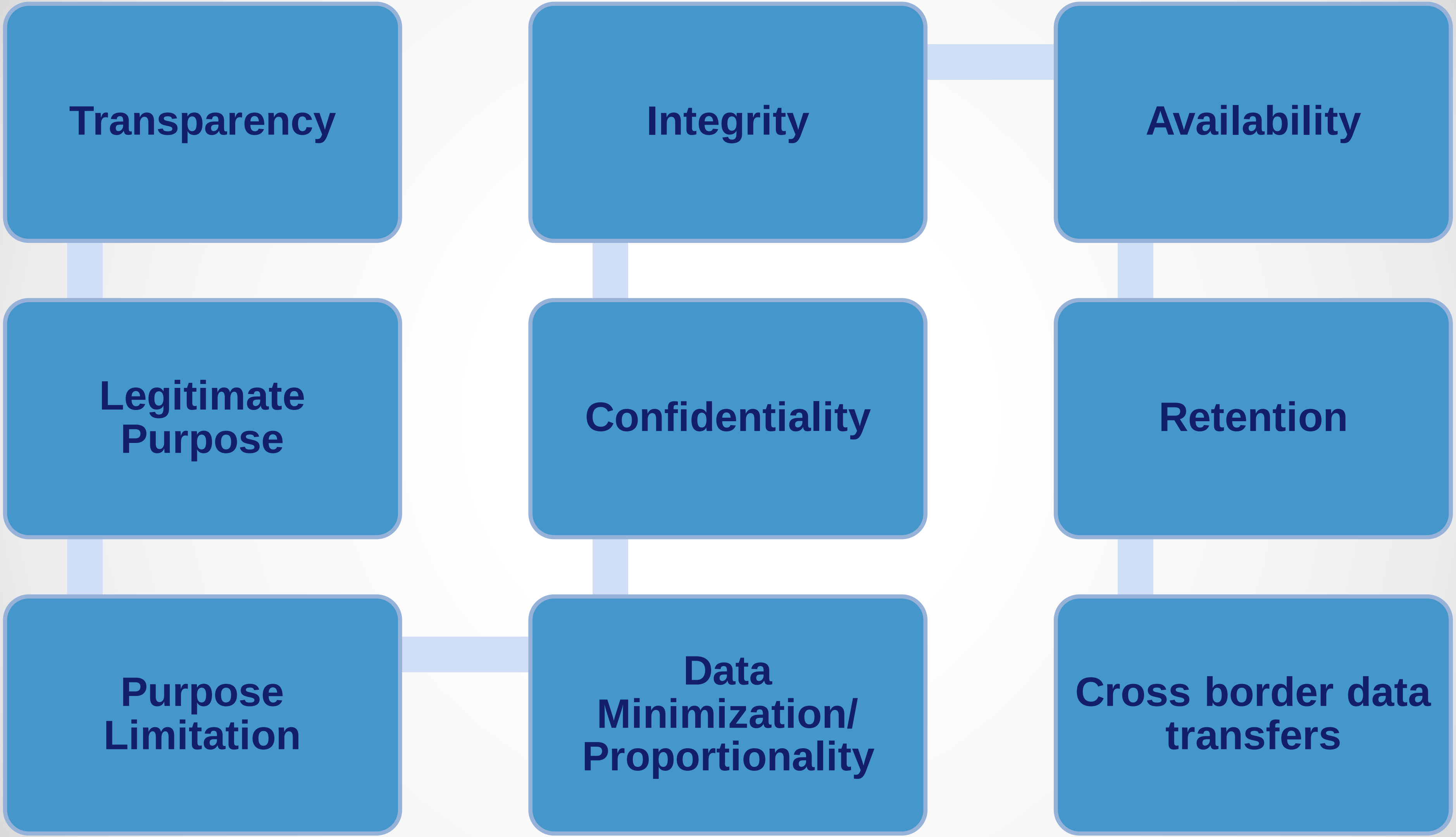
Workshop on Privacy Impact Assessment

NATIONAL
PRIVACY
COMMISSION



Transparency

Legitimate Purpose

Purpose Limitation

Data Minimization/ Proportionality

Confidentiality

Integrity

Availability

Retention

Cross border data transfers

Assignment

- Select the case your group will work on (or use your own work process).
- Identify the “roles” involved in the Information Life Cycle.
- Assign each role to one or more team members.
- Assign someone to be the Chief Executive (CEO, Mayor, Head of Agency)

- Deliverables, Part 1:
  - Information Life Cycle and Roles
  - Worksheets for Steps 1 to 3
  - Privacy Risk Map
- Deliverables, Part 2
  - Worksheet for Steps 4 and 5

Case Study A

Vaccination Program

The Department of Health requires those who participate in the Libreng Bakuna Program to sign up using forms provided for the purpose by the DOH.

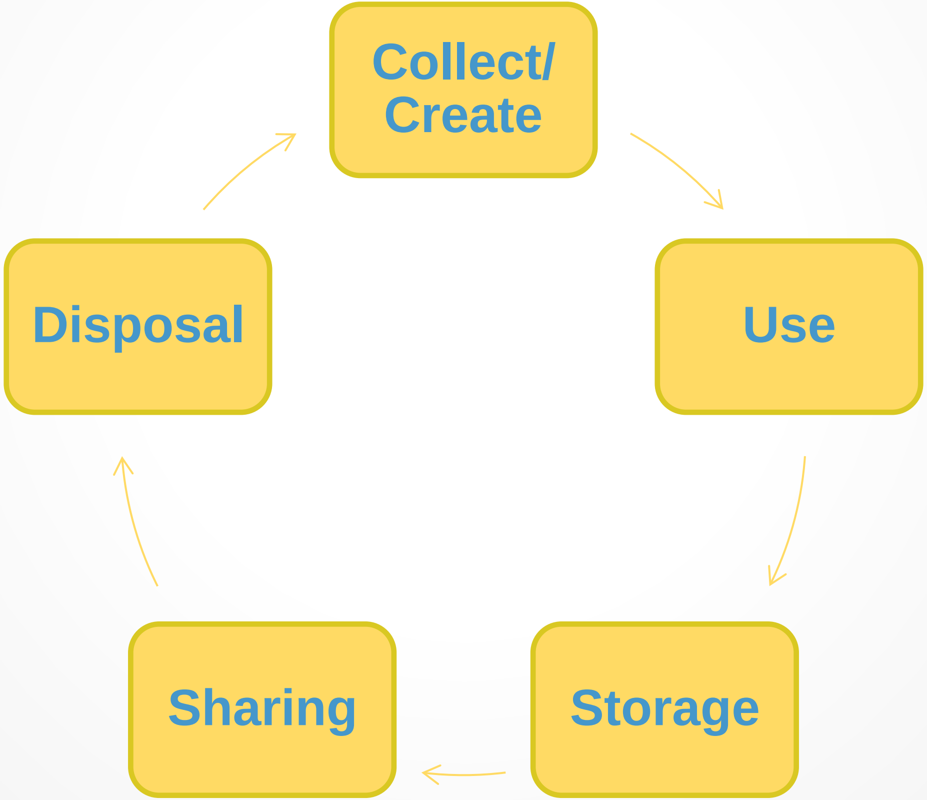
The forms indicated that the participants must enter their name, age, address, proof of billing/residence, government-issued identification, name, age, and gender of child/children to be enrolled.

The sheets will be kept in a folder in the office of the Barangay Health Officer.

Around one hundred families plan to avail of the free vaccination.

Case Study B	Case Study C	Case Study D
Closed Circuit TV	Feelings Graph	Email Invitation
In an effort to reduce criminality in the barangay, barangay officials decide to install high-definition CCTVs at critical locations in the neighborhood. To save costs, the cameras were connected by wi-fi to the cable TV network in the area and feed into a data center in the barangay hall. Some hackers took over one of the cameras and used it to film an intimate moment with another neighbor. This footage was broadcast on pornographic website.	In order to test a new feature in its smartwatch, a company ordered all 500 of its employees to wear the new smartwatch 24 x 7. The new feature collects information on heartbeat and skin temperature at any given time, e.g. when talking to the boss, or while having merienda with a co-employee. The resulting “Feelings Graph” is then posted to a social media site where the wearer can attach captions to specific events on the graph to explain what was happening on key portions of the graph.	A church worker collected emails of church-goers interested to participate in a seminar on alcoholism and drug-abuse self-rehabilitation. These seminars are conducted once a month. An email blast was sent displaying all the emails of the persons who were invited or expressed interest. One of the invited seems to be a known celebrity, and another seems to be an LGU member. The list is leaked to the press, and speculation about the identities becomes a trending topic on Twitter.

WHO should participate in the PIA?
Those involved in the Information Life Cycle



Collect/ Create

Use

Storage

Sharing

Disposal

STEP 1: Define the process.

1. What data is being collected by this process (list all, including personal as well as non-personal) 2. Which data (if any) is considered sensitive personal information (underline these)	
3. Who are we collecting this data from 4. How are we collecting this data	
5. Why is this data being collected 6. Will we use this data to make any decisions that have a legal effect on the data subject	
7. Who will be handling and accessing this data 8. Will the data be shared with any other organizations	
9. What is the key benefit/s the data subject gets from this process 10. What is the key benefit/s for the community or society	

Step 2: Ensure that processing is legally allowed and in compliance with the Data Privacy Act of 2012.

1. What is the legal basis for collecting this data 2. Are we over-collecting	
3. How will consent be obtained 4. Do individuals have the opportunity and/or right to decline to provide data 5. What happens if they decline	
6. How will the data collected be checked for accuracy 7. How will data subjects be allowed to correct errors, if any	
8. Will the data be re-used 9. How	
10. How long are we required to keep the data 11. How do we plan to dispose of the data	

Step 3: Define the the probability that the activity involving data will result in harm, or a loss of the rights and freedoms of the data subject.

1. How easy would it be to identify me (on a scale of 1 to 4) if this data were to be breached or exposed?	1: virtually impossible 2: difficult but possible 3: relatively easy 4: extremely easy	
2. What things might happen if someone unauthorized gets this data 3. How might this happen (describe scenario/s) 4. How much damage would this cause me (on a scale of 1 to 4)	1: slight inconvenience 2: stressful inconvenience 3: major difficulties 4: extreme consequences	
5. What things might happen if someone alters or changes my data 6. How might this happen (describe scenario/s) 7. How much damage would this cause me (on a scale of 1 to 4)	1: slight inconvenience 2: stressful inconvenience 3: major difficulties 4: extreme consequences	
8. What things might happen if this data suddenly becomes unavailable 9. How might this happen (describe scenario/s) 10. How much damage would this cause me (on a scale of 1 to 4)	1: slight inconvenience 2: stressful inconvenience 3: major difficulties 4: extreme consequences	
11. What things might happen if this data is used for other purposes 12. How might this happen (describe scenario/s) 13. How much damage would this cause me (on a scale of 1 to 4)	1: slight inconvenience 2: stressful inconvenience 3: major difficulties 4: extreme consequences	

Privacy Risk Map

Extreme				
Major				
Stressful				
Slight				
	Nil	Low	Med	High

Step 4. Review existing controls, if any. Identify new controls using privacy-by-design principles.

		Cost/Effort (H/M/L)
Is there a way we can increase the benefits provided? If yes, how?		
Is there a way we can collect less data and thus reduce the exposure level?		
How can we reduce the privacy risks related to someone unauthorized getting this data?		
How can we reduce the privacy risks related to someone altering or changing the data?		
How can we reduce the privacy risks related to the data suddenly becoming inaccessible?		
How can we reduce the privacy risks related to re-using the data for other purposes?		

Step 5. Summary (done by the “Chief Executive”)

Given this process	
With this legal purpose	
Providing this benefit (H/M/L)	
With privacy risk of (H/M/L)	
Controls Complexity (H/M/L)	
Overall Assessment	

Summary

- This is not the OFFICIAL way to do a PIA or PbD. There are many ways to do a PIA, such as a workshop, a workflow, a survey, an interview. (See ISO 29134)
- This SIMULATION is meant to show the ROLES that need to be included in a PIA, the CONCEPTS which must be considered, and the essential ELEMENTS.
- PIAs submitted to the NPC will be reviewed for: stakeholder involvement, thoroughness of risk analysis, and completeness of controls framework.
- After six months, we will also review status of controls implementation, as well as results of a breach drill for the process.