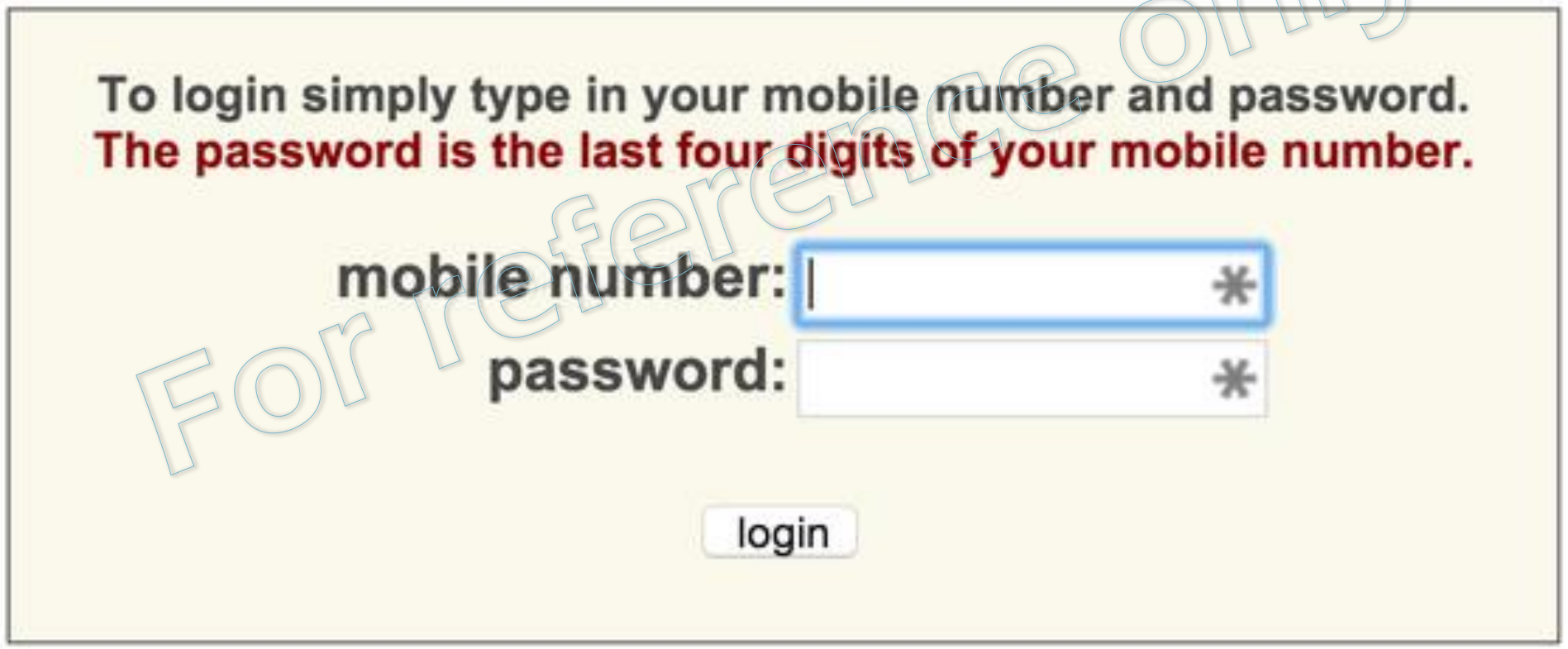
Design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public

Physical Security

"the lock"

Source: https://twitter.com/secfails

Technical Security

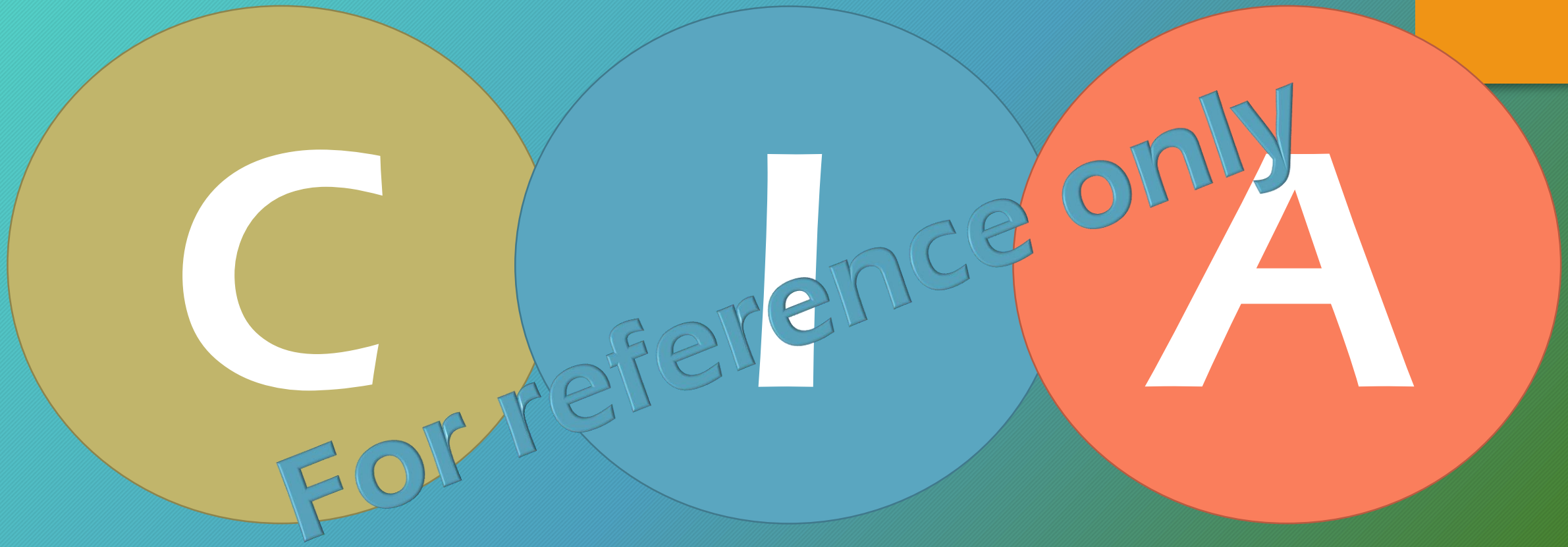


Technical Security

video

Breaches

ROREN MARIE M. CHIN, National Privacy Commission
ROREN MARIE M. CHIN, National Privacy Commission



RORENMARIE M. CHIN, National Privacy Commission

Confidentiality Breach

Due to the unauthorized disclosure of or access to personal data

RORENMARIE M. CHIN, National Privacy Commission

The Ashley Madison hackers have posted personal data like e-mail addresses and account details from 32M of the site's members.

The group claimed two motivations:

First, they've criticized Ashley Madison's core mission of arranging affairs between married individuals.

Second, they've attacked its business practices, in particular its requirement that users pay $19 for the privilege of deleting all their data from the site (but, as it turns out, not all data was scrubbed).

Photograph by Philippe Lopez – AFP/Getty Images

Robert Hackett, What to know about the Ashley Madison hack (Aug. 26, 2015)available at http://fortune.com/2015/08/26/ashley-madison-hack/ (last accessed 2/22/17).

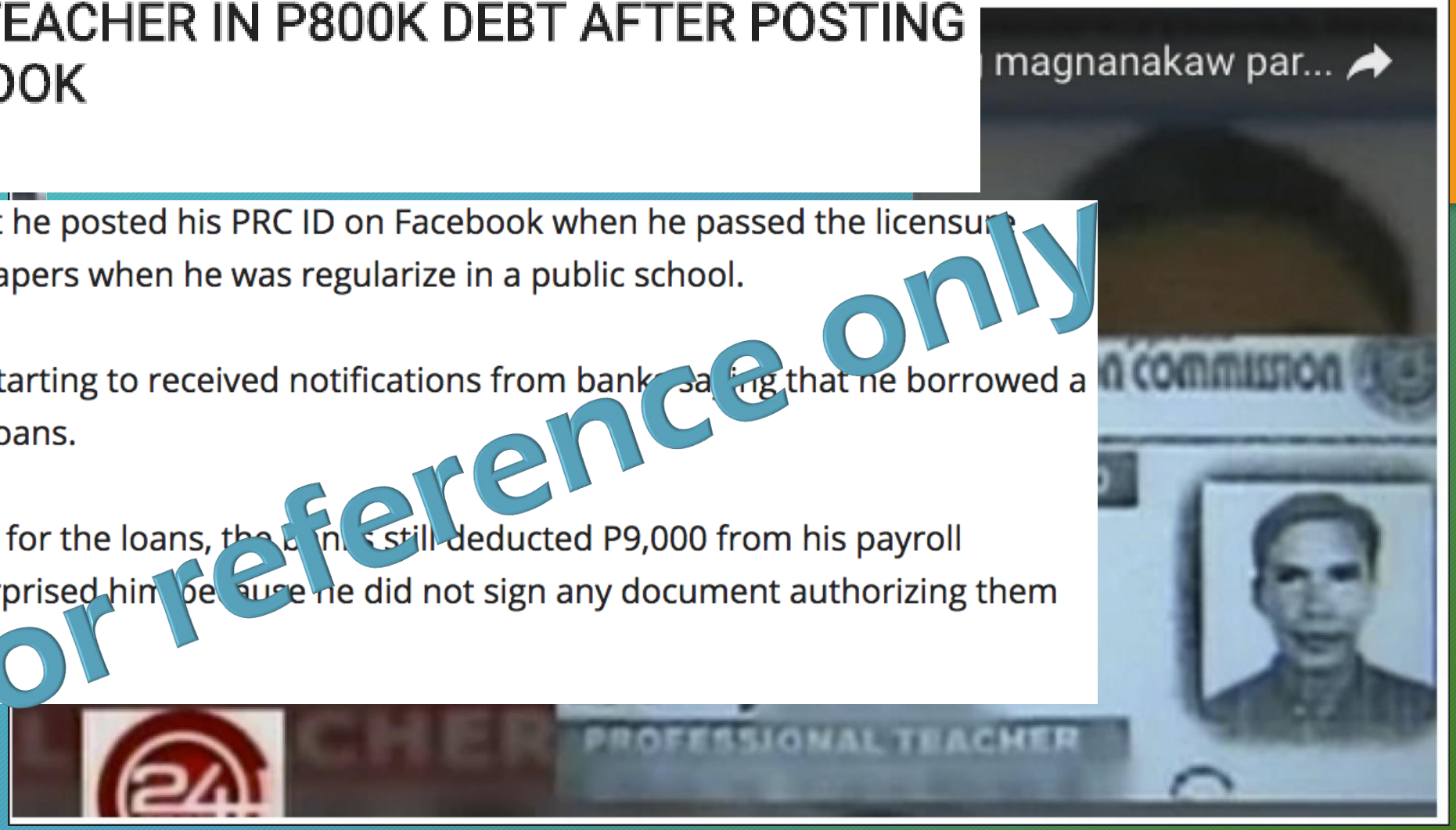
PUBLIC SCHOOL TEACHER IN P800K DEBT AFTER POSTING PRC ID ON FACEBOOK

Date - Saturday, February 27, 2016

In an interview, he said that he posted his PRC ID on Facebook when he passed the licensure exam. He also posted his papers when he was regularize in a public school.

Few months later, he was starting to received notifications from banks saying that he borrowed a total of P800,000 in salary loans.

Though he denied applying for the loans, the banks still deducted P9,000 from his payroll account every month. It surprised him because he did not sign any document authorizing them to deduct the amount.



Available at: http://www.socialtrendsph.com/2016/02/public-school-teacher-in-p800k-debt_37.html

ABS-CBN NEWS

Save

Home > Regions

Ombudsman: Charge docs, nurses in Cebu 'canister scandal'

Share

ABS-CBN News

Posted at May 06 2008 11:03 AM | Updated as of May 06 2008 07:03 PM

The Ombudsman found that the medical attendants committed misconduct for "unlawful behavior and gross negligence of a public officer" and negligence, for "acting or omitting to act in a situation where there is a duty to act"

Source: http://news.abs-cbn.com/nation/regions/05/06/08/ombudsman-charge-docs-nurses-cebu-canister-scandal

The Office of the Ombudsman in the Visayas has recommended the filing of criminal and administrative charges against doctors and nurses involved in what is now known as the "canister scandal" at the government-run Vicente Sotto Memorial Medical Center in Cebu province.

Integrity

Due to alteration of personal data

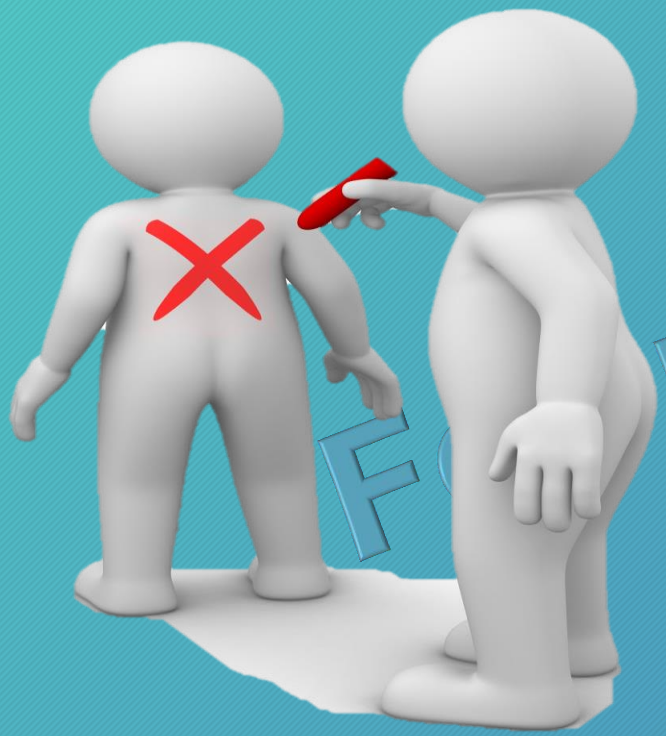
Availability

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

Rights of the Data Subject

ROREN MARIE M. CHIN, National Privacy Commission
ROREN MARIE M. CHIN, National Privacy Commission

RIGHT TO WITHDRAW / SUSPEND / BLOCK



The data subject has the right to withdraw, suspend, or order blocking, removal or destruction of his or her personal information from the personal information controller's filing system

RIGHT TO BE INFORMED

The data subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed

RIGHT TO DISPUTE / CORRECT

The data subject has the right to dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable.

RIGHT TO ACCESS

The data subject has right to reasonable access to, upon demand, his/her personal information.

RIGHT TO DAMAGES

The data subject has right to be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

PENALTIES

RORENMARIE M. CHIN, National Privacy Commission

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. a CIO who did not properly deploy security measures on email or devices, or a health worker who provided password to someone else)	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

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

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

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

Thank you!

Visit us at:

https://privacy.gov.ph/

Like us at:

https://www.facebook.com/IvyDPatdu

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

Contact us at:

info@privacy.gov.ph

RAREN MARIE M. CHIN, National Privacy Commission

RAREN MARIE M. CHIN, National Privacy Commission