DATA PRIVACY TOOLKIT

FOR RESEARCH INVOLVING HUMAN PARTICIPANTS

With funding support from the Philippine Council for Health Research and Development (PCHRD)

Cite as:
Sy, P.A., Nicolas, F., Navera, J.C., Regnim, J.M., & Caraan, A. (2021). Data Privacy Toolkit for Research Involving Human Participants. Social Sciences and Philosophy Research Foundation, Inc.
DOI: 10.6084/m9.figshare.14815881

Display type set in Lovelo Line, Blogger Light, Economica, Hussar Bold, and Hussar Ekologiczy.

Text type set in Lazord Sans Serif, Archivo Narrow, TS Tarek Black, Codec Pro, League Spartan, Josefin Sans Bold, Muli Bold, and MediaPro.

Edited by
Selena Sison

Illustrations by
Ralph Rodrigo Yap, Mark Luis Bulan,
and Mark Ian Medina

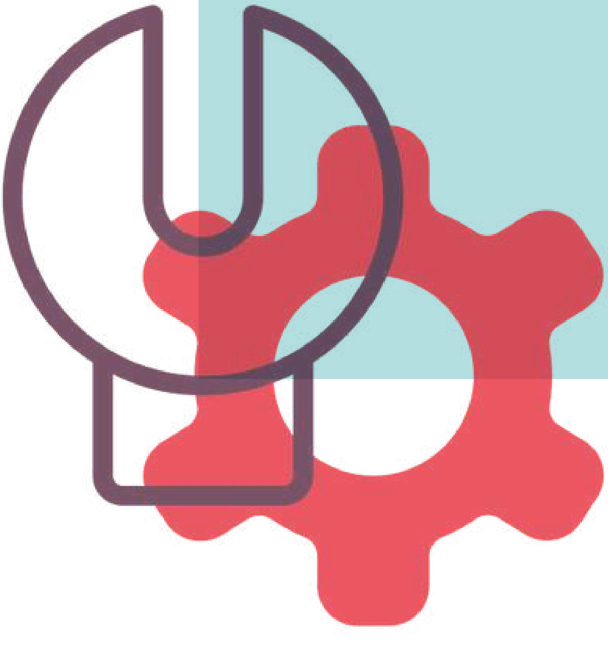
Book design by
Georgina Mia B. Gato

Photos from Unsplash, Pexels, and Freepik

Printed in the Philippines

DATA PRIVACY TOOLKIT FOR RESEARCH INVOLVING HUMAN PARTICIPANTS

Peter A. Sy
Fatima May Nicolas
J.C. Navera
Jewel Mae Regnim
Aleli Caraan



FOREWORD

Congratulations to the Social Sciences and Philosophy Research Foundation, Inc. (SSPRF) on the successful development of the Data Privacy Toolkit for Research Involving Human Participants!

The Toolkit, launched at this most opportune time, will surely aid researchers in conducting effective studies while having utmost regard for the data privacy rights of human participants or research subjects, and maintaining the confidentiality of their personal data. Research subjects will also be guided on their data privacy rights as participants in research studies and on the appropriate ways to exercise such rights.

Republic Act (R.A.) No. 10173, otherwise known as the Data Privacy Act of 2012 (DPA), recognizes that research serves a public interest and is vital to national development. [1] It is the intent of the DPA to grant a certain degree of flexibility in the processing of personal data for purposes of research. In fact, personal data processed for research is included under the DPA's special cases which fall outside the scope of the law to the minimum extent necessary for research purposes intended for a public benefit and subject to the requirements of applicable laws, regulations, or ethical standards.

It is worth noting that despite the exemption, researchers are required to comply with the relevant provisions of the DPA. Processing should still adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. Furthermore, reasonable and appropriate physical, organizational, and technical security measures must be implemented once personal data has been collected from the research subjects.

The DPA is not meant to impede the conduct of research. On the contrary, it strengthens it. The DPA should be read together with ethical standards and other applicable laws on research. This improved quality standard will foster trust in the research sector, encourage more individuals to partake in research studies, and entice potential grants and funding for the same.

To the SSPRF, the National Privacy Commission is one with you in ensuring that data privacy rights of research subjects in the conduct of ethical research studies are upheld at all times. Again, congratulations and we look forward to your future endeavors.

Raymund Enriquez Liboro
Commissioner
National Privacy Commission

[1] See: National Privacy Commission, NPC Advisory Opinion No. 2019-017 (March 5, 2019).

PREFACE

The Data Privacy Toolkit for Research Involving Human Participants (privacyph.org/toolkit) is an output of the participatory action research project, “Development of a Data Privacy Toolkit for Research Involving Human Participants in the Philippines”, funded by the Philippine Council for Health Research and Development. Along with its companion Primer (privacyph.org/primer) and Online Course (privacyph.org/course), the Toolkit is intended to be used as an instrument to operationalize privacy protection in research.

Our Project sought to employ a “toolkit approach” as a set of tools put together to address issues and concerns under the new privacy regulations. Such an approach emphasizes the deployment of “tools” or the means to solve otherwise complex problems with uncertain outcomes. It aims at a demonstrable resolution of conflicts and competing interests, and at the promotion of initial common understanding—enough to engage actors and stakeholders and help them solve the problems at hand.

However useful it may seem, the Toolkit is not a stand-alone instrument. Privacy, after all, is an ethical, legal, and cultural concept that strongly resists essentialist characterizations. Merely following a compliance checklist cannot exhaust the attendant contextual issues that privacy practitioners encounter in research. Earlier ethics interventions have noted the possible limitations of the toolkit approach due to its "one-size-fits-all" design, which may need to suit particular local needs. Taking this to heart, our Project made a special case for research involving human participants. While the National Privacy Commission already has a privacy toolkit for organizations in general, it lacks any specifics on human subjects research, especially when research itself is supposedly given special consideration under the law. Hence, there is the need for special tools specifically developed for and driven by research practitioners themselves. The Project also developed a companion Primer and Online Course to better lay down the essential concepts and frameworks used in the Toolkit itself.

This Toolkit would not have been possible without our fruitful partnership with colleagues from Silliman University, University of the Philippines Diliman, Mindanao State University–Iligan Institute of Technology, University of the Philippines Baguio, Mindanao State University–General Santos City, the Philippine Sociological Society, and the University of San Carlos. Together, we conducted privacy workshops for researchers, ethics committee members, and stakeholders from Luzon, Visayas, and Mindanao. Insights from prior privacy-related engagements (workshops, forums, consultation meetings) with the Department of Health (DOH), the Philippine Health Research Ethics Board (PHREB), and the Philippine Social Science Council (PSSC) were also incorporated into our materials. However, none of the flaws or oversights this Toolkit may contain can be attributed to any of these institutions.

The Project Team hopes that this Toolkit, as well as the companion Primer and Online Course, will be useful to ethics reviewers, researchers, research participants, and other entities in incorporating the privacy protection of data subjects in their present and prospective endeavors. We welcome feedback to help us further develop our materials. For more information on Project activities and updates, visit privacyph.org.

ACKNOWLEDGMENTS

This Toolkit (privacyph.org/toolkit) would not have been possible without the contributions of various organizations and individuals. First, our utmost thanks to the Philippine Council for Health Research and Development (PCHRD) and its Executive Director, Dr. Jaime Montoya, for their sponsorship and endorsement. The grant gave us the means to pursue this Project, engage the research community in our workshops across the country, and enabled us to develop this Toolkit and the companion Primer (privacyph.org/primer) and Online Course (privacyph.org/course). We would also like to thank the institutions that endorsed the Project and whose workshops drove the development of this Toolkit: the National Privacy Commission (NPC) through Commissioner Raymund Enriquez Liboro; the Philippine Health Research Ethics Board (PHREB) through its Chair, Dr. Leonardo de Castro; and the Commission of Higher Education (CHED) through its Commissioner, Dr. Prospero de Vera.

Our sincere gratitude is also due to the universities that hosted the stakeholding and validation workshops: Mindanao State University-Iligan Institute of Technology and Mindanao State University-General Santos City; Silliman University (Dumaguete) and the University of San Carlos (Cebu); and the University of the Philippines Diliman and the University of the Philippines Baguio. We are most grateful to participants from the following institutions:

MINDANAO

Assumption College of Davao
Ateneo de Davao University
Bangsamoro Ministry of Health
Capitol University
Corazon Locsin Montelibano Memorial Regional Hospital
Cotabato City State Polytechnic College
Davao Medical School Foundation, Inc.
Department of Science and Technology-Region IX
Holy Trinity College of General Santos City
Iligan Medical Center College
Jose Rizal Memorial State University
Justiniano R. Borja General Hospital
Mindanao State University-General Santos City
Mindanao State University-Iligan Institute of Technology
Mindanao State University-Marawi
Pateros Catholic School
Philippine Science High School-Caraga Region Campus
San Agustin Institute of Technology
Southern Christian College
University of Science and Technology of Southern Philippines
University of Southeastern Philippines
University of the Immaculate Conception
University of the Philippines Diliman
Western Mindanao State University
Xavier University-Ateneo de Cagayan
Zamboanga City Medical Center

VISAYAS

Aklan State University
Cebu Doctors' University
Cebu Institute of Technology–University
Cebu Technological University
Chong Hua Hospital
Gov. Celestino Gallares Memorial Hospital
Holy Name University
Iloilo Science and Technology University
Negros Oriental State University
Silliman University
Southwestern University PHINMA
St. Paul University
University of Cebu
University of San Carlos
University of Southern Philippines Foundation
University of the Visayas
Velez College
Western Mindanao State University

LUZON

Adamson University
Ateneo de Manila University
Ateneo de Zamboanga University
Ateneo de Naga University
Baguio General Hospital and Medical Center
Bicol Regional Training and Teaching Hospital
Bicol University
Central Luzon State University
City College of Angeles
De La Salle University–Manila
De La Salle University–Health Sciences Institute
Lyceum University of the Philippines–Manila
Mariveles Mental Hospital
Makati Medical Center
Northwestern University
Philippine Children's Medical Center
Saint Paul University
San Lazaro Hospital
University of Asia and the Pacific
University of Luzon
Veterans Regional Hospital
University of Northern Philippines
University of Saint Louis–Tuguegarao
University of Santo Tomas
University of the Philippines Baguio
University of the Philippines Diliman
University of the Philippines Los Baños
University of the Philippines Manila

We are thankful to these institutions' research directors, researchers, ethics committee members, and other stakeholders who contributed their time, concerns, questions, suggestions, and ideas. Engagements with the participants in previous workshops with PHREB, the Department of Health (DOH), and the Philippine Social Science Council (PSSC) have also been beneficial for this Toolkit's development. Special thanks are due to Roren Marie Chin, who provided exceptional assistance with the earlier DOH workshops and later with her work at the NPC, for arranging collaborations with the Commission.

We are grateful to Atty. Ivy Patdu, former Deputy Commissioner of the NPC, for her guidance on the initial PIA Worksheets and other templates. She also endorsed us to the Office of the Australian Information Commissioner (OAIC), which graciously granted us an opportunity to interview its officers and shared with us their templates. The NPC's own toolkit has been the baseline document for this Toolkit, and our research ethics review forms have incorporated elements from those of the National Ethics Committee (NEC), UPM Research Ethics Board (UPMREB), and UPD CSSP Research Ethics Committee. Our thanks are due to them as well.

Finally, we would like to thank the Social Sciences and Philosophy Research Foundation, Inc. (SSPRF) and its President, Dr. Grace H. Aguiling-Dalisay, for their unwavering trust and support to the Project; and Helen Fabrero, Fernand Francis Hermoso, and Ross Kline Empleo for reviewing the manuscripts.

CONTENTS

01 INTRODUCTION

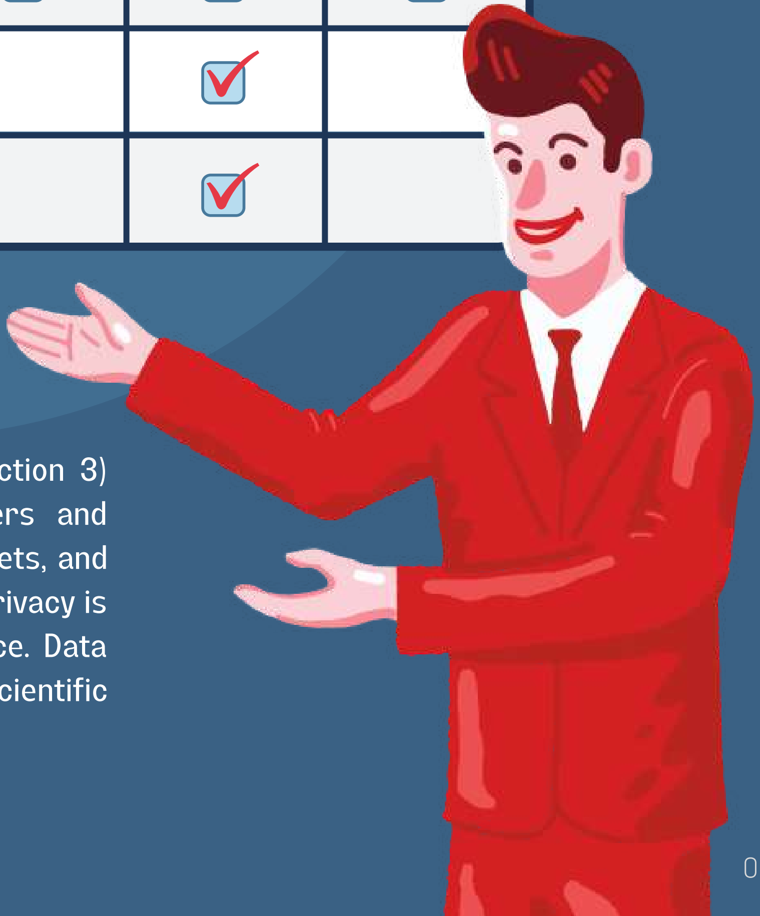
The Data Privacy Toolkit for Research Involving Human Participants is designed to guide researchers and research organizations in upholding the data privacy rights of research participants in accordance with the Data Privacy Act of 2012. This Toolkit comes with a companion Primer (privacyph.org/primer) and Online Course (privacyph.org/course). If you are unfamiliar with data privacy issues in research, we strongly recommend first perusing the Primer or taking the Online Course before you use this Toolkit. This Introduction aims only to provide an overview of the templates, worksheets, and forms found herein.

Properly appreciated, data privacy protection is a context-dependent, context-sensitive, thoughtful process—there is no "one size fits all" template that would apply to every situation. This process may vary from one context to another. Special tools are therefore needed to account for the contextuality of health and social research involving human participants. Developed to address such a need and seeking to aid researchers, research ethics committees, research project leaders, and research institutions in handling privacy issues and concerns, this Toolkit offers practical guidance in the conduct and evaluation of research involving human participants. Note, nonetheless, that context is everything; thus, however useful this Toolkit may be, researchers, research project leaders, and research institutions may still have to improvise to meet their precise needs.

In developing this Toolkit, we specifically have in mind the following *primary* users of the different templates, worksheets, and forms:

	Researchers	Research Directors	Ethics Reviewers	Project Leaders, Dept. Heads
Privacy by Design (Section 2)	✓	✓	✓	✓
PIA Worksheets (Section 4.1)		✓		✓
Privacy Management Plan (Section 4.4)	✓	✓	✓	✓
Data Breach Response (Section 4.5)	✓	✓	✓	✓
Consent (Section 4.2)	✓	✓	✓	
Data Sharing Agreement (Section 4.3)	✓	✓	✓	✓
Informed Consent Assessment (Section 4.6.1)	✓		✓	
Research Proposal Assessment (Section 4.6.2)	✓		✓	

Figure 1. *Intended primary users of this Toolkit.*



Ideally, the Data Protection Officer (see Section 3) takes the lead in engaging all researchers and stakeholders with these templates, worksheets, and forms—helping them understand that data privacy is an encompassing concern *beyond* compliance. Data privacy is essential to *public trust* in the scientific enterprise.

Central to privacy protection is the concept of "privacy by design" that needs to be imbibed in your entire organizational life. Your Data Protection Officer (DPO) and their team have to see to it that such a concept is understood especially by the people processing personal data.

Privacy by Design & Privacy Impact Assessment

Privacy by Design (PbD) (Section 2), especially in large research organizations, entails having a proactive, competent Data Protection Officer. For certain organizations, conducting periodic Privacy Impact Assessments (PIA), obtaining serious commitments from senior management and administration as well as significant buy-ins from stakeholders are consequential advantages of having a competent DPO. PIA is an internal process or mechanism aimed at addressing privacy issues and concerns. Conducting a PIA (worksheets found in Section 4.1[2]) is necessary to come up with a robust Privacy Management Plan (Section 4.4).

With increasing international collaboration among researchers and advanced research done across state borders, we also added another layer of prescribed qualifications from other territories (such as the US and the EU) on top of those from the National Privacy Commission (NPC).

[2] "Live" versions of the PIA Worksheets are available at privacyph.org/piaworksheets. Note that if it's your first time to use the PIA Worksheets in this Toolkit to do your first PIA, use Worksheets 4.1.1-4.1.6 sequentially. Before using Worksheet 4.1.7, use the forms in Sections 4.4 and 4.5. This way you'll have solid PIA as the basis for your organization's Data Privacy Manual.

If you're in a hurry and are already familiar with data privacy principles discussed in our Primer (privacyph.org/primer), check out our Compliance Matrix (Appendix A). This provides a quick view of the things you need for compliance purposes. Otherwise, read on and see how you can use the tools included here to thoughtfully consider your situation and get your organization to comply with the regulations. Unless the template or form is self-evident, instructions are provided.

PIA is an organization's systems, programs, processes, and procedures involved in the processing of personal information. Ideally led by the DPO, the conduct of a PIA is best done in the form of a workshop and must be participated in by the heads of the organization's units involved in processing personal data, as well as by important stakeholders. To get started, it is highly recommended that the PIA workshop participants or privacy impact assessors read our Data Privacy Primer (privacyph.org/primer) for a general overview of the Data Privacy Act of 2012 as it applies to research involving human subjects. The Toolkit provides templates as examples. Such templates are meant to help organizations conduct a Privacy Impact Assessment with key personnel and stakeholders as well as come up with appropriate privacy rules and plan of action. It is recommended that the forms be answered in the following sequence: Personal Data Inventory; Consent; Data Use and Disclosure; Data Sharing; Assessing Privacy Risks; then Risk Treatments, Controls, Actions.

Personal Data Inventory. The first step in Privacy Impact Assessment is the identification or inventory of the personal data that you keep or process. The collection of personal data will be easier when you have the forms and documents used to collect personal data within and outside of your organization. In the case of research projects, such forms may include survey questionnaires, interview guides, and project employee forms. The worksheet in Section 4.1.1 helps you take stock of the personal data holdings of your programs, projects, systems, and so on. Key personnel must fill out the table with some (if not all) of the 18 personal data types including name, address, age, religious and educational affiliations, ethnic origin, political association, biometrics (e.g., fingerprints, iris scans, faceprints) as well as unique identifiers issued by government agencies (e.g., TIN, UMID, Driver's License, Passport, GSIS or SSS, or Voter's Registration number). IP addresses and MAC addresses are also unique identifiers that can be inventoried.

Consent. In most research, consent is required for the valid collection, use, or disclosure of personal data. The worksheet provided in Section 4.1.2 helps ensure that the consent process involved is compliant with privacy regulations. To use the Consent Worksheet properly, one will have to mark the appropriate column (yes or no) where applicable. After marking the appropriate column, PIA workshop participants or privacy impact assessors may then give a brief explanation or comment on why (or why not) such a scenario does (or does not) apply.

Here, an assessment of the consent-taking process observed by the organization for the collection and use of personal data needs to be distinguished from the prescribed consent template in Section 4.2. The latter is for specific research proposals that research ethics committees will review.

Data Use And Disclosure. PIA participants need to be able to identify the primary and secondary purposes for which the collection of personal data is done. The researcher must not collect or use more personal data than what is necessary to meet their declared purposes. In case personal data are being collected, used, or disclosed for a secondary purpose, Worksheet 4.1.3 requires that the researcher also specify or describe such secondary purpose in relation to the primary purpose that research participants have consented to. The worksheet also encourages PIA participants to propose rules that can be incorporated into the organization's Data Privacy Manual. [3]

Data and Records Management. With institutions holding various analog and digital records of their activities and transactions, they must have a systematic plan for the retention and disposal of such records. Improper or inadequate storage of records can lead to leakages and data breaches, [4] which may threaten the privacy and security of data subjects. These security threats range from human neglects and errors to natural disasters and electronic malware. To mitigate these, institutions need to have physical, technical, and organizational privacy and security measures applied to their programs, practices, or systems. The worksheet provided in Section 4.1.4 examines the sufficiency of the safeguards placed

[3] See also Appendix: Compliance Matrix. To draft your organization's privacy manual, you may use the outline at privacyph.org/draftmanual

[4] A breach is any unauthorized or accidental access, alteration, disclosure, or destruction of personal data.

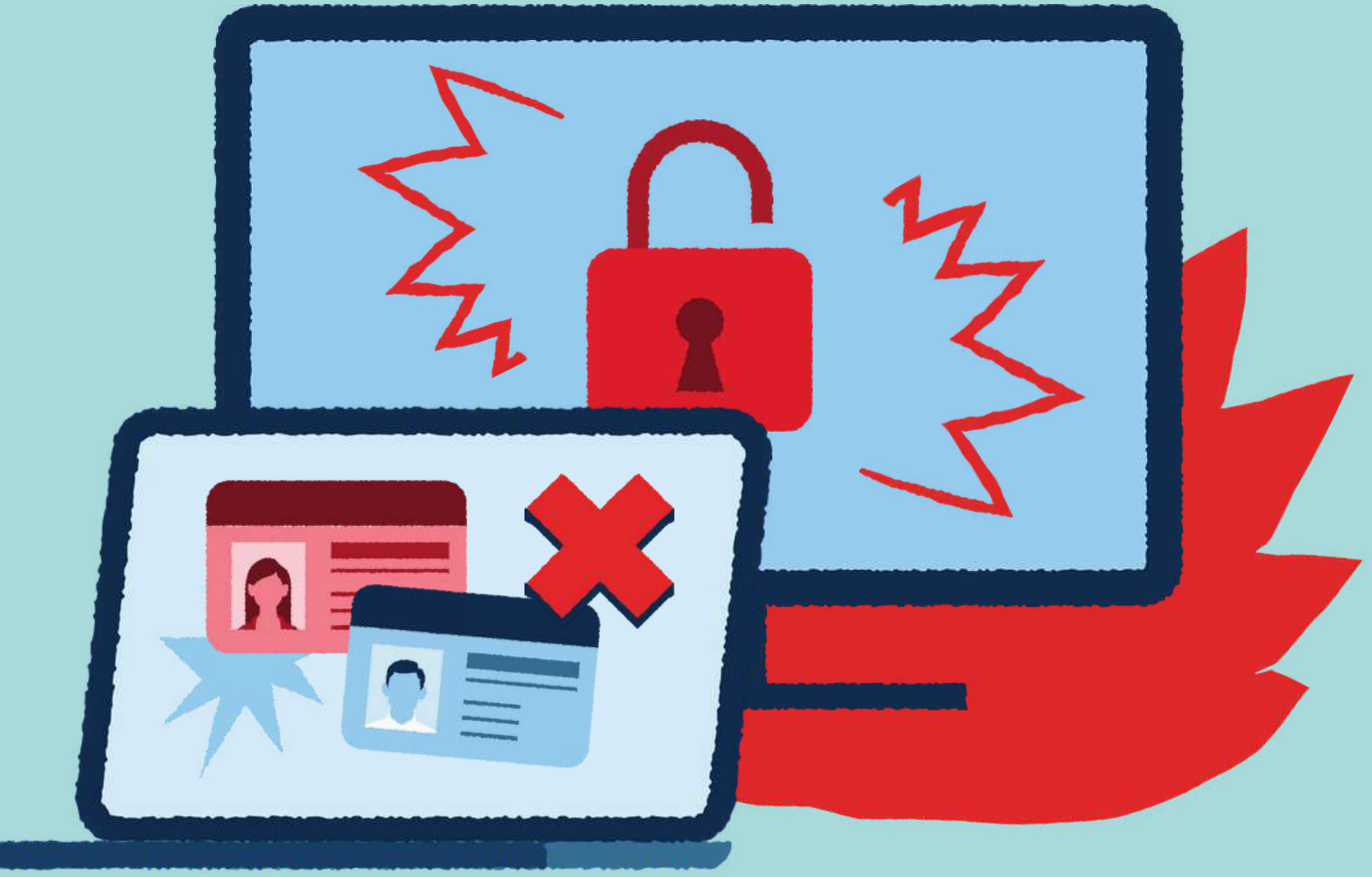
throughout the entire data life cycle. This Worksheet includes the identification of the type, value, and risk level of the information your organization will be handling so you can organize them according to your archival and records management system. Special attention is also given to records disposition schedules.

Data Sharing. The worksheet in Section 4.1.5 ensures that the data sharing agreements[5] entered into by the researcher or the research institution provide sufficient privacy protection or are in compliance with the law. Here, the focus is the practice and the general terms and conditions used in the data sharing arrangements made.

Assessing Privacy Risks. A privacy risk assessment is about being able to determine and quantify the data privacy risks involved in the collection and use of personal data. Worksheet 4.1.6 requires PIA workshop participants and key personnel to fill out the columns pertaining to the project, program, or system's data flow. After completing the section on data flow, the PIA workshop participants may then identify the threats to the personal data collected and used by your organization. Essentially, privacy risk assessment follows a similar pattern to standard risk assessments that typically involve identifying the risks, risk analysis, and risk evaluation and mitigation.

- ***Identifying the risks***. This step involves the identification of risks to the personal data collected if a privacy breach were to occur. These risks include, but are not limited to, the disappearance of personal data, unwanted change of personal data,

[5] As defined in Sec. 3 of NPC Circular 16-02, a data sharing agreement refers to any contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties. A sample template for such an agreement is provided in Section 4.3 of this Toolkit.



change in processing, illegitimate access to personal data, and unavailability of legal or organizational remedies.

- ***Risk Analysis.*** After identifying the risks, the risk impact assessors have to pinpoint their elements, namely: (a) likelihood of the risk occurring, and (b) severity of such a risk (see Figure 2). Risk analysis enables you to determine threat levels to which your organization needs to respond accordingly. To calculate the threat level, the likelihood must be multiplied by the severity of the risks.

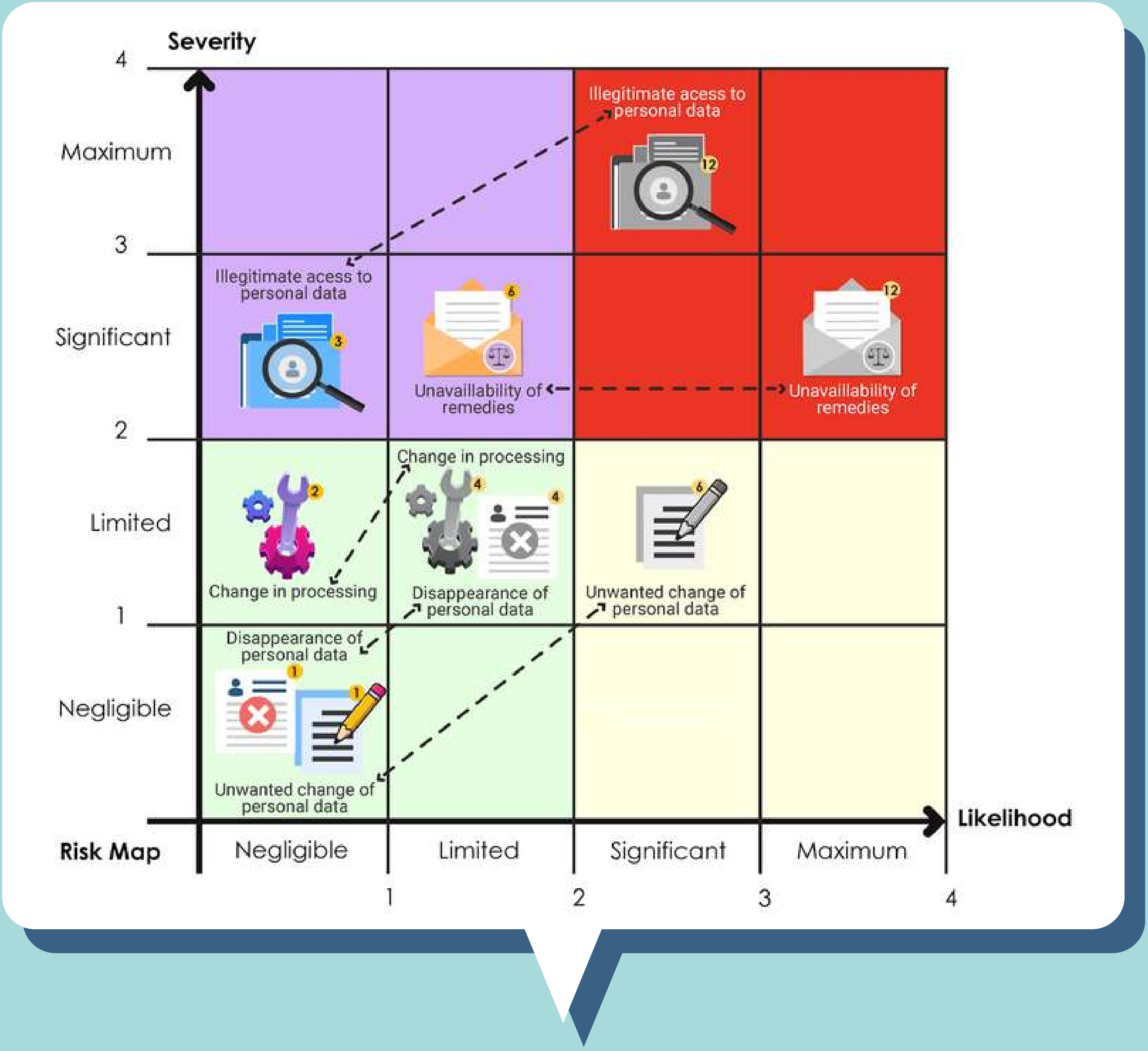


Figure 2. *Risk Map.*[6]

Privacy risks are levels of severity (harm) multiplied with degrees of likelihood (probability). Illegitimate access, unavailability of legal or organizational remedies, changes in processing, disappearance of personal data, and unwanted change of personal data are examples of risks that may be negligible, limited, significant, or maximum. They can go up or down the scale (value or weight), depending on the way these risks are treated or addressed.

[6] Cf. Commission Nationale de l'Informatique et des Libertés. (2012). Methodology for Privacy Risk Management: How to implement the Data Protection Act. https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

However, this risk formula should not give us any false sense of accuracy. It merely emphasizes the need to get a quantified, systematic sense of the privacy risks our organizations are exposed to, allowing us to provide the appropriate, proportional response. Any appreciation of risk is, in part, a function of knowledge of such a risk. With data privacy, ignorance is not bliss.

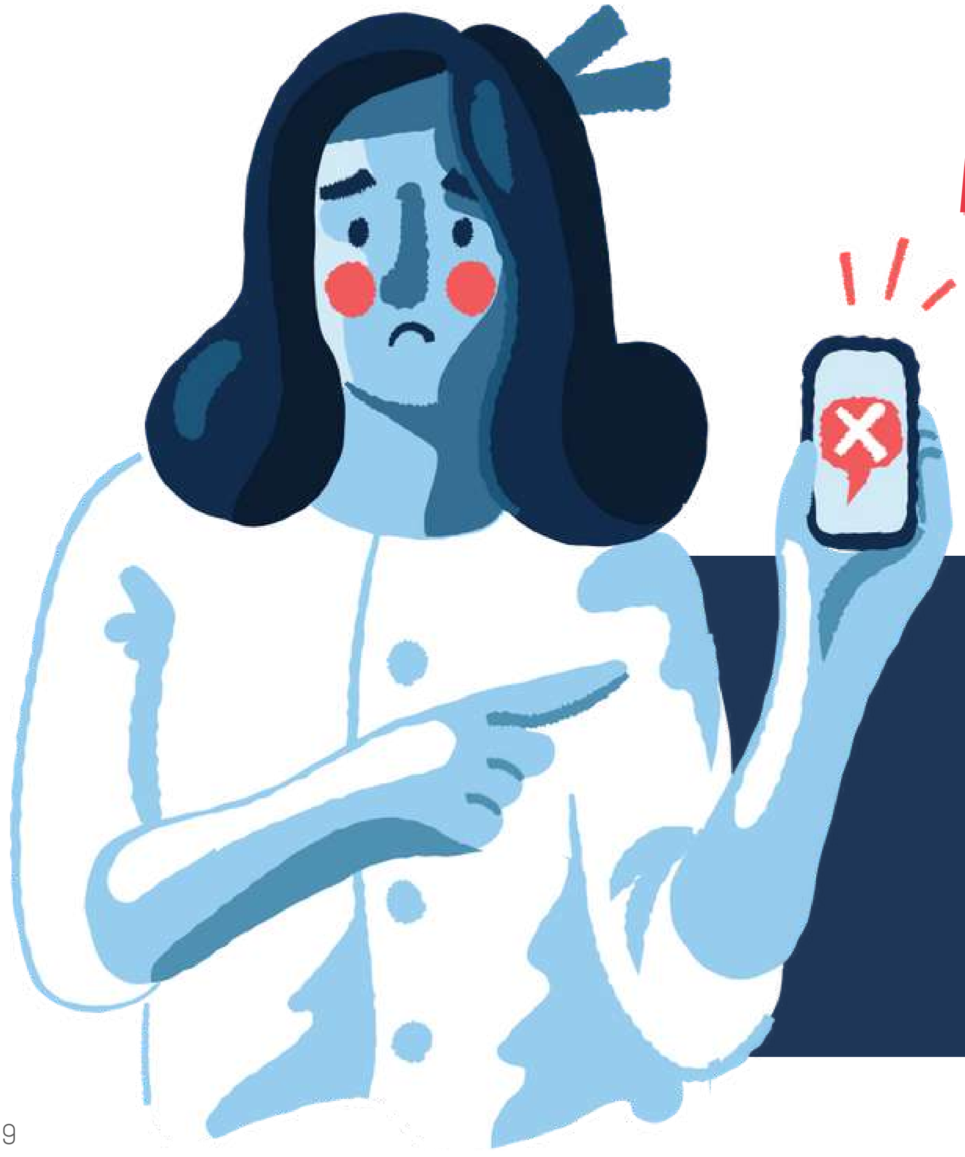
Once the privacy threat level is calculated, it can be categorized into different tiers. These tiers may range from negligible to maximum and all values in between. There will usually be varying degrees of risk depending on the context and specific data sets of the project, program, or system. It is incumbent upon the privacy impact assessors to make sense of the risk factors in their own settings.

- ***Risk Evaluation and Mitigation.*** Once the threat, vulnerability, impact, and likelihood have been determined, risk assessors can start identifying mitigating measures necessary to address the issues. See, for instance, Figure 2, where the unavailability of legal or organizational remedies (significant to maximum) for data subjects poses greater risk than changes in data processing (negligible to maximum). The organization would have a clearer picture of what and where they should implement its risk mitigation strategies. Taking into account the risk rating of a breach, available resources of an organization, and the latest data privacy practices, risk assessors should be able to gauge the best mitigation measures to implement and in what data processing stage it should be placed. An accountable person should be monitoring the mitigating measures as practiced or implemented, and review their results.

Once you are done with the risk assessment stage of the PIA and you have your risks identified, analyzed, and marked for mitigation, you are ready to treat such risks through your organizational controls and actions.

Risk Treatments, Controls, Actions. The researcher and research institution must take reasonable steps to keep the data secure. What is reasonable may vary from one organization to another, depending on its size and organizational complexity as well as on the nature and extent of risks faced. Aside from the risks identified, the privacy assessor must also identify the existing controls to treat the risks, if any, and propose mitigation measures or actions. Worksheet 4.1.7 is for the last stage in a general assessment of the current data privacy and security situation in your organization. The assessment prepares you to take appropriate steps in protecting personal information from misuse, loss, unauthorized access, modification, or disclosure. It is a direct input to your organization's Privacy Management Plan and Privacy Manual. (For other compliance requirements, see also Appendix: Compliance Matrix.)

In the conduct of a PIA, risk assessors should also be aligning their work with the organization's Privacy Management Plan (PMP) that includes a breach response protocol. The data gathered from the PIA exercise would be good baseline information in the formulation of a sound PMP.



Privacy Management Plan & Data Breach Response

A Privacy Management Plan is a document that identifies specific, measurable goals and targets in your organization's data privacy practice. Section 4.4 expounds how exactly the plan will be implemented using the following four-step process:

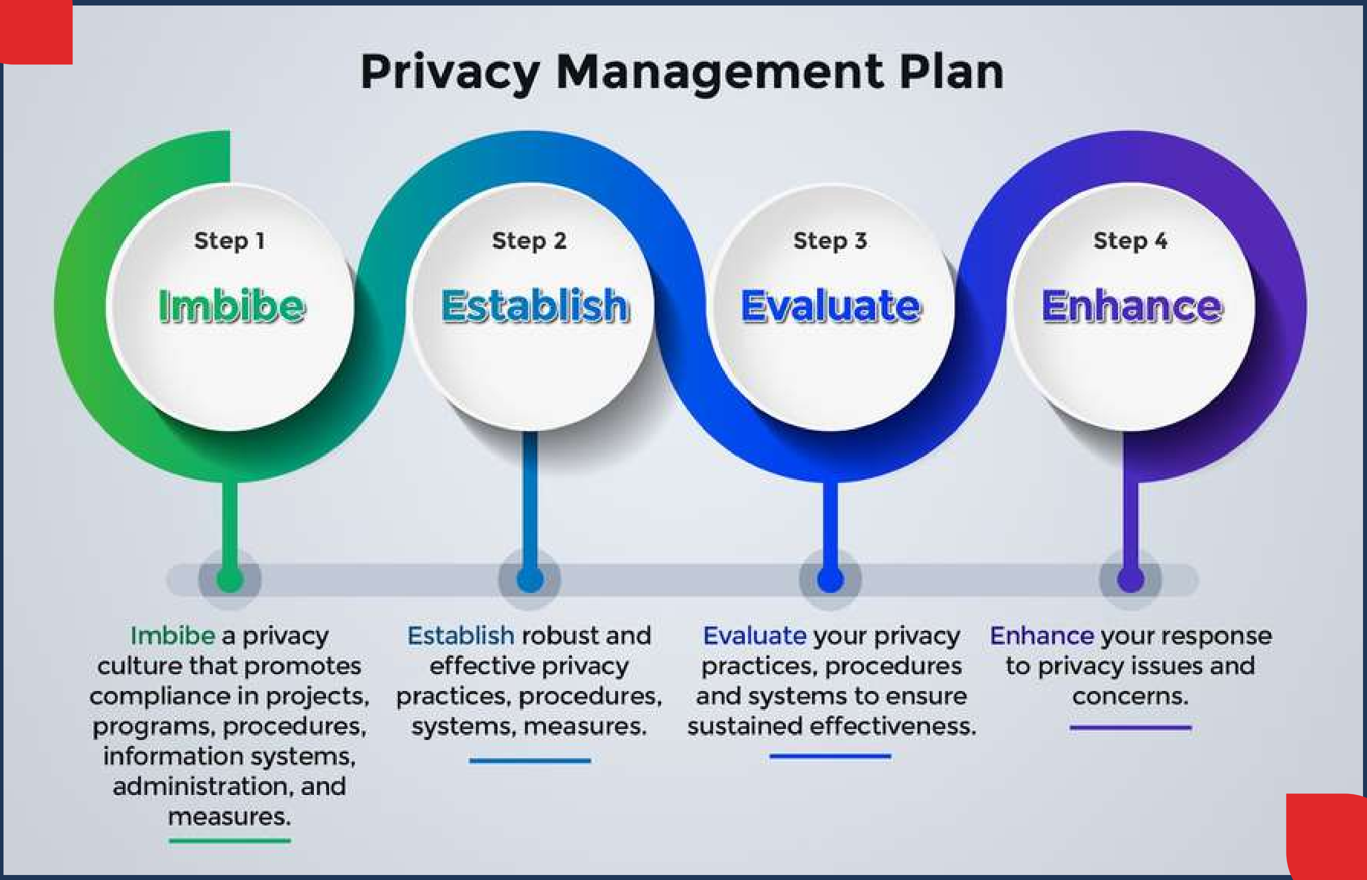

Privacy Management Plan
Step 1
Imbibe
Step 2
Establish
Step 3
Evaluate
Step 4
Enhance
Imbibe a privacy culture that promotes compliance in projects, programs, procedures, information systems, administration, and measures.
Establish robust and effective privacy practices, procedures, systems, measures.
Evaluate your privacy practices, procedures and systems to ensure sustained effectiveness.
Enhance your response to privacy issues and concerns.

Figure 3. Privacy Management Plan.[7] *A 4-step process of planning and managing effective privacy practices, measures, and responses in view of compliance requirements.*

1

Step 1 is to *imbibe* a privacy culture in an institution. Using Privacy by Design (PbD) tenets, institutions must appoint a DPO who works with top management and stakeholders to put in place mechanisms for privacy protection in all levels of the organization, and coordinates with the National Privacy Commission (NPC) and other privacy-related authorities.

[7] Cf. Office of the Australian Information Commissioner. (2016, May 16). Privacy management plan template (for organisations). OAIC. https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-plan-template-for-organisations/

Step 2 is to *establish* robust and effective privacy systems and measures. Through the concerted efforts of the DPO, and the administration, privacy workshops should be organized to stay updated with the requisite competencies for data privacy. An inventory of the privacy risks should be taken. Adequate privacy measures must be implemented and need to be codified in the form of an Organizational Privacy Manual so the staff can be guided accordingly.

2

Step 3 is to *evaluate* the research institution's privacy practices to ensure sustained effectiveness. The institution must provide a channel where the staff can provide feedback regarding the applied security measures and protocols. Documentation of feedback should be done by the DPO's team. Results from the analysis can be used to improve on the institution's privacy response.

3

Step 4 is to *enhance* the institution's response to privacy issues and concerns. Along with evaluations from the institution's staff, an external figure should also assess all privacy mechanisms and identify areas for improvement. The DPO's team must monitor the latest privacy laws and technologies, examine the implications of such developments, and introduce those that will minimize the risks to the institution.

4

Useful during and after PIAs, the template (Section 4.4) contains four forms: one for each step. Each form provides for specific actions to be implemented in line with the given step and in compliance with the Data Privacy Act. The second column of each form requires the planners and managers to input the position (e.g., Data Privacy Officer, Personal Information Controller, etc.) in the institution that will be responsible for the implementation of such actions. A column is also provided for the due date to execute such actions.

Data Breach Response. Researchers, project leaders, and research institutions must take reasonable steps to guard against data breaches. A protocol for dealing with the aftermath of a possible breach incident needs to be put in place. A Data Breach Response Questionnaire (Section 4.5) is provided to help responders identify if the organization has the means to detect data breaches and deal with their effects. Planners, managers, and data breach responders will mark the appropriate column (yes or no) depending on whether the given data breach response requirement is present in their projects, programs, and systems. After marking the appropriate column, they may also provide an explanation or comment on why (or why not) such a data breach response is (or is not) present.

Once you are organizationally prepared to deal with privacy issues and concerns as well as with possible data breaches (as demonstrated in your PMP, privacy manual, and breach response protocol), you look now to “where the rubber meets the road”: the review of research proposals done on both technical and ethical grounds. Research ethics review is specifically where you would want to discuss your privacy compliance requirements as well.

Research Ethics Review Process & Research Proposal Evaluation

Privacy protection in research settings works hand in hand with the research ethics review process. While there is a general mechanism to protect personal data at the institutional level, at the end of the day, it is the research ethics review that keeps the balance between advancement of knowledge and safe and ethical use of personal data.

Just like an ethics review, a privacy review is a review of documents. The review requires a thorough understanding of the research proposal or project based on the documents submitted. As for the research proposal or protocol, it is incumbent upon researchers to demonstrate familiarity with (if not mastery of) the privacy issues and concerns in their projects. Such familiarity or mastery will be the basis for a fair review of the research project. To aid the researcher and the ethics reviewer, the subsequent subsections provide two review forms on consent and proposal. These forms (or some other iterations) are already being used in many parts of the country. We are simply extending them to include privacy concerns into the screening.

Some research ethics committees tend to be hyper-focused on informed consent documents, forgetting that the process needs to be complemented by an independent risk analysis. Physical, psychological, social, dignitary, and privacy harms as well as how likely they are to occur in the context of a particular research project—these are the overall considerations in the assessment of the informed consent process and the research proposal itself. We have especially incorporated in our evaluation instruments some essential tracer questions for data privacy.

- ***Informed Consent Assessment Form.*** As part of the consent process, informed consent forms provide prospective research and data subjects with a detailed and focused explanation of the research project. It is supposed to explain the possible risks and benefits to research participants. Privacy measures aimed at managing risks must be stated as well. Reviewers can use the assessment tool to ensure that the research subjects fully know the extent of their participation in the research process and that their consent is legitimately obtained.

- ***Research Proposal Assessment Form.*** Research proposals detail their objectives and study significance as well as their methodological plan and theoretical framework. This form (Section 4.6.2) is designed to gauge whether a proposal is aligned with national ethical principles and data privacy standards and protocols. Reviewers can use the form to ensure that the research proposal reflects scientific and ethical soundness. The proposal shall also articulate data protection measures. The researchers or study proponents may improve upon the final proposal based on the results of the assessment. Supplementary review tips for proposals are available at privacyph.org/researchreviewtips.

All things considered, using this Toolkit is a balancing act between safely facilitating scientific research and protecting the privacy rights of research participants. The tools and templates may be perceived as labor-intensive or excessively detailed, but when used judiciously and efficiently, the Toolkit can help researchers, project leaders, and research institutions ensure the data privacy protection of their research participants. With this Toolkit, maintaining proportionality in such exercises (i.e., riskier research projects entail greater privacy review) necessitates streamlining the research process and mitigating any lapses. It is our fervent hope that this Toolkit will be an effective means in advancing safe and privacy-aware scientific research.

Whatever lingering concerns or questions you may have on the forms, worksheets, or templates herein, you may raise through our Q&A page at privacyph.org/qanda.

02 PRIVACY BY DESIGN IN RESEARCH[8]

Privacy by Design (PbD) is an approach characterized by privacy as a default setting throughout the whole lifecycle of information. PbD entails that data privacy is embedded or integrated into the design of:

- technologies,
- business processes,
- operations,
- procedures,
- information architecture, and
- information systems.

By making data privacy the *default* choice in systems, processes, projects, and programs, PbD emphasizes the prevention and mitigation of privacy breaches more than remedies to these incidents. PbD acknowledges the need to commit to strong privacy practices based on standards and susceptible to review.

Operationally in research institutions, PbD entails having at least a data protection officer; a privacy management plan, including robust data management; privacy-oriented research proposals or protocols; and privacy-trained, privacy-protecting human resources.

Data Protection Officer (DPO)

An institutional DPO:

☐ Should have comprehensive knowledge on privacy practices as well as the sector where their organization functions;

☐ Conducts Privacy Impact Assessments (PIA) for the whole institution and research projects, including assessment of systems, processes, procedures, programs, and related projects;

☐ Updates management and compliance officers on the latest privacy laws and technologies;

☐ Provides training on privacy practices of the organization.

To know more roles and functions of the DPO, visit: privacyph.org/dpo.

[8] Updated 1 June 2021. Link to latest version: privacyph.org/pbdresearch. Send comments, suggestions to: psy@up.edu.ph

Privacy Management Plan

A Privacy Management Plan is designed to help organizations identify the goals and steps for complying with privacy protection laws. For the PMP template, visit privacyph.org/mgt.

Data Management

- ☐ Collection of data should be based on a specified purpose, limited to what is necessary, retained only until it has fulfilled its purpose, and then securely destroyed.
- ☐ Data with "expired" or non-valid consent should be properly de-identified and disposed.
- ☐ De-identification, pseudonymization, or anonymization of data sets should be practiced for proper release and sharing of data with researchers, analysts, journals, etc.
- ☐ De-identification practices are for scraping photos of Exchangeable Image Format (EXIF) sensitive records, for masking [9] sensitive data on videos, and for avoiding aggregate information that is potentially discriminating for certain marginalized groups.
- ☐ This entails end-to-end data security: full "data flow"/"information lifecycle" privacy protection.

Research Proposals/Protocols

- ☐ Inclusion of "Data Management Plan" section in the proposal. See privacyph.org/mgt.
- ☐ Inclusion of "Ethical Considerations" section that details, among others, the process of how informed consent is obtained from data subjects or a strong justification of why it should be waived or obtained in forms other than written or signed by research or data subjects.

Human Resources in Research [10]

- ☐ Inclusion of appropriate privacy policies in employment contracts and terms of reference.
- ☐ Orientation on privacy rules in on-boarding and off-boarding procedures.
- ☐ Inclusion of data privacy policies in employee manuals.

[9] Videos may contain seemingly benign but rather sensitive data (e.g., heart rates). See, for instance, Wu, Hao-Yu, Michael Rubinstein, Eugene Shih, John Guttag, Frédo Durand, and William Freeman. "Eulerian Video Magnification for Revealing Subtle Changes in the World." ACM Transactions on Graphics 31, no. 4 (July 1, 2012): 1–8.

[10] "Insiders" have been associated with the majority (58%) of recent data breaches (Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare Data Breaches: Implications for Digital Forensic Readiness. Journal of Medical Systems, 43(1). https://doi.org/10.1007/s10916-018-1123-2).

PRIVACY OFFICER / DATA PROTECTION OFFICER[11]

Qualifications

General Qualifications

☐ Specialized knowledge and skills necessary for the performance of duties and responsibilities specified below;

☐ Expertise in relevant privacy or data protection policies and practices;

☐ Sufficient understanding of the information processing operations (including information systems, data security needs) of the organization's personal information controller (PIC) and processors (PIP);

☐ Comprehensive knowledge and understanding of the sector or field in which the organization operates;

☐ Familiarity with the administrative functions of the privacy practice;

☐ Excellent communication, problem solving, and research skills;

☐ Strong interest in privacy laws and regulations;

☐ High integrity and detail oriented;

☐ Strong organizational skills and work well with management and staff;

☐ No conflict of interest: not an implementer of programs (other than privacy), nor an owner of business processes (other than those related to privacy).

Duties & Responsibilities

General Duties

- Be the advocate that maintains the privacy of research and data subjects;
- Oversee activities that keep the practice in compliance with rules that govern personal data (or the privacy of protected health information) in oral, written, and electronic form;
- Monitor the PIC/PIP's compliance with the DPA, its IRR, issuances by the NPC, and other applicable laws and policies;
- Document the processing operations, activities, measures, projects, programs, or systems of the PIC/PIP;

[11] This template incorporates provisions from NPC Advisory No. 2017-01 "Designation of Data Protection Officers" and HIPAA. Send comments, suggestions to: psy@up.edu.ph. Shortcut to this page: privacyph.org/dpo.

- Analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
- Inform, advise, and issue recommendations to the PIC/PIP;
- Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing;
- Advice the PIC/PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;
- Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC/PIP;
- Advise the PIC/PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);
- Ensure proper data breach and security incident management by the PIC/PIP, including the latter's preparation and submission to the National Privacy Commission (NPC) of reports and other documentation concerning security incidents or data breaches within the prescribed period;
- Inform and cultivate awareness on privacy and data protection within the organization of the PIC/PIP, including all relevant laws, rules and regulations, and issuances of the NPC;
- Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC/PIP relating to privacy and data protection, by adopting a Privacy by Design approach;
- Serve as the contact person of the PIC/PIP vis-à-vis data subjects, of the NPC, and of other authorities in all matters concerning data privacy or security issues or concerns and the PIC/PIP;
- Cooperate, coordinate, and seek advice of the NPC regarding matters concerning data privacy and security;
- Perform other duties and tasks that may be assigned by the PIC/PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.

Specific Duties

1. Management Advisor

Work with the management team and compliance officers to comply with laws governing the privacy of individually identifiable information. Stay current on privacy laws and updates in privacy technology. Immediately notify the management of requested investigations and reviews by authorized government agencies.

2. Human Resources and Training

Develop, or serve as team leader in the development of, the practice's privacy policies and procedures. Integrate those policies into the practice's day-to-day activities and provide training, either as on-the-spot refresher courses or planned courses. Oversee sanctions according to policies and procedures and bring them to the attention of the practice's leadership committee.

3. Risk Management

Collaborate with the security official to ensure that privacy and security risks are analyzed and policies and procedures are developed, updated, and enforced to prevent unauthorized disclosure of identifiable personal information.

4. Business Associates

Lead the practice of updating business associate contracts and, with the appointed lawyers, of developing and executing business associate agreements in accordance with the privacy laws and regulations.

5. Complaint Management

Implement and manage complaints regarding the practice's standards and protocols, including documenting and investigating and, if necessary, mitigating those complaints. Educate the workforce on the practice's policies and procedures on complaints and prohibited retaliatory actions against individuals who exercise their patient rights.

6. Other Duties in Special Settings

6.1. Patient Rights

Oversee patient requests to the practice and help the employees understand how to address patient questions about the practice's privacy initiatives. Develop an effective internal and external communications effort to help patients and the workforce understand how the practice protects patient rights.

6.2. Research Subject Rights

Help the research staff understand how to address research subjects' questions about research and science and the institution's privacy initiatives. Develop measures to help research subjects and research staff understand how they collectively and individually uphold privacy rights.

04 TEMPLATES

4.1 PIA Worksheets

4.1.1 Personal Data Inventory

Personal Data	Project/System/ Procedure/Admin 1	Project/System/ Procedure/Admin 2	Project/System/ Procedure/Admin 3
	Description Rabies Vaccination Project / Dog Owners Database / Aftercare Procedure / Health Division	Description Dental Work Project / Volunteer Dentists Database / Free Dental Service / Health Division	Description Community Dev Project / Volunteer Database / Tree Planting Activity / Environment Division
Name	Leonor B. Dagohoy		
Home Address	Mia Alta, Antipolo City, Rizal		
Business Address	Roxas Avenue, UP Diliman, Quezon City		
Email Address	lbdagohoy@health.com		
Contact Number (Home)	+6395 0000 0721		
Contact Number (Work)	+6395 0082 0721		
Age	34		
Date of Birth	21 February 1987		

Personal Data	Project/System/ Procedure/Admin 1	Project/System/ Procedure/Admin 2	Project/System/ Procedure/Admin 3
Marital Status	Single		
Color, Race, Ethnic Origin	Brown, Filipino, Tagalog		
Religion	Roman Catholic		
Education	Philippians University		
Photos (identifiable)	*1 x 1 photo here*		
Biometrics	*thumbmark here*		
Political Association	Liberal		
Health	N/A		
Sexual Life / Preference / Practice	N/A		
Offense(s) committed or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in such proceedings	N/A		

Issued by government agencies unique to an individual:			
Unique identifiers (e.g., TIN, UMID no., Driver's License no, Passport no., GSIS/SSS no., Voter's Registration no., etc.)	SSS no.: 45-8672723-9		
Previous or current health records	N/A		
Licenses or its denials, suspension, or revocation	N/A		
Tax returns	N/A		
Information specifically established by an executive order or an act of Congress to be kept classified	N/A		
Detailed narratives or information that may point to identifiable individuals	Owns a two-tailed Japanese Spitz named Whitey		
Others. Please add as many as being collected.	N/A		

4.1.2 PIA Worksheets

Consent

Instructions

1. Fill the appropriate cells on the Prelims / Transparency / Proportionality / Collection sections in relation to your responses in Sec. 4.1.1.

2. Mark the appropriate column (yes or no) depending on whether or not the given circumstances apply to the project/program/system.

3. After marking the appropriate column, the user is also tasked with giving an explanation or comment on why the given circumstance applies (or does not) to the project/program/system.

Prelims

	Yes	No	Explanation/Comment
Will the project involve the collection of new information about individuals?		X	The project will gather information readily available from WYZ's database.
Is the information about individuals likely to raise privacy concerns or expectations, e.g., health info, or other information people would consider particularly private?			
Will you be using information about individuals for a purpose that it is not currently used for, or in a way it is not currently used?			
Will the initiative require you to contact individuals in ways which they may find intrusive?			
Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?			
Does the initiative involve you using new technology which might be perceived as being privacy intrusive, e.g., biometrics or facial recognition?			

	Yes	No	Explanation/Comment
Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?			

Transparency

	Yes	No	Explanation/Comment
Are data subjects aware of the nature, purpose, and extent of the processing of their personal data?	✓		The data subjects are aware and they consented that their data be used for the project.
Are data subjects aware of the risks and safeguards involved in the processing of their personal data?			
Are data subjects aware of their rights as a data subject and how these can be exercised?			
Is there a document available for public review that sets out the policies for the management of personal information? Please identify the document(s) and provide link(s) where available.			
Are there steps in place to allow an individual to know what personal information the program holds about them and for what purposes it is collected, used, and disclosed?			

Proportionality

	Yes	No	Explanation/Comment
Is the processing of personal information...			
• Adequate	✓		The consent document indicates collection of data proportionate to the purpose declared.
• Relevant			

	Yes	No	Explanation/Comment
• Suitable			
• Necessary, and			
• Not excessive in relation to the declared and specified purpose?			
Is personal information being processed because the purpose of the processing could not be reasonably fulfilled by other means?			

Collection

	Yes	No	Explanation/Comment
Is the collection of personal information done for a declared, specified, and legitimate purpose?	✓		The collection is in line with what is agreed upon in the informed consent form.
Is individual consent secured prior to the collection and processing of personal data?			
Is consent time-bound in relation to the declared, specified, and legitimate purpose?			
Can consent be withdrawn?			
Is all the information collected necessary for the program?			
Is it not possible for the individual to remain anonymous for the purpose of the program?			
Is the information being collected directly from the individual?			
Will any information also be collected indirectly about the individual?			
Will this program assign or collect unique identifiers? Is it necessary to assign a unique identifier to individuals to enable your organization to carry out the program?			
Will a unique identifier of another agency be used?			

4.1.3 PIA Worksheets

Data Use & Disclosure

Instructions

1. Fill the appropriate cells on the Data Use and Disclosure / Another Organization / Data Quality / Collection sections in relation to your responses in Sec. 4.1.1.

2. Mark the appropriate column (yes or no) depending on whether or not the given scenario regarding data use and disclosure applies to the project/program/system.

3. After marking the appropriate column, the user is also tasked with giving an explanation or comment on why such a scenario applies (or does not) to the project/program/system.

4. For the Proposed Rules section, present appropriate use and disclosure rules that your institution should implement.

Data Use and Disclosure

	Yes	No	Explanation/Comment
Personal information will only be used or disclosed for the primary purpose identified.	✓		Information of the data subjects shall only be used for the creation of a database on dog owners in Brgy. Z
Personal information will also be used or disclosed for a secondary purpose.			
If using personal information for a secondary purpose, which of the following applies?			
• The individual has consented to the use or disclosure.			
• The secondary purpose is related to the primary purpose.			
• The individual would reasonably expect the organization to use or disclose the information for the secondary purpose.			

	Yes	No	Explanation/Comment
• It is necessary for research, or the compilation or analysis of statistics in the public interest. If yes, please explain.			
• To lessen or prevent a serious and imminent threat to an individual's life, health, safety, or welfare.			
• To lessen a serious threat to public health, public safety, or public welfare.			
• On suspicion or unlawful activity as part of reporting its concerns to relevant persons or authorities.			
• As required or authorized by law. (Please cite the relevant law)			

By Another Organization

	Yes	No	Explanation/Comment
Will this program use or disclose a unique identifier assigned to an individual by another organization?		X	The identity of the subject is not necessary for the project. Thus, the anonymization measures used in the previous research will not be used. The project shall use a new measure to prevent subjects from being identified.
The unique identifier assigned to an individual by another organization will be used and/or disclosed only when:			
• The individual has consented.			
• It is necessary for the organization to fulfill its obligation to the other organization.			
• There is a serious threat to individual or public health, safety, or welfare.			
• Upon the request of a government agency to monitor unlawful activity or as part of an investigation.			
• It is required or authorized by law.			
	If YES, please cite the relevant law.		

Data Quality

	Yes	No	Explanation/Comment
Please identify all steps taken to ensure that all data that is collected, used, or disclosed will be accurate, complete, and up to date.			
• Information was obtained from a reputable source such as another government agency.	✓		List of dog owners was secured from Brgy. Z
• The system is regularly tested for accuracy.			
• There is periodic review of the information.			
• A retention schedule is in place that deletes information that is over a certain period.			
• Staff are trained in the use of the tools and receive periodic updates.			
• Reviews of audit trails are undertaken regularly.			
• There is independent oversight.			
• Incidents are reviewed for lessons learnt and systems/processes updated appropriately.			
• Others, please specify.			

Proposed Rules

Use Rules	Disclosure Rules

4.1.4 PIA Worksheets
Data & Records Management

Instructions

1. Fill the appropriate cells on the Data Security / Record Management sections in relation to your responses in Sec. 4.1.1.

2. Mark the appropriate column (yes or no) depending on whether or not the project/program/system has taken the given steps pertaining to data security and records management.

3. After marking the appropriate column, the user is also tasked with giving an explanation or comment on why the project/program/system has (or has not) taken such steps.

4. For the Proposed Rules section, present appropriate security and records management rules that your institution should implement.

> You may take suggestions from Rule IV "Organizational Security Measures", Rule V "Physical Security", Rule VI "Technical Safeguards", Rule VII "Cloud Services", and Rule VIII "Use of Social Media" of the Health Privacy Code.[12]

Data Security

	Yes	No	Explanation/Comment
The program has taken reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure.	✓		
If yes, which of the following has the program undertaken to protect personal information across the information lifecycle:			
• Identifying and understanding information types.			

[12] Department of Health, Department of Science and Technology, and Philippine Health Insurance Corporation. (2016).Health Privacy Code of Joint Administrative Order No. 2016-0002. DOH. http://ehealth.doh.gov.ph/images/HealthPrivacyCode.pdf.

	Yes	No	Explanation/Comment
• Assessing and determining the value of the information.			
• Identifying the security risks to the information.			
• Applying security measures to protect the information.			
• Managing the information risks.			

Record Management

	Yes	No	Explanation/Comment
The program will take reasonable steps to destroy or de-identify personal information if it is no longer needed for any purpose.			
	If YES, please list the steps:		

Proposed Rules

Organizational	Physical	Technical	Cloud Services	Social Media

4.1.5 PIA Worksheets

Data Sharing

Instructions

1. Fill the appropriate cells on the Cross-Border section in relation to your responses in Sec. 4.1.1.

2. Mark the appropriate column (yes or no) depending on whether or not the given items pertaining to cross-border data sharing apply to the project/program/system.

3. For the Proposed Rules section, present appropriate data sharing rules that your institution should implement (use "Proposed Rules").

Cross-Border

	Yes	No	Explanation/Comment
The program will transfer personal information to an organization or person outside of the Philippines		X	The project is solely Philippine-based. Also, the organization stated in the consent form that their data shall only be used in this project.
	If YES, please describe:		
Personal information will only be transferred to someone outside of the Philippines if any of the following apply:			
• The individual consents to the transfer.			
• The organization reasonably believes that the recipient is subject to laws or a contract enforcing information handling principles substantially similar to the DPA of 2012.			
• The transfer is necessary for the performance of a contract between the individual and the organization.			

	Yes	No	Explanation/Comment
• The transfer is necessary as part of a contract in the interest of the individual between the organization and a third party.			
• The transfer is for the benefit of the individual.			
• It is impractical to obtain consent.			
• If it were practicable, the individual would likely consent.			
The organization has taken reasonable steps so that the information transferred will be held, used, and disclosed consistently with the DPA of 2012.			
	If YES, please describe:		

Proposed Rules

Required Reporting	Access to Information	Patient Registry	Health Research

4.1.6 PIA Worksheets
Assessing Privacy Risks

Instructions

1. Fill the appropriate cells on the Data Flow section in relation to your responses in Sec. 4.1.1. Under the Data Flow section, supply the information related to the collection, use, disclosure, and disposal of personal data in the project/program/system.

2. Under the Threats section, identify and discuss the threats and vulnerabilities involved in the collection, use, retention, disclosure, and disposal of your personal data, which you provided in Sec. 4.1.1.

3. To score threats, vulnerabilities, or risks, please use the risk assessment matrix provided below.

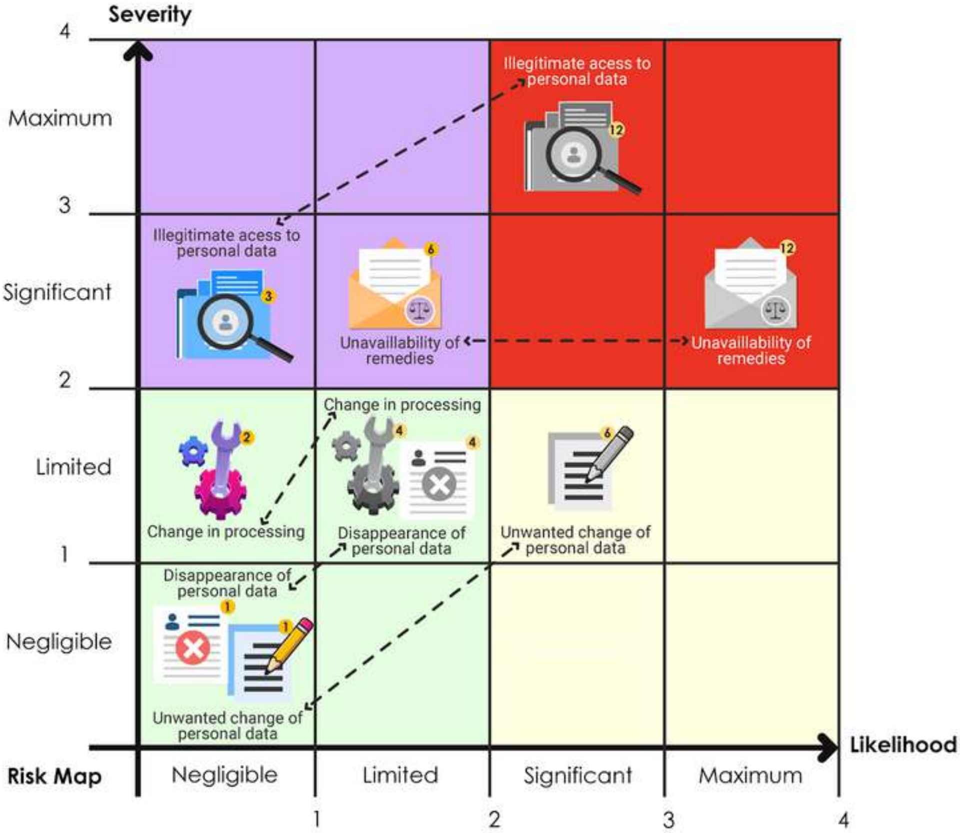
   a. There are two scales involved in the risk assessment matrix. The likelihood of the given risks are plotted on the x-axis, while the severity of the same risk is plotted on the y-axis.

   b. In order to calculate the risk level, the likelihood must be multiplied by the severity of the risks.

   c. Once the risk level is calculated, they can be categorized into different tiers. These tiers may range from negligible to maximum and all values in between.

4. For the Proposed Rules section, present rules that shall protect your OWN privacy (use "Proposed Rules").

Chart



Data Flow

Personal Data	Collect	Use	Disclose	Dispose
	By? From? How? When? Where? Why? Authority?	By? How? When? Where? Why?	By? From? How? When? Where? Why? Authority?	By? From? How? When? Where? Why? Authority?
Name	Collected by G org from Brgy. Z. G org sent a request to the barangay 5 months prior to the project that is to be conducted at the barangay's clinic. The period is to give them time to consider the request. The collection of names was authorized then by the barangay.	Names were used by G org to determine the number of participants for the project.	Disclosed by Brgy. Z to G org through email. Disclosure was authorized by the said barangay. The database was sent 3 months prior to the event.	Disposal of personal information shall be conducted by G org. The written and electronic records shall be properly disposed of and deleted after the project is finished. This shall prevent the participants from being identified. The disposal was authorized by G org.

Personal Data	Collect	Use	Disclose	Dispose
Home Address				
Business Address				
Email Address				
Contact Number (Home)				
Contact Number (Work)				
Age				
Date of Birth				
Marital Status				
Color, Race, Ethnic Origin				
Religion				
Education				
Photos (identifiable)				
Biometrics				
Political Association				
Health				
Sexual Life / Preference / Practice				
Offense committed or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in such proceedings				
Issued by government agencies unique to an individual:				
- Unique identifiers (e.g., TIN, UMID no., Driver's License no., Passport no., GSIS/SSS no., Voter's Registration no., etc.)				
- Previous or current health records				
- Licenses or its denials, suspension, or revocation				

Personal Data	Collect	Use	Disclose	Dispose
- Tax returns				
Specifically established by an executive order or an act of Congress to be kept classified				
DETAILED narratives or information that may point to identifiable individuals				
Others, please add as many as will be collected:				

Threats

	Threat	Vulnerability	Impact	Likelihood	Risk Rating
Collection					
Use					
Retention					

	Threat	Vulnerability	Impact	Likelihood	Risk Rating
Disclosure/ Sharing					
Disposal					

Proposed Rules

Role	Collection	Use	Disclosure	Disposal

4.1.7 PIA Worksheets

Risk Treatments, Controls, Actions

Instructions

1. From the risks identified in the Sec. 4.1.6., list the existing controls to treat the identified risks and write down additional proposed mitigation measures in response to said risks, if any.

2. Using the Privacy Management Plan template provided in Sec. 4.4, outline (under the Management Plan section of this worksheet) a Privacy Management Plan for your project/program/system.

3. Under the Most Significant Findings section of this worksheet, state the most significant privacy risk findings from your project/program/system and offer further recommendations to be applied in consideration of those findings.

4. After going through Sections 4.1.1–4.1.6, state your proposed rules for projects, programs, procedures, systems, admin divisions using this Draft Privacy Manual / Protocol Template (privacyph.org/draftmanual).

Threats

Personal Data	Risks	Rating	Existing Controls	Proposed Mitigation Measure (Justification)
General				
Collection				

Personal Data	Risks	Rating	Existing Controls	Proposed Mitigation Measure (Justification)
Use				
Retention				
Disclosure/ Sharing				
Disposal				

Most Significant Risk Findings

Summary of Most Significant Risk Findings	
Findings	Recommendations

Management Plan

Management Plan			
Imbibement of Privacy Culture	Establishment of Privacy Practices	Evaluation of Privacy Practices	Enhancement of Privacy Response

4.2 Informed Consent Form[13]

TITLE

STUDY PROPONENT/PRINCIPAL INVESTIGATOR
⊰⊰ State NAME and CONTACT INFO. ⊱⊱

CONFLICT OF INTEREST/COMPETING INTERESTS
Declaration
⊰⊰ There are no conflicts of interest to declare in relation to this study. ⊱⊱

⊰⊰ Info on receiving financial payment from the Sponsor/Funder to cover the cost of conducting this study ⊱⊱

INTRODUCTION
You are being invited to participate in this study because ⊰⊰ explain the main features of the study population to which the research participant belongs, indicating as well as the sample size needed ⊱⊱. This consent form provides you with information to help you make an informed choice. Please read this document carefully. If you have any questions, they should be answered to your satisfaction before you decide whether to participate in this study.

STUDY BACKGROUND AND RATIONALE
⊰⊰ State why this study is being conducted. ⊱⊱

BENEFITS
⊰⊰ State the benefits of the study. Include monetary benefits if any. ⊱⊱

ALTERNATIVES TO THIS STUDY
⊰⊰ If the research subject chooses not to participate, what alternatives do they have, if any? ⊱⊱

ONE'S PARTICIPATION
⊰⊰ Describe the intervention for the study group. ⊱⊱

⊰⊰ Describe study procedures here involving the study participants. State possible expenses of the participant, if any. ⊱⊱

⊰⊰ For clinical trial: provide clear identification of experimental components of the study. ⊱⊱

[13] Updated: 9 June 2021. Shortcut to this form: privacyph.org/consent. Send comments, suggestions to: psy@up.edu.ph

⊰⊰ How long will one's participation last? ⊱⊱

⊰⊰ Can participants choose to leave the study? Without a need to explain themselves? Explain the consequence (if any) if they decline to participate. ⊱⊱

RISKS

⊰⊰ State risks (severity and likelihood) that the study may introduce into the situation or that may affect the study participants. Indicate compensation terms if a study-related incident were to occur. ⊱⊱

PRIVACY AND CONFIDENTIALITY

⊰⊰ How will participant information be kept confidential? Name the people who have legitimate access to the owner's data. Describe the data sharing agreement with the third parties, if any. ⊱⊱

⊰⊰ Describe briefly your plan to protect participants' privacy, especially your plan to mitigate potential unauthorized access or disclosure of personal information. Include a description of the physical and technical security measures you will conduct while keeping their data. ⊱⊱

RIGHTS

⊰⊰ Explain in plain language their rights as participants and procedures on how they can assert them. Indicate possible conditions for breaking confidentiality (e.g., subpoena, public interests and safety and the like.) ⊱⊱

GROUP CONFIDENTIALITY

⊰⊰ If focus group session or similar arrangement is done ⊱⊱

In order to respect the privacy of all participants in this study, a participant must agree to maintain the confidentiality of the information discussed by all participants and researchers during the focus group session.

OPEN DATA

⊰⊰ If de-identified data is archived or shared online or with other authorized researchers ⊱⊱

I understand that the information I provide in this study will be used for research purposes. It will not be used in any manner which would allow identification of my individual responses.

Anonymized research data will be archived at ⊰⊰ URL of open data site ⊱⊱ in order to make them available to other researchers in line with safe data sharing practices.

DISPOSAL

⊰⊰ After the information from the participant has served its purpose, explain how you plan to properly dispose or destroy it. ⊱⊱

CONTACT INFO

If you have further questions or concerns about your participation in this study, or if you suffer any injury related to the study, please contact:

__________________________ ________________________
Name Telephone

If you have questions about your rights as a participant or about ethical issues related to this study, you may speak with someone who is not involved in the study at all. That person is:

__________________________ ________________________
Name Telephone

SIGNATURES

⊰⊰ Summarize important points of agreement here ⊱⊱

- I understand that my participation is voluntary; I can withdraw from the study at any time and I do not have to give any reasons for why I no longer want to take part.
- All of my questions and concerns have been answered.
- I understand the information indicated in this informed consent form.
- I understand that my participation in this study includes being ⊰⊰ interviewed, recorded (audio or video), other activities expected ⊱⊱
- [Optional, usually for clinical trial] I allow access to my records and specimens, as explained in this consent form.
- By signing this form, none of my legal rights have been given up.
- [Optional, usually for clinical trial] I understand that my doctor or healthcare provider may be informed of my participation in this study.

________________________________ ________________
Signature Over Printed Name of Participant/ Date
Substitute Decision-Maker

________________________________ ________________
Signature Over Printed Name of Date
Person Conducting the Consent Discussion

ONLY IF the participant is unable to read, has relevant disabilities, or is a minor, accomplish this subsection:

- This form was accurately explained to, and clearly understood by, the participant/substitute decision-maker, and
- Informed consent was freely given by the participant/substitute decision-maker.

________________________________ ________________
Signature Over Printed Name Date
of Impartial Witness/Translator

4.3 Health Data Sharing Agreement Template[14]

Rationale: This Health Data Sharing Agreement seeks to support direct care and the resolution of a public health crisis brought about by COVID-19. The Department of Health (DOH) expects organizations to make it easier to share health data and to follow best practice in safely doing so. For these purposes, relevant personal confidential data should be shared among the duly authorized care and data professionals who have a legitimate relationship with the individuals concerned or with the governmental bodies tasked to address the pandemic. In particular, the processing of health data involved in this Agreement is covered by one or more of the following:

☐ For the performance of a contract with the data subject or to take steps to enter into a contract;
☐ For compliance with a legal obligation;
☐ To protect the vital interests of a data subject or another person;
☐ For the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
☐ For the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests, rights, or freedoms of the data subject.

This Health Data Sharing Agreement (HDSA) defines the arrangements for sharing patient data between [ORGANIZATION] and the organizations listed below.

1. Parties to the Agreement: Full name and address of the organization which is party to this Agreement.

2. What is the Sharing Agreement meant to achieve? There must be a clear objective or set of objectives.

Sample: To enable clinical, administrative, and support staff to have access to clinical and administrative information held on [ORGANIZATION] networked systems in order to be able to provide effective and seamless care to [ORGANIZATION's] patients while in their care, as well as to address related public health issues brought about by the pandemic.

3. What information needs to be shared? This should be the *minimum* amount of data necessary to achieve the objectives of the Agreement. List all the individual elements required.

[14] Shortcut to this evolving document: privacyph.org/datasharing. Originally patterned after a UK NHS data sharing agreement template, this document welcomes more comments and suggestions to address local needs. Feel free to contribute. Send comments, suggestions to: psy@up.edu.ph

4. Who needs access to the shared personal data? You should employ "need to know" principles. Only relevant staff should have access. This should also address any necessary restrictions on onward transmission.

5. When should it be shared? Is the sharing an ongoing routine process or does it only take place in response to particular events?

6. How should it be shared? Address the security issues involved in the transmission or access of data. Establish common rules for its security.

7. How can we check that the sharing is achieving its objective? How will you judge that the sharing is still appropriate and confirm that the safeguards still match the risk? How will you ensure that the arrangement will be formally terminated when no longer required?

8. What risks does the data sharing practice pose? Is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine the individual's trust in the organizations that keep records about them?

9. Where and how will the information be held and for how long? What format is it in? (e.g., removable media, computer system, etc.) How will the data be transferred? (e.g., SFTP, physical transfer of media (USB drive, hard drive), email, etc.)

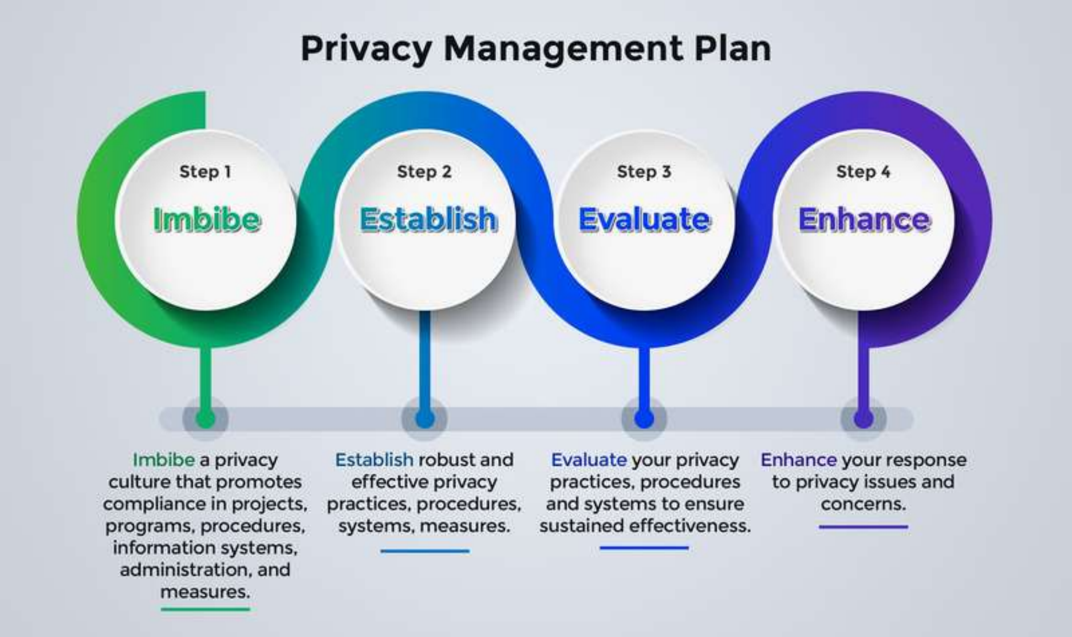
10. When will this agreement be reviewed and by whom? This Agreement will be reviewed ___ months after its signing and __ thereafter. The organization responsible for initiating the review process is [ORGANIZATION].

This **Agreement** must be approved and adopted by all parties before any data sharing takes place. All parties will ensure that this Health Data Sharing Agreement (HDSA) is disseminated to all relevant staff involved.

Organization 1
On behalf of [ORGANIZATION]
Name:
Position:
Date and Signature:

Organization 2
On behalf of [ORGANIZATION]
Name:
Position:
Date and Signature:

4.4 Privacy Management Plan[15]



Privacy Management Plan

Imbibe a privacy culture that promotes compliance in projects, programs, procedures, information systems, administration, and measures.

Establish robust and effective privacy practices, procedures, systems, measures.

Evaluate your privacy practices, procedures and systems to ensure sustained effectiveness.

Enhance your response to privacy issues and concerns.

STEP 1

Imbibe a privacy culture that promotes compliance in projects, programs, procedures, information systems, administration, and measures.

Action	Position/Person Responsible	Due	Notes/Status
Adopt a "privacy by design" approach (see Privacy by Design in Health; Privacy by Design in Research).			
Assign key roles and responsibilities (e.g., Data Protection Officer (DPO)[16], Data Custodian) for privacy management.			

[15] Last revised 14 June 2019. Shortcut to this template: privacyph.org/mgt. Developed from the "Privacy management plan template" of the Office of the Australian Information Commissioner; revised periodically. Request latest version from, send feedback to: psy@up.edu.ph

[16] See DPO Duties and Responsibility: privacyph.org/dpo

Action	Position/Person Responsible	Due	Notes/Status
Assign staff responsibilities for managing privacy and coordinating with personnel concerned with other related functions in the organization, such as information security, data management, and archiving.			
Create reporting mechanisms that ensure that senior management is routinely informed about privacy issues and concerns.			
Ensure that the staff understand their privacy obligations and the roles of the National Privacy Commission and other related agencies.			

STEP 2

Establish robust and effective privacy practices, procedures, systems, and measures.

Action	Position/Person Responsible	Due	Notes/Status
Keep an up-to-date inventory of your organization's personal information holdings (information types, locations, custodians).	Personal Information Controller	15th of June (semi-annual)	Active
Develop and maintain processes around the handling of personal data prior to collection, while personal data are held, and once they are no longer needed.			
Integrate privacy into staff training, induction/on-boarding, off-boarding/termination processes.			
Implement risk management processes to identify, assess, and manage privacy risks across the organization (see **Privacy Impact Assessment**).			

Action	Position/Person Responsible	Due	Notes/Status
Develop and implement a clearly expressed and up-to-date privacy policy (see **Privacy Manual** [17]).			
Establish processes for receiving and responding to privacy enquiries and complaints (see **Data Breach Management and Response Questionnaire**).			
Establish processes that allow individuals to promptly, easily access and correct their personal data.[18]			
Create a **Data Breach Response and Management Plan**.			

STEP 3

Evaluate your privacy practices, procedures, and systems to ensure sustained effectiveness.

Action	Position/Person Responsible	Due	Notes/Status
Regularly monitor and review privacy processes, policies, and notices.	Data Protection Officer		On hold
Document compliance with privacy obligations, including keeping records on privacy process reviews, breaches, and complaints.			
Measure your performance against this privacy management plan.			
Create and promote channels for staff and clients to provide feedback on your privacy and business processes.			

[17] A **Privacy Manual** is your organization's own Privacy Rules that takes into account the risks identified in your **Privacy Impact Assessment** exercises. In the Health Sector, the Health Privacy Code may serve as template for the Manual.

[18] Certain research activities are *possible* exceptions to this.

STEP 4

Enhance your response to privacy issues and concerns.

Action	Position/Person Responsible	Due	Notes/Status
Use the results of evaluations to drive the improvements on your practices, procedures, processes, and systems.	Data Protection Officer		Proposed
Have your privacy processes externally assessed or audited to identify areas for improvement.			
Keep up to date with issues and developments in privacy law and changing legal obligations, especially those required by the National Privacy Commission.			
Monitor and address new security and privacy risks and threats.			
Examine and address the privacy implications, risks, and benefits of new technologies. Consider implementing privacy-enhancing technologies that allow you to minimize privacy risks and better manage the personal information you handle.			
Introduce initiatives that promote good privacy standards in your business practices and information processes.			
Participate in privacy events organized with the privacy community.			

4.5 Data Breach Response[19]

To cover a wide range of issues in data breach response, answer the guide questions below. Please supply justification where appropriate.

Issue	Yes / No	Justification / Comments
1. Do you know **how** a data breach is identified?[20]		
2. Do your staff know **what to do** if they suspect a data breach has occurred? Do they know their specific roles?		
3. Do you know who is *ultimately responsible* for your entity's handling of a data breach in accordance with the plan?		
4. Can you tell us who are on your data breach **response team**?		
5. Do you need to include *external* expertise in your response team (e.g., data forensics expert, privacy expert)?		
6. Have you set up clear **reporting lines** for your organization?		
7. Do you know when you need to notify the National Privacy Commission or the individuals affected by a data breach?[21]		

[19] Last revised 21 July 2019. Developed from OAIC, "Guide to developing a data breach response plan, Consultation Draft" (October 2015); revised periodically with aim to reflect latest development. Request latest version from, send feedback to: psy@up.edu.ph. Use this questionnaire to develop your own Data Breach Response and Management Plan. Practice periodic data breach drills. NPC Circular 16-03 (Personal Data Breach Management, 15 Dec 2016) provides definitive guidance on the subject.

[20] Breaches include that of availability (personal data loss), integrity (unauthorized alteration of personal data), and confidentiality (unauthorized disclosure of or access to personal data). A breach is to be reported to the NPC within 72 hours upon knowledge of the breach.

[21] NPC Circular 16-03, esp. Sec 17&18.

Issue	Yes / No	Justification / Comments
8. Have you considered in what circumstances law enforcement authorities (like the NBI or the PNP) or regulators (like the NPC) need to be contacted?		
9. Do you have an established organizational approach to responding to **media inquiries** or public concerns, including having a designated spokesperson and a proactive communication strategy?		
10. In relation to the (potential) data breach, do you know what **records** are to be kept, and how to manage them?		
11. Does your plan refer to any strategies for identifying and addressing any weaknesses in data handling that contributed to the breach?		
12. Do you know how frequently your **plan** is tested and reviewed, and who is responsible for doing so?		
13. Have you participated in any privacy breach response exercises at your institution in the last 12 months?		
14. Are there any *other* matters specific to your circumstances that might mitigate or aggravate a data breach (e.g., an insurance policy that may apply to damages caused by data breach or damage to data infrastructure)?		

4.6 Ethics Review Process

4.6.1 Informed Consent Assessment Form[22]

Name	
Title of the Study	
Institution	

Questions for reviewing the informed consent process and form:

	YES	**NO**
Is it necessary to seek the informed consent of the participants?		

If NO, please explain.	

If YES, is the following information COMMUNICATED with and UNDERSTOOD by the participants?

	YES	**NO**
1. Statement that the activity to be participated in *is* research.		
2. Statement describing the purpose of the study.		
3. Expected duration of participation in the study.		
4. Projected number of participants.		
5. Responsibilities of the participant.		
6. Description of all relevant procedures, especially those potentially invasive of privacy and bodily integrity.		
7. Interventions related to the study and probability of random assignment.		
8. Study aspects that are experimental.		
9. Foreseeable risks to participants. (e.g., possible discrimination, etc.)		
10. Possible conditions for breaking confidentiality such as subpoena and legal public interests.		
11. Description of the security measures applied during the storage of data.		
12. Reasonably expected benefits and compensation or absence of thereof.		

[22] Originally based on assessment forms from UP Manila, National Ethics Committee, UP College of Social Science and Philosophy. Updated 5 June 2021. Shortcut to live version of this form: privacyph.org/consentassess. Send comments, suggestions to psy@up.edu.ph

13. Anticipated expenses, if any, to the participant in the course of the study.		
14. Possibility of post-study access to the study product.		
15. Statement describing extent of participant's right to access his/her records.		
16. Access to data limited only to those who legitimately need it, the owner of the data, the researchers?		
17. Access by third parties or third-party service providers?		
18. Practice of privacy management and breach management procedures in place?		
19. Plans of retention of data only until it has served its declared purpose.		
20. Physical and digital storage of data have security measures.		
21. Encryptions are applied to the stored sensitive data.		
22. Plans of disposal of data gathered after the study.		
23. Immediate destruction of data deemed unnecessary or superfluous to the study.		
24. Plans to develop commercial products from the data gathered and whether the participant will receive monetary or other benefit from such development.		
25. Compensation or treatment entitlements of the participant in case of study-related injury.		
26. Statement that participation is voluntary, and that the participant may withdraw anytime without penalty or loss of benefit to which the participant is entitled.		
27. Person to contact for pertinent questions or for assistance in a research-related injury.		
28. Person to contact in the study team for further information regarding the study.		
29. Information on the effect of refusal to participate or discontinuance at any time. Will it involve a penalty or loss of benefits to which the subject is entitled?		
30. Sponsor, institutional affiliation of the investigators, and nature and sources of funds.		
31. Third parties are under a legal data sharing agreement.		

	YES	NO
Is the informed consent written or presented in lay language that participants can understand?		
Does the protocol include an adequate process for ensuring that consent is voluntary?		

Concern/s	
Recommendations	□ Approved
	□ Minor Revisions Required
	□ Major Revisions Required
	□ Disapproved

Name and Signature of Reviewer	**Date of Review**

4.6.2

Ethics Review Process

Research Proposal Assessment Form[23]

Name				
Title of the Study				
Institution				
Assessment Point	Yes	No	Not Applicable	Remarks
1. Study Design				
1.1. Is the **study objective** reviewed for its viability?				
1.2. Is/Are the **research question(s)** backed by the literature review?				
1.3. Does the **literature review** have animal/human studies showing known risks and benefits of intervention?				
1.4. Is the **research design** appropriate in view of the objectives?				
1.5. Does the **sampling design** apply appropriate sampling methods and techniques?				
1.6. Is the computation of **sample size** reviewed?				
1.7. Does the **statistical analysis plan** (SAP) use appropriate statistical methods or techniques?				

[23] Originally based on assessment forms from UP Manila, National Ethics Committee, UP College of Social Science and Philosophy. Updated 5 June 2021. Shortcut to this form: privacyph.org/proposalassess. Send comments, suggestions to psy@up.edu.ph. See also Research Proposal Review Guide for Data Privacy Concerns: privacyph.org/researchreviewtips.

1.9. Is the **inclusion criteria** precise for both scientific merit and safety concerns; and of equitable selection of participants?				
1.10. Is the **exclusion criteria** precise for both scientific merit and safety concerns; and of justified exclusion?				
1.11. Is the **withdrawal criteria** precise for both scientific merit and safety concerns?				
2. Conduct of the Study				
2.1. Are **human participants**[24] necessary for the conduct of the study?				
2.2. Is the manner of participant **recruitment** appropriate?				
2.3. Is the **duration** of participant involvement in the study discussed?				
2.4. Are the safeguards for **data processing** (collection, storage, access, disposal, and terms of use) adequate for the study?				
2.5. Does the **data management plan** (DMP) explicitly describe the handling of personal information?				
2.6. Is the **collection** of data done according to the declared purpose of the research?				
2.7. Do the physical and digital **storage** of data have appropriate physical and technical measures?				

[24] A screener on whether an activity is "human subjects/participants research" is available at privacyph.org/humanresearch.

2.8. Are organizational, physical, and technical measures reviewed for **data security**?				
2.9. Do the **privacy notices** (e.g., project information sheet, website) utilized to inform the public contain adequate information about the study and its privacy safeguards?				
3. Ethical Considerations				
3.1. Are there any potential **conflicts of interest or competing interests** (e.g., financial, familial, proprietary considerations)? If so, are they managed well?				
3.2. Is the manner of obtaining **informed consent** appropriate?				
3.3. Is the feasibility of obtaining **assent** (if the study involves children), instead of consent, practiced?				
3.4. Is the **community** involved in the decision making about the conduct of study?				
3.5. Does the study involve individuals who belong to **vulnerable** groups?				
3.6. Are there probable **risks** to the human participants in the study?				
3.7. Are the participants informed of the data subject's **privacy rights**, and the cases where those rights are exempted?				

3.8. Are the **incentives** or reimbursement of study-related expenses appropriate?				
3.9. Is **access to data** limited only to those who legitimately need it, the owner of the data, the researchers, and the third party?				
3.10. Are third parties under a legal **data sharing agreement**?				
3.11. Are the **terms of collaborative study** reviewed for intellectual property rights, publication rights, information and responsibility sharing, transparency, and capacity building?				
3.12. Is the **retention** of data only until its purpose is fulfilled?				
3.13. Is the immediate **destruction** of data (deemed unnecessary) practiced?				

Concern/s	
Recommendations	☐ Approved
	☐ Minor Revisions Required
	☐ Major Revisions Required
	☐ Disapproved
Name and Signature of Reviewer	**Date of Review**

APPENDIX

PRIVACY COMPLIANCE MATRIX

Privacy Compliance Requirements & Tools

	DPO Appointment	Registration of Data Processing Systems	Privacy Impact Assessment	Privacy Management Program	Organizational Privacy Manual [25]	Breach Response Plan	Annual Security Incident Report (ASIR)
Due Date	(asap/ overdue)	(asap/ overdue)	(internal)	(internal)	(internal)	(internal)	2020: overdue
NPC Guidance Docs	NPC Circular 16-01, Advisory No. 2017-01	NPC Circular 17-01	NPC Advisory No. 2017-03	NPC Circulars 16-01, 16-02	NPC Circular 16-03	NPC Circular 16-03	NPC Circular 18-02
NPC Forms	www.privacy.gov.ph/guidelines-on-dpo-registration-process	www.privacy.gov.ph/wp-content/uploads/ 06-Registration-of-Data-Processing-Systems.pdf	www.privacy.gov.ph/wp-content/files/attachments/nwsltr/ NPC PIA 06 18.pdf	www.privacy.gov.ph/exercising-breach-reporting-procedures/	www.privacy.gov.ph/creating-a-privacy-manual/	www.privacy.gov.ph/wp-content/ uplo ads/05-Data-Breach-Management.pdf	www.privacy.gov.ph/wp-content/files/attachments/nwsltr/Final Advisory18-02 6.26.18.pdf
Project Tools	DPO Duties and Responsibilities	N/A	PIA Worksheets	Privacy Management Plan (PMP) Template	PMP Template + PbD Guidelines	Breach Response Questionnaire	N/A

[25] Organizational Privacy Manual corresponds to NPC's "Pillar 4" (Implementation of Privacy & Data Protection Measures" detailing specific data privacy rules and measures that an organization and its personnel would follow.

DATA PRIVACY TOOLKIT FOR RESEARCH INVOLVING HUMAN PARTICIPANTS