RIGHT TO PRIVACY
Right to 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)].
HIPPOCRATIC OATH

Whatever I see or hear, whether professionally or privately which ought not to be divulged, I will keep secret and tell no one.
Doctor-Patient Confidentiality

• Full disclosure of information on the part of the patient is a prerequisite to quality care and better health outcomes.

• Communication between doctor and patient is generally considered privileged and should not be inquired upon even by the Courts. The provision is intended to make sure that information obtained by physicians in the course of treatment will not be used to blacken the reputation of a patient (Rules of Court).

Protecting Patients from Harm includes Respect for their Right to Privacy

Health information is valuable and its unauthorized use or disclosure may put patients at risk for unwanted publicity, discrimination, identity theft and other acts prejudicial to the patient.
RIGHT TO INFORMATION PRIVACY

The individual’s ability to control the flow of information concerning or describing him, which however must be overbalanced by legitimate public concerns. To deprive an individual of his power to control or determine whom to share information of his personal details would deny him of his right to his own personhood.

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.
SCOPE AND DEFINITIONS
Data Privacy Act applies to the processing of personal data by any natural and juridical person in the government or private sector.
Personal Data

• 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
Are these personal data?

A. “Man born on June 19, 1861”
B. “Philippine national hero born on June 19, 1861”
C. “Jose Protacio Rizal”

De-Identification

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, equivalent geocodes, except for the initial three digits of the ZIP code if more than 20,000 people
3. All elements of dates except years (ages over 89 → age 90 or older)
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers including license plates
13. Device identifiers and serial numbers
14. Web URLs
15. Internet protocol addresses
16. Biometric identifies (i.e. retinal scans, fingerprints)
17. Photos
18. Any unique identifying number, characteristic or code

Those who process Personal Data:

*Personal Information

Controller

*Personal Information

Processor
Personal Information Controller

- Individual, Corporation, other body → the one who controls the processing of personal data, the one who decides.
- There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing.
Personal Information Processor

- Individual, Corporation or other body who processes the personal data for a Personal Information Controller
- Personal information processor should not make use of personal data for its own purpose
Uphold Rights of Data Subject

Data Privacy Principles

Security Measures
DATA PRIVACY PRINCIPLES
NOTICE

TRANSPARENCY

LEGITIMATE PURPOSE

PROPORTIONALITY
General Data Privacy Principles

• **Transparency.** The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised.

• Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.
Privacy Notice

• WHAT personal data will be collected
• WHY personal data is processed
  • Purposes of collection and processing, including direct marketing, profiling or research;
  • Basis of processing not based on the consent of the data subject;
• HOW personal data will be collected, used, accessed and stored, including security measures in place
  • Automated processing that will be basis of making decisions that would affect data subject
  • The period for which the information will be stored
PRIVACY NOTICE

• WHO will process personal data
  • The identity and contact details of the personal data controller or its representative
  • The recipients or classes of recipients to whom the personal data are or may be disclosed
  • Transfer of personal data outside the country

• RIGHTS OF DATA SUBJECTS, including the right to file a complaint before the National Privacy Commission.
Rights of Data Subjects

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 Data Portability
8. Right to File a Complaint
General Data Privacy Principles

• **Legitimate purpose.** The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

• Processing of personal data should have the individual’s consent, or must be authorized or allowed by the Constitution or by law.
CONSENT refers to 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.

The consent shall be evidenced by written, electronic or recorded means.
• The complainant attended the accident and emergency department of a public hospital. A few months later, she was contacted by an organisation carrying out research. The researchers knew when she had attended the hospital and why, and they asked her to answer some questions.
CASE STUDY 1/97
https://www.dataprotection.ie/docs/Case-Study-1-97-Hospital-Patient's-Data/156.htm

• The hospital was in fact aware of its obligations under the Data Protection Act, but it contended that it had met these in two ways:

1. It listed "personnel engaged in medical research" as disclosees in its entry in the Public Register of Data Controllers.

2. It made patients aware of the research project by putting a NOTICE in the waiting area of the accident and emergency department. This notice told patients that the hospital intended to disclose their information to the researchers, and invited them to let the receptionist know if they objected.
• On the Noticed Placed in the waiting area: The issue to be decided was whether this was an adequate way of informing patients that their information would be disclosed to the researchers.

• In different circumstances, it might have been. In this case, however, account ought to have been taken of the particular environment in which patients' data were obtained. Many patients presenting themselves at the casualty department of a hospital may be expected to be in a state of some anxiety or discomfort. Consequently, they may not be expected to be alert to matters not relating directly to their condition. In such circumstances there is a special need for the data controller to satisfy itself that any uses of the data which are unlikely to be anticipated by the data subject are fully explained.
Sometimes, Consent is NOT Necessary

- Contractual or Legal Obligation
- Personal Information (not Sensitive)
- To protect life, health, vitally important interests
- Legitimate interests
- National Emergency, public order, public safety
Sometimes, Consent is NOT Necessary

- Law/Regulation
- Sensitive Personal Information
- Provided to government under legal mandate
- Protection of rights in court

To protect life and health

Sometimes, Consent is NOT Necessary

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

IDP 2017
When is consent NOT required?

• Processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing (Emergency, Public Health Emergency).

• Processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured.
Johns Hopkins Hospital to pay $190M settlement after gynecologist secretly recorded patients

Available at https://www.youtube.com/watch?v=iJQHWgQvDaE
General Data Privacy Principles

• **Proportionality.** The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.
PROPERTY OF THE NATIONAL PRIVACY COMMISSION
Para Makautang...
(Please bring this requirements)

- 6pcs 2x2 Picture
- 4pcs 1x1 Picture (Whole Body)
- 3 Valid ID's
- Brgy. Clearance
- NBI Clearance
- Mayors Permit
- Medical
- Cedula
- Birth Certificate (NSO)
- SSS/TIN
- Co-Maker
- X-Ray (Whole Body)
- Police Clearance
- Proof of Billing
- Form 137

Ninja Pepe
Like This Page - February 8 - Edited
SECURITY MEASURES
Organizational
Physical
Technical

Confidentiality
Integrity
Availability
ORGANIZATIONAL SECURITY MEASURES
Data Protection Officer

• Relevant privacy or data protection policies and practices
• Processing operations
• Sector or Industry

THE DPO SHOULD POSSESS SPECIALIZED KNOWLEDGE AND DEMONSTRATE RELIABILITY NECESSARY FOR THE PERFORMANCE OF HIS OR HER DUTIES AND RESPONSIBILITIES.

Privacy Impact Assessment

- **Personal Data Flow**
  - Source and Collection
  - Accountable and responsible persons
  - Purpose of processing
  - Personal Data Processing
  - Security measures
  - Transfer outside country

- **Identify and Assess Privacy Risks**
  - Privacy Risk Identification
  - Privacy Risk Analysis
  - Privacy Risk Evaluation (Level of Impact and Likelihood of Risks)

- **Address risks**
The determination of the appropriate level of security must take into account the nature of the personal data to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation.
Privacy Manual

• Overview
• Scope and Limitations
• Records of Processing Activities
• Data Protection Policies and Security Measures
• Policies and procedures for data subjects to exercise their rights under the Act
• Regular review and monitoring of privacy and security policies
Procedure for collection, use or disclosure, storage and disposal of personal data

| Revised Rules of Evidence, Rules of Court, (March 14, 1989) | Section 24 (c), Rule 128: Disqualification by reason of privileged communication. — The following persons cannot testify as to matters learned in confidence in the following cases: A person authorized to practice medicine, surgery or obstetrics cannot in a civil case, without the consent of the patient, be examined as to any advice or treatment given by him or any information which he may have acquired in attending such patient in a professional capacity, which information was necessary to enable him to act in capacity, and which would blacken the reputation of the patient |
| An Act Defining Violence Against Women and Their Children, Providing for Protective Measures for Victims, Prescribing Penalties Therefore, and for Other Purposes, “Anti-Violence Against Women and Their Children Act of 2004”, Republic Act No. 9262, (March 8, 2004) | Section 44. Confidentiality. — All records pertaining to cases of violence against women and their children including those in the barangay shall be confidential and all public officers and employees and public or private clinics to hospitals shall respect the right to privacy of the victim. Whoever publishes or causes to be published, in any format, the name, address, telephone number, school, business address, employer, or other identifying information of a victim or an immediate family member, without the latter's consent, shall be liable to the contempt power of the court. Any person who violates this provision shall suffer the penalty of one (1) year imprisonment and a fine of not more than Five Hundred Thousand pesos (P500,000.00). |
| Philippine National AIDS Council Resolution No. 1, Rules and Regulations Implementing the Philippine AIDS Prevention and Control Act of 1994 (RA 8504), (April 13, 1999) | Sec. 41. Medical Confidentiality. Medical confidentiality shall protect and uphold the right to privacy of an individual who undergoes HIV testing or is diagnosed to have HIV. It includes safeguarding all medical records obtained by health professionals, health instructors, co-workers, employers, recruitment agencies, insurance companies, data encoders, and other custodians of said record, file, or data. Confidentiality shall encompass all forms of communication that directly or indirectly lead to the disclosure of information on the identity or health status of any person who undergoes HIV testing or is diagnosed to have HIV. This information may include but is not limited to the name, address, picture, physical description or any other characteristic of a person which may lead to his/her identification. To safeguard the confidentiality of a person's HIV/AIDS record, protocols and policies shall be adopted by concerned officials, agencies and institutions. |

PHYSICAL SECURITY MEASURES
Physical Security Measures

• 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.

• The room and workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.
Records room, work stations and data centers should have limited access.

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

Technical Security Measures

- SECURITY POLICY
- SYSTEM MONITORING
- SAFEGUARDS: ENCRYPTION, AUTHENTICATION PROCESS
- INCIDENT RESPONSE, CORRECT AND MITIGATE BREACH, RESTORE SYSTEM
National Privacy Commission Issuances

16-01 SECURITY OF PERSONAL DATA IN GOVERNMENT AGENCIES

16-02 DATA SHARING AGREEMENTS INVOLVING GOVERNMENT AGENCIES

16-03 PERSONAL DATA BREACH MANAGEMENT

Circular 17-01 REGISTRATION OF DATA PROCESSING SYSTEMS

Advisory 17-01 DESIGNATION OF DATA PROTECTION OFFICERS

16-04 RULES OF PROCEDURE OF THE NATIONAL PRIVACY COMMISSION
Demonstrate Compliance

1. Governance
2. Risk Assessment
3. Organization
4. Day to Day
5. Data Security

6. Breaches
7. Third Parties
8. Manage HR
9. Continuity
10. Privacy Ecosystem
WHY SHOULD PERSONAL DATA BE PROTECTED?

ACCOUNTABILITY
<table>
<thead>
<tr>
<th>CRIME</th>
<th>IMPRISONMENT</th>
<th>FINE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing of Personal/Sensitive Information for Unauthorized Purpose</td>
<td>Processing information when not authorized (purpose other than medical treatment)</td>
<td>1yr 6mos – 7 years</td>
</tr>
<tr>
<td>Access to Personal/Sensitive Information due to Negligence</td>
<td>Persons who provide access due to negligence shall be liable</td>
<td>1-6 years</td>
</tr>
<tr>
<td>Concealment of Security Breach</td>
<td>Duty to notify Privacy Commission in case of breach</td>
<td>1yr 6mos – 5 years</td>
</tr>
<tr>
<td>Improper Disposal</td>
<td>Negligently dispose, discard or abandon personal data of an in an area accessible to the public or placed in its container for trash collection.</td>
<td>6 months – 3 years</td>
</tr>
</tbody>
</table>
“In this digital era, information is the currency of power – valuable, coveted, but at a very high risk.”

-Senator Edgardo Angara, sponsorship speech for the Data Privacy Act
What can you “buy” with your personal data?
Four people nabbed in Recto for producing counterfeit documents

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
Thank you!

Ivy D. Patdu
National Privacy Commission