COMPLIANCE FRAMEWORK and DATA PRIVACY ACCOUNTABILITY

Robert S. Paguia, LLB, MPM

Office of the Privacy Commissioner

National Privacy Commission

5 PILLARS OF COMPLIANCE

1	2	3	4	5
Appoint a Data Protection Officer	Conduct a Privacy Impact Assessment	Create a Privacy Management Program	Implement Data Privacy and Security Measures	Be ready in case of a Data Breach

4th Pillar: Demonstrate your Compliance

Implement Privacy & Data Protection Measures

The Data Privacy Accountability and Compliance Framework

A. Choose a DPO

B. Register
C. Records of processing activities
D. Conduct Risk Assessment

E. Privacy Management Program
F. Privacy Manual

G. Privacy Notice
H-O. Data Subject Rights
P. Data Life Cycle

Q. Organizational
R. Physical
S. Technical
- Data Center
- Encryption
- Access Control Policy
- Vulnerability Assessment and Penetration Testing

T. Data Breach Management;
- Security Policy
- Data Breach Response Team
- Incident Response Procedure
- Document
- Breach Notification

U. Third Parties;
- Legal Basis for Disclosure
- Data Sharing Agreements
- Cross Border Transfer Agreement

V. Trainings and Certifications
W. Security Clearance

X. Continuing Assessment and Development
- Regular PIA
- Review Contracts
- Internal Assessments
- Review PMP
- Accreditations

Y. New technologies and standards
Z. New legal requirements

GENERAL DATA PRIVACY PRINCIPLES

1. TRANSPARENCY

2.LEGITIMATE PURPOSE

3.PROPORTIONALITY

1. GOVERNANCE

A. DESIGNATE A DPO

The Registration System is one of the means by which the NPC can ensure compliance with the law and its IRR by the Personal Information Controllers (PICs) and Personal Information Processors (PIPs).

Registration of all the organization's data processing systems will also assist both the Commission and those involved in processing of personal data (PIP and PIC) in upholding the rights of the Data Subject.

C. RECORDS OF PROCESSING ACTIVITIES

PROCESSING refers to any operation or any set of operations performed upon personal data including but not limited to the COLLECTION, RECORDING, ORGANIZATION, STORAGE, UPDATING or MODIFICATION, RETRIEVAL, CONSULTATION, USE, CONSOLIDATION, BLOCKING, ERASURE or DESTRUCTION of data.

Generally, it is changing information in any manner detectable by any witness or observer.

2. RISK ASSESSMENT

B. REGISTER WITH NPC

Compliance with the law (RA 10173 or the Data Privacy Act of 2012) starts by appointing or designating a Data Protection Officer (DPO) or in certain cases a Compliance Officer for Privacy (COP).

The DPO or COP shall be accountable for ensuring compliance with the law, its Implementing Rules and Regulations (IRR), Circulars, Advisories and other Commission issuances.

For additional information, please see NPC Advisory No. 2017-01.

D. CONDUCT OF RISK OR IMPACT ASSESSMENT

This is the part where privacy risks identified by an organization through the Privacy Impact Assessment (PIA) are described. This also includes the actions being proposed to mitigate and manage those privacy risks.

3. ORGANIZATION

E. PRIVACY MANAGEMENT PROGRAM

A PMP is a strategic framework to help PICs and PIPs build a robust privacy infrastructure supported by an effective on-going review and monitoring process to facilitate compliance.

It minimizes the risks of privacy breaches, maximizes the ability to address underlying problems, and reduces the damage arising from breaches.

Demonstrates commitment to building trust with employees and clients through open and transparent information policies and practices.

F. PRIVACY MANUAL

The Privacy Manual serves as a guide or handbook for ensuring compliance by organizations and entities with the law (DPA of 2012), its IRR, Circulars, Advisories and other Issuances of the Commission.

It encapsulates the privacy and data protection protocols that need to be observed and carried out within the organization or entity for specific circumstances (see data life cycle, from collection to destruction), directed toward the fulfilment and realization of the rights of the data subjects.

4. DAY to DAY

G. PRIVACY NOTICE

A Privacy Notice is a statement made to a Data Subject describing how an organization or entity COLLECTS, USES, TRANSMITS, RETAINS, DISCLOSES and DESTROYS personal information.

It is sometimes referred to as a Privacy Statement or a Fair Processing Statement.

It should be easy to read for the same to be effective and easily understood by Data Subjects.

PRIVACY NOTICE and PRIVACY POLICY

To simplify the difference, a privacy policy is **internally focused**, telling employees what they may do with personal information, while a privacy notice is **externally facing**, telling customers, regulators and other stakeholders what the organization does with personal information.

Privacy Policy: *An internal statement that governs an organization or entity's handling practices of personal information. It is directed at the users of the personal information. A privacy policy instructs employees on the collection and the use of the data, as well as any specific rights the data subjects may have.*

Privacy Notice: *A statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information. A privacy notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy. Special privacy notices are also mandated by specific laws such as GLBA and COPPA in the United States*

(https://www.csoonline.com/article/3063601/privacy/privacy-policies-and-privacy-notices-whats-the-difference.html)

PRIVACY NOTICE and PRIVACY POLICY

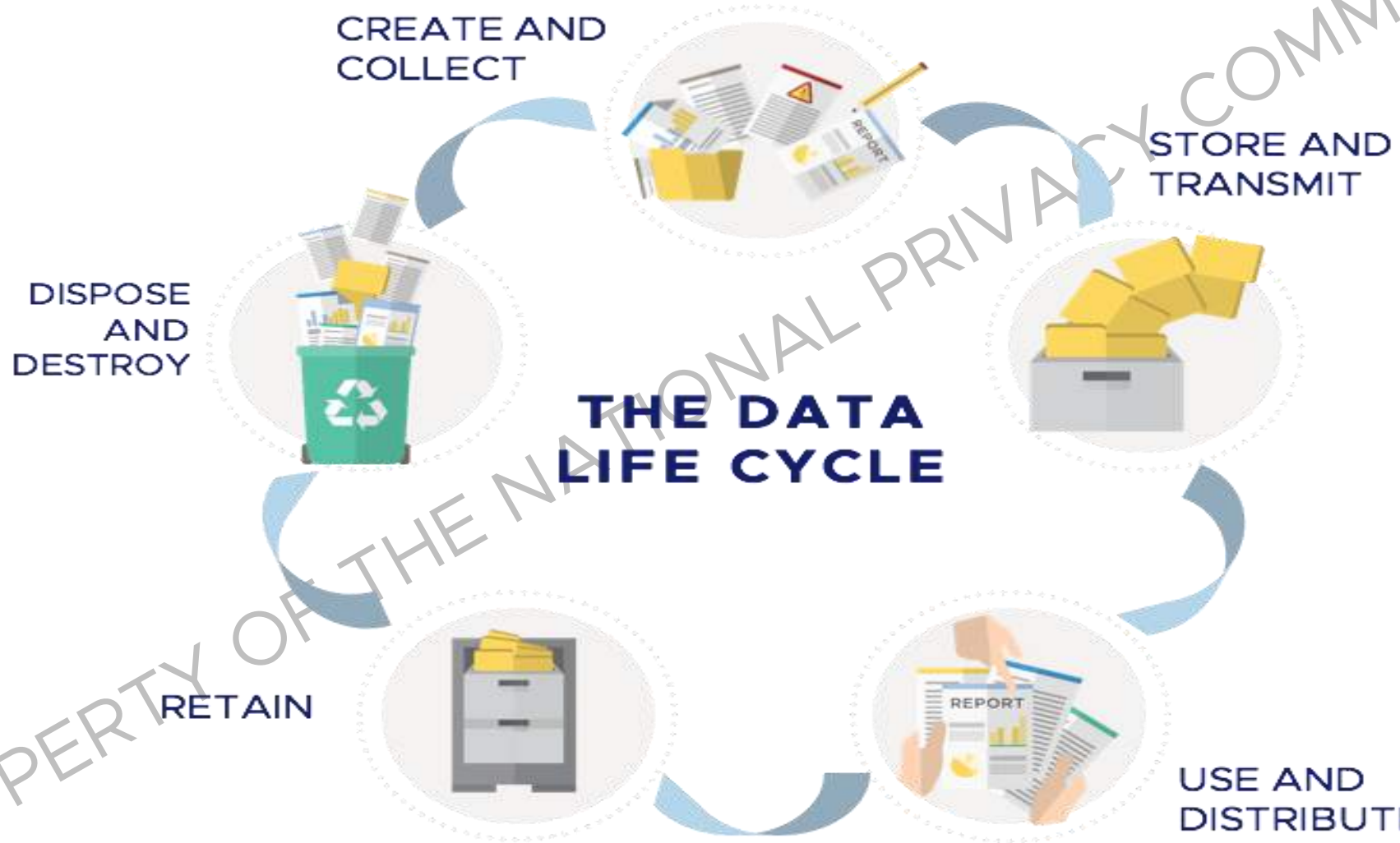
PRIVACY POLICY	PRIVACY NOTICE
SCOPE Type of Information (electronic, paper, encrypted) Who the policy applies to (employees, contractors, vendors)	WHEN YOU COLLECT PERSONAL INFORMATION
POLICY STATEMENT Expected Behavior Consequences of Non-compliance	WHY YOU COLLECT PERSONAL INFORMATION
DEFINITION OF PERSONAL INFORMATION Information classification	WHAT INFORMATION IS COLLECTED
PROTECTION STANDARDS	HOW YOU PROTECT THE INFORMATION
DESTRUCTION STANDARDS	WHEN YOU SHARE THE INFORMATION
WHO TO CALL FOR QUESTIONS & CONCERNS	WHO TO CONTACT Where questions should be directed How to opt-in / opt-out What to do if there is a problem
EFFECTIVITY DATE	EFFECTIVITY DATE

(https://www.csoonline.com/article/3063601/privacy/privacy-policies-and-privacy-notices-whats-the-difference.html)

H to O
RIGHTS OF THE DATA SUBJECTS

H. Right to Information
I. Right to Access
J. Right to Object
K. Right to Erasure or Blocking
L. Right to Damages
M. Right to File a Complaint
N. Right to Rectification / Correction
O. Right to Data Portability

P. THE DATA LIFE CYCLE



5. DATA SECURITY

Q. ORGANIZATIONAL SECURITY MEASURES

Appoint a Data Protection Officer (DPO)

Conduct Privacy Impact Assessment

Training and Capacity Building

Medical group fined $140K for tossing patients' health records into public dump

Names, Social Security numbers, and medical diagnoses for more than 67,000 Massachusetts residents in the US were tossed into a public dump as is – no redacting, no shredding, no nothing – according to a press release put out by Attorney General Martha Coakley last week.

For the alleged mishandling and improper disposal of medical records, former owners of a medical billing practice, along with the doctors involved, have agreed to pay a $140,000 settlement.

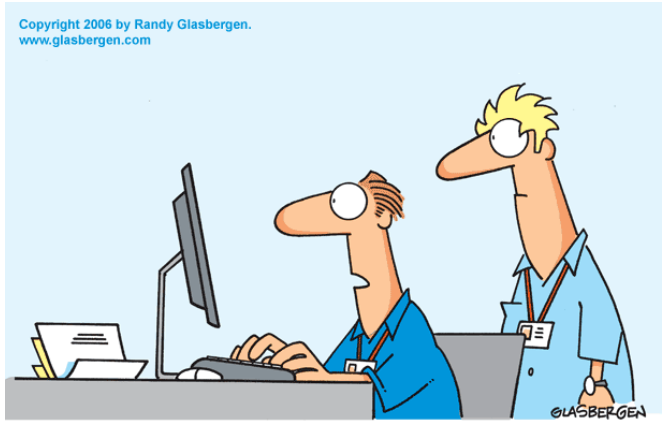
https://nakedsecurity.sophos.com/2013/01/15/medical-patients-health-records-dump/

R. PHYSICAL SECURITY MEASURES

Should help prevent theft

Workstations secured

- Security locks at the entrance of the office where data is stored
- Biometrics verification (fingerprint, eye, etc.)



"Information security is a major priority at this company.
We've done a lot of stupid things we'd like to keep secret."

S. TECHNICAL SECURITY MEASURES

Implementation of ICTs (Firewalls, Encryption, passwords, etc.)

Protection against Ransomwares, Malwares, etc.

6. BREACHES

T. DATA BREACH MANAGEMENT

1. **Security Incident Management Policy** – this is intended to manage Security Incidents including Data Breaches.
2. **Data Breach Response Team** – PICs and PIPs shall form a Data Breach Response Team (DBRT) which shall have at least one (1) member with the authority to make immediate decision regarding critical action, if necessary. The team may include the DPO. (Circular 16-03, Section 5)
3. **Incident Response Procedure** – PICs and PIPs shall implement policies and procedures for guidance of its DBRT and other personnel in the event of a security incident. (Circular No. 16-03, Section 8)
4. **Breach Documentation** – All actions undertaken by the PIC and PIP shall be properly documented which may be in the form of reports that include description of the data breach, actions taken and decisions made by the DBRT and outcome of the breach management, among others. (Circular No. 16-03, Section 8)
5. **Breach Notification** – both the Commission and the Data Subjects shall be duly notified within a period of 72 hours upon knowledge of or reasonable belief by the PIC or PIP that a security incident occurred. (Section 38, IRR)

7. DISCLOSURE TO 3RD PARTIES

U. THIRD PARTIES

1. **Legal Basis of Disclosure** – Sharing of personal information between and among organizations and entities are required to be covered by an agreement especially if the data being shared refer to sensitive personal information.
2. **Data Sharing Agreements** – refers to a CONTRACT, JOINT ISSUANCE or any similar document that contains the terms and conditions of the sharing arrangement between two or more parties.
3. **Cross Border Transfer Agreement** – globally, there is a general recognition that there should be some law regarding cross-border data transfers but a wide variety of approaches to this issue exist, and there is no single global model for managing it. See Section 50, IRR

8. MANAGE HR

V. TRAININGS AND CERTIFICATIONS

Orientation or training programs regarding privacy or security policies should be provided to employees.

Additional training specifically tailored to their roles should be given to those who handle personal data. The training and education should be current and relevant.

Some Certifications recommended by the Commission are (a) ISO/IEC 27001:2013, (b) ISO/IEC 27002:2013, (c) ISO/IEC 27018:2014, (d) Certified Information Systems Auditor (CISA), (e) Certified Information Security Manager (CISM), (f) Certified in the Governance of Enterprise IT (CGEIT) and (g) Certified Information Systems Security Professionals (CISSP).

W. SECURITY CLEARANCE

This allows authorized access to personal information that would otherwise be forbidden.

PICs and PIPs shall only grant security clearance to an employee when the performance of his or her official functions directly depends on and cannot otherwise be performed unless access to the personal data is allowed. This will ensure confidentiality of the personal data.

Other means to ensure confidentiality of personal data is the use of **Non-Disclosure Agreements** (NDA).

9. CONTINUITY

X. CONTINUING ASSESSMENT & DEVELOPMENT

Assess and Revise Program Controls

- The effectiveness of program controls should be **monitored regularly**, **audited periodically** and where necessary, **revised accordingly**.

- The monitoring should address the following questions:
  - What are the latest threats and risks?
  - Are the program controls addressing new threats and reflecting the latest complaint or audit findings?
  - Are new services being offered involve increased collection, use or disclosure of personal data?
  - Is training necessary? If yes, is it taking place? Is it effective? Are policies and procedures being followed? Is the training up-to-date?

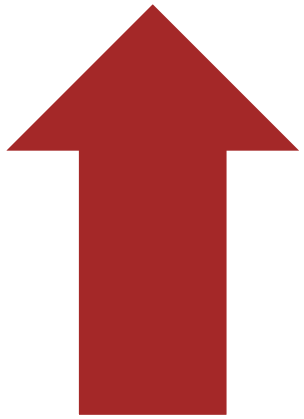
- Review and Monitoring
  - Schedule Regular PIA
  - Review Forms, Contracts, Policies, and Procedures on a regular basis
  - Review, Validate and Revise Privacy Manual.

10. PRIVACY ECOSYSTEM

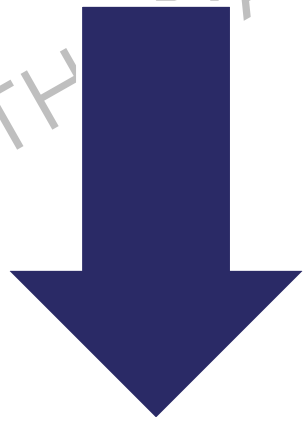
Y. NEW TECHNOLOGIES & STANDARDS

Z. NEW LEGAL REQUIREMENTS

PRIVACY and DATA PROTECTION



Maximizing BENEFITS



Minimizing HARM

In today's data-driven economy, ***privacy has become the proxy for trust:*** if you allow my privacy to be breached, you lose my trust, and if you lose my trust, you lose my business.

DONDI O. MAPA
Former Deputy Privacy Commissioner
National Privacy Commission

NATIONAL PRIVACY COMMISSION

3rd Level, Core G,

GSIS Headquarters, Financial Center Area, Roxas Boulevard, Pasay City

CONTACT US

info@privacy.gov.ph

privacy.gov.ph

facebook.com/privacy.gov.ph

twitter.com/PrivacyPH

Trunk line: 920-0101

Office extension numbers:

OPC – 7001	FAO – 7011
PIAD – 7021	CID – 7031
CMD – 7041	

NATIONAL PRIVACY COMMISSION

Thank you!