DATA PRIVACY PROTECTION & RESEARCH INVOLVING HUMAN PARTICIPANTS: A PRIMER

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

Cite as:
Sy, P. A., Navera, J. C., Tan, K., & Nicolas, F. (2021). *Data Privacy Protection and Research Involving Human Participants: A Primer.* Social Sciences and Philosophy Research Foundation, Inc.
DOI: 10.6084/m9.figshare.14479353

Display type set in Blanka, Hussar Bold, Hussar Ekologiczy. and Lovelo.

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 and Mark Luis Bulan

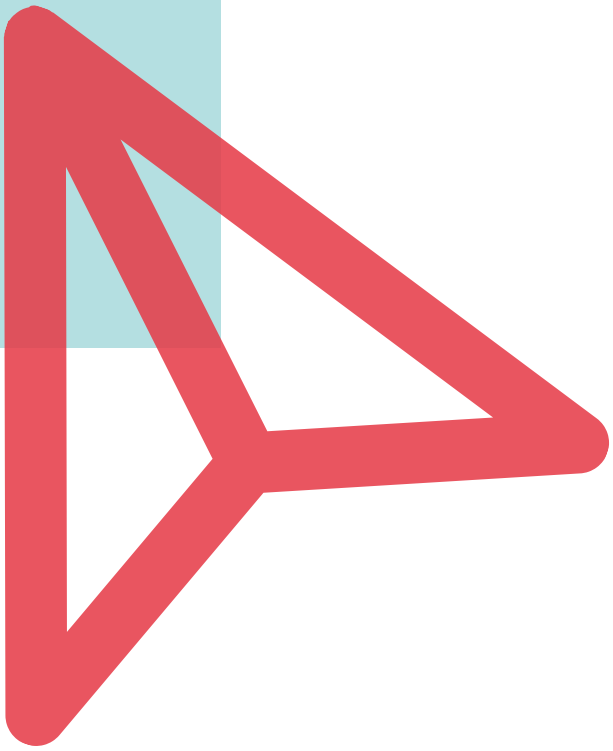
Book design by
Georgina Mia B. Gato

Photos from Unsplash, Pexels, and Freepik

Printed in the Philippines

DATA PRIVACY PROTECTION & RESEARCH INVOLVING HUMAN PARTICIPANTS: A PRIMER

Peter A. Sy
J.C. Navera
Katrina Tan
Fatima Nicolas
University of the Philippines



FOREWORD

Congratulations to the Social Sciences and Philosophy Research Foundation (SSPRF), Inc. for the successful development and launch of the Primer on Data Privacy Protection and Research Involving Human Participants! This will guide researchers and ethics review committees in complying with privacy regulations, as they apply to health and social research involving human participants.

Health and social sciences researchers often collect and process personal information from human participants involved in their studies. In this respect, the role of ethics review committees to effectively evaluate the extent to which a research proposal is able to protect a human participant's right to privacy, is instrumental. With the passage of the Republic Act No. 10173 or the Data Privacy Act of 2012, additional guidelines and regulations were formulated for the processing and protection of personal information. This primer responds to the need for knowledge dissemination and eventual integration of concepts related to privacy protection of human participants into the development of health and social sciences research protocols.

Among others, the Data Privacy Protection Primer showcases a contextualized understanding of various issues relating to privacy protection in research, institutional measures to address these issues, and the importance of confidentiality and de-identification. As the national coordinating body for health research, the Department of Science and Technology–Philippine Council for Health Research and Development (DOST-PCHRD) values privacy protection of human participants involved in health research projects. With this, we enjoin health researchers, ethics review committees, and other stakeholders to support the Social Sciences and Philosophy Research Foundation's initiative to advance capacities on data privacy protection in the research sector.

JAIME C. MONTOYA, MD. MSc, PhD, CESO II
Executive Director III
Philippine Council for Health Research and Development

PREFACE

With the Data Privacy Act of 2012, the Philippines has enacted its first comprehensive law on privacy protection. Patterned after the European Union's Data Protection Directive (now superseded by the General Data Protection Regulation), the law penalizes the unauthorized processing of personal information.

The law's impact on human subjects research, however, remains ambiguous. While Section 3(j) of the law appears to give some leeway for "personal information processed for journalistic, artistic, literary or research purposes," a closer reading of the law and other public articulations by the National Privacy Commission suggests that this is not a blanket exemption for research. Section 5(c) of the law's Implementing Rules and Regulations, in particular, allows for such processing "subject to the requirements of applicable laws, regulations, or ethical standards."

In this regard, the Social Sciences and Philosophy Research Foundation, Inc. (SSPRF), with funding from the Philippine Council for Health Research and Development (PCHRD), initiated the "Development of a Data Privacy Toolkit for Research Involving Human Participants in the Philippines: A Participatory Action Research Project." The Project's objectives are twofold: (1) to uncover issues and concerns relating to the impact of the Data Privacy Act on research involving human participants in the country and (2) to offer practical guidance to Filipino researchers and ethics review committees based on the Project's findings and insights.

As a Project output, this Primer on Data Privacy Protection and Research Involving Human Participants is primarily intended to address the needs of research ethics committees, Philippine research and higher education institutions, researchers, patient organizations, other stakeholders, and the general public. The Primer aims at aiding individuals and organizations in adhering to the ethical guidelines and standards of the National Privacy Commission (NPC) and the Philippine Health Research Ethics Board (PHREB). Likewise, this material may also serve as supplementary

reading for those who wish to know the concepts and application of the Data Privacy Act in the context of research, especially health-related studies, in the Philippines.

This Primer seeks to serve as a baseline discussion on data privacy in research covering the main thematic areas of inquiry, namely: (1) Privacy Rights, (2) Principles of Data Privacy, (3) Contextual Issues, (4) Privacy and Welfare Protection in Research, and (5) Confidentiality and De-identification. Inputs from workshops on data privacy and research conducted by the Project Team in collaboration with 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, have greatly contributed to the development of this Primer and the two other project outputs: the Data Privacy Toolkit and Online Course. These workshops were attended by research directors, ethics committee members, and researchers 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. However, none of the flaws or oversights this primer may contain can be attributed to any of these institutions.

The discussion questions incorporated in each section have been designed to test and further enhance the reader's understanding of the different aspects of data privacy in human subjects research.

The Project Team hopes that this Primer as well as its companion Toolkit and Online Course will be useful to ethics reviewers, researchers, research participants, and other entities in understanding the concepts and application of data privacy principles and practices in their present and prospective endeavors. We welcome feedback to help us further develop our materials. You may leave your comments and suggestions via the "live" version of this document accessible at privacyph.org/projbrief. For more information on Project activities and updates, visit privacyph.org.

ACKNOWLEDGMENTS

We would like to express our gratitude to the Philippine Council for Health Research and Development (PCHRD) and its Executive Director, Dr. Jaime Montoya, for funding our project to develop a privacy toolkit and an online course on privacy in human subjects research. Special thanks are due to Faye Margaret Lagrimas of the Research Information, Communication, and Utilization Division for helping us navigate the institutional requirements of the project.

The Project would not have been possible without the partnerships developed along the way. The endorsements from Raymund Enriquez Liboro, Commissioner and Chair of the National Privacy Commission (NPC); Dr. Leonardo de Castro, Chair of the Philippine Health Research Ethics Board (PHREB); and, Dr. Prospero de Vera, Commissioner and Chair of the Commission of Higher Education (CHED), are just the right boost for the Project in gaining the trust and confidence of our institutional partners. Colleagues and co-organizers 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, and the University of San Carlos have worked hard to make our consultation and validation workshops run smoothly. Workshops with PHREB, the Department of Health (DOH), and the Philippine Social Science Council (PSSC) have also provided us with invaluable inputs.

Special thanks are due to our resource persons, including Dr. Maria Carinnes Alejandria (University of Santo Tomas), Atty. Ivy Patdu (former Deputy Commissioner, National Privacy Commission), Prof. Erwin Bañez (University of the Philippines Diliman), Dr. Raymond Francis Sarmiento (University of the Philippines Manila), Dr. Mario Aguja (President, Philippine Sociological Society), Dr. Erlinda Palaganas (University of the Philippines Baguio), Atty. Sharon Rose Carolino (University of the Philippines Baguio), Dr. Judith Rafaelita Borja (University of San Carlos), Dr. Maria Cecilia Gastardo-Conaco (University of the Philippines Diliman), and Dr. Maria Fiscalina Nolasco (University of San Carlos), for generously sharing their time and expertise. We would also like to thank the many members of the Philippine research community for their active engagement through our workshops and online editable documents. We hope that this work offers you practical suggestions in dealing with privacy risks without compromising the quality of research in the country.

A final word of thanks to the Social Sciences and Philosophy Research Foundation, Inc. (SSPRF) and its President, Dr. Grace Aguiling-Dalisay, for their unfailing support. Special gratitude is due to SSPRF's Ms. Aleli Caraan and Ms. Jewel Regnim, whose company we cherish amidst the drudgery of work, for their critical support in project management.

CONTENTS

01 Introduction

07 Privacy Rights

16 Principles of Data Privacy

27 Contextual Issues

36 Privacy and Welfare Protection in Research

61 Confidentiality & De-identification

70 Postscript

71 Appendix A: Summary of Tools & Templates

72 Appendix B: Privacy Compliance Matrix

73 Appendix C: Case Vignettes for Privacy in Research

INTRODUCTION

"All research on individuals and groups threatens their privacy."[1]

With the enactment of the Data Privacy Act of 2012, Filipinos doing research involving human participants face new regulatory challenges over the extent to which they process the personal information of their (data) subjects. Particularly impacted by the new legislation are the fields of health and allied health sciences and social research, fields whose inquiries often require the processing of sensitive personal information. The law ostensibly provides enough leeway for research.[2] Subsequent qualifiers in the law and its Implementing Rules and Regulations,[3] however, do not warrant any wholesale exemption for research. This is consistent with similar privacy laws elsewhere: e.g., the EU's General Data Protection Regulation (GDPR; Recital 159), the US HIPAA Privacy Rule, Australia's Privacy (Market and Social Research) Code 2014. Section 19, in particular, sets

Definition

1 "**Human participants**" is used here interchangeably with "human subjects," defined as "a living individual about whom an investigator…conducting research: (i) obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (ii) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens" (45 Code of Federal Regulations 46.102e). Private information is not the same as personal information (see Definition 2). With the Data Privacy Act (DPA) of 2012, processing of personal information is regulated, regardless of source or location (whether private or public). A screener on whether an activity is "human subjects research" is available at privacyph.org/humanresearch.

[1] British Association Study Group. (1979). Does Research Threaten Privacy or Does Privacy Threaten Research? In M. Bulmer (Ed.), Censuses, Surveys and Privacy (pp. 37–54). London: Macmillan Education UK.

[2] Rep. Act No. 10173 (2012), sec. 4 (d): The Act does not apply to "…personal information processed for journalistic, artistic, literary or research purposes."

[3] See Rule IV, Section 20(c); Sec. 5c; Sec. 37; Sec. 49, IRR of Rep. Act No. 10173.

limitations on the non-applicability of certain privacy rights in research, upholding the *strict confidentiality* of participants' personal information and restricting its use "*only for the declared purpose.*" [4] The "strict confidentiality" and "only for the declared purpose" requirements are not necessarily making it easier for researchers. These can, for instance, be strictly interpreted to mean that anonymized data cannot be processed for purposes other than those indicated in the original consent for the source personal data. [5] Section 20 (c) of the Act's Implementing Rules and Regulations further stipulates the provision of "adequate safeguards" [6] and the need to follow **ethical standards** when processing such information in research. Non-compliance or unauthorized processing of personal information can mean serious criminal liabilities under the Act, resulting in fines *and* imprisonment.

There is also the question of what constitutes "research." *Narrowly*, it refers to "a class of activity designed to develop or contribute to generalizable knowledge. Generalizable knowledge consists of theories, principles or relationships, or the accumulation of information on which they are based, that can be corroborated by accepted scientific methods of observation and inference." [7] That definition could

Definition

2 "**Personal information**" refers to any information (whether recorded in a material form or not) from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual (RA 10173 (2012), sec. 3 (g)).

Definition

3 RA 10173 also refers to "**sensitive personal information**" that includes information (1) about an individual's race, ethnic origin, marital status,age, color, and religious, philosophical or political affiliations; (2) about an individual's health, education, genetic or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceeding or the sentence of any court in such proceedings; (3) issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (4) is specifically established by an executive order or an act of Congress to be kept classified (sec. 3 (l)).

[4] Rep. Act No. 10173 (2012), sec. 19: "The immediately preceding sections [privacy rights, namely: Sec 17 (Transmissibility of Rights of the Data Subject) and Sec 18 (Right to Data Portability)] are not applicable if the processed personal information are [sic] used only for the needs of scientific and statistical research… Provided, That the personal information shall be held under **strict confidentiality** and shall be used **only for the declared purpose**" (emphasis added).

[5] Beyleveld, D., & Histed, E. (2000). Betrayal of Confidence in the Court of Appeals. *Medical Law International,* 4(3–4), 277–311. https://doi.org/10.1177/096853320000400407.

[6] In GDPR language, "The processing of personal data for archiving purposes in the public interest, scientific or historical **research** purposes or statistical purposes **should be subject to appropriate safeguards for the rights and freedoms of the data subject**…" (sec. 156, Gen Data Protection Reg 2016/679; emphasis added). Again, no blanket exemption for research.

[7] CIOMS, 2002. International ethical guidelines for biomedical research involving human subjects. *Bulletin of Medical Ethics*, (182), 17.

exclude many research activities in the social sciences. Broadly, research could refer to any systematic inquiries by diverse academic disciplines or by non-academic groups or individuals. In the GDPR, journalism is the reference practice allowed to abrogate certain privacy rights. However, locally, professional recognition may entail some formal professional accreditation; for instance, for journalism, Rep. Act No. 53 exempts publishers, editors, and duly accredited reporters from revealing the sources of news information obtained in confidence.

In operational terms for research organizations, following ethical standards in research entails having their research proposal or protocol reviewed by a trained, duly accredited research ethics review committee. Research ethics review mitigates the potential assault on the privacy of individuals and groups. It supports science as a *public good.* Ethics review seeks to make the processing of personal information in the context of research a balance between the protection of the right to privacy and the

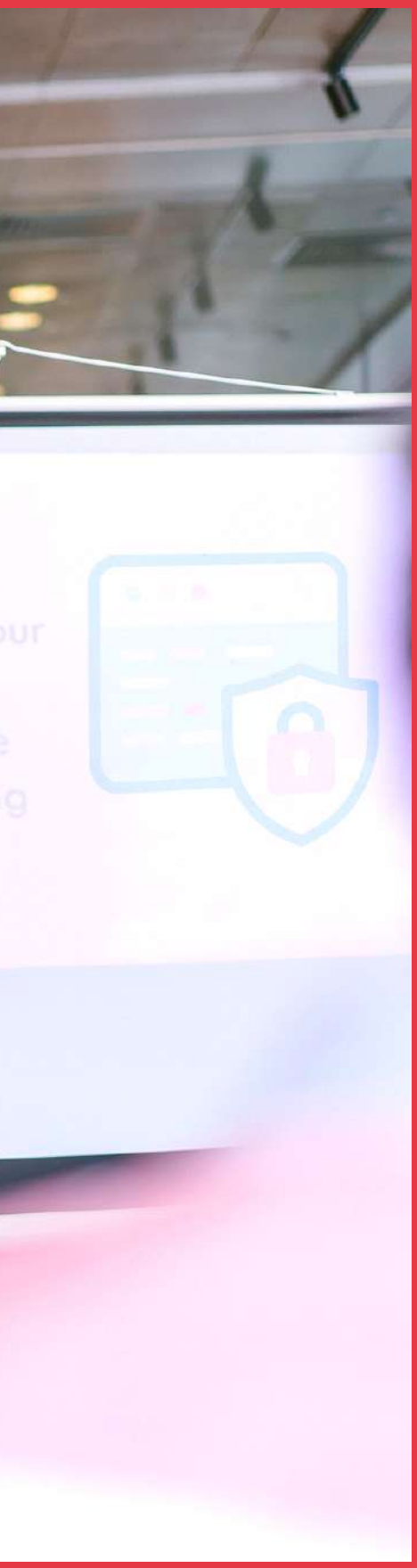
Definition

4 The Implementing Rules and Regulations (IRR) of the Act uses the ad hoc term "**personal data**" to refer to both personal information and sensitive personal information as well as to "privileged information." **Privileged information** refers to any and all forms of data which, under the Rules of Court and other pertinent laws, constitute privileged communicatioon (e.g., patient-doctor, lawyers-client, husband-wife communications).

Definition

5 A **data subject** is "an individual whose personal information is processed" (Rep. Act No. 10173). **Research participants could be *simultaneously* research subjects and data subjects**. Certain research, however, processes information not only of its human subjects but also of "third-party" data subjects. In the latter case, such data subjects are not necessarily research subjects and have unlikely consented to the processing of their personal information.


Talking Point
Activity – 5 minutes



Definition

6 By "**processing**" the law refers to a broad range of activities including (but not limited to) copying, deleting, sharing, storing, and transferring of personal data (sec. 3, par. j), activities that are practically inescapable in research involving human subjects.

need to generate knowledge or foster innovation. Beyond compliance and the threat of criminal and civil liabilities, stakeholders and researchers should make the privacy protection of data subjects an integral part of research culture and protocols.

In this light, the Primer aims to provide Stakeholding Workshop participants with a baseline discussion on privacy protection in research involving human participants, on the rights and principles governing privacy, and on other attendant issues concerning the impact of privacy regulation on research. This Primer includes five (5) thematic areas, namely:

1. Privacy Rights
2. Principles of Data Privacy
3. Contextual Issues
4. Privacy and Welfare Protection in Research
5. Confidentiality & De-identification

Overlaps among these areas are unavoidable; they differ primarily in emphasis. Privacy rights are human rights of study participants and data subjects. The Principles of Data Privacy section seeks to guide researchers and organizations in dealing with personal data out of respect for privacy rights. It provides an overall framework for compliance with the privacy regulation, in a manner facilitative of scientific research as a general public interest, notwithstanding the perceived tension between these two areas. Albeit inexhaustive, an accounting of Contextual Issues of data privacy in research is necessary

for any individual and organizational understanding of data privacy in the first place, as privacy, by its nature, is context-sensitive. The Privacy and Welfare Protection in Research section details institutional measures to address privacy protection and compliance issues. The final section on Confidentiality and De-identification emphasizes specific approaches in which research and data subjects intersect. Proper de-identification, in particular, enables the researchers and research organizations to share and store information safely and beyond the immediate limitations the law may have set.

The "Further Discussion" areas directly relate to the sections immediately before them. They are meant to extend the conversation, raise concerns, or *clarify* issues in relation to diverse practices of research in the Philippines. Efforts are made to cover the broadest range of research activities as part of contextual considerations of data privacy. Matters that become unambiguous or gain relative consensus among workshop participants could be moved to the main "baseline discussion." The questions are not meant to be "pop quizzes"; they are raised to help facilitate discussions around the five thematic areas. The questions are meant to help workshop participants examine the accompanying practical tools (linked from relevant sections) that enable them to address privacy issues and concerns or help researchers and research institutions deal with privacy regulations efficiently.

PRIVACY RIGHTS

01

The Data Privacy Act of 2012 strengthens individual rights pertaining to one's personal information. With the data privacy law in place, it is important for researchers to be aware of the rights of the people from whom they acquire personal data. Based on the EU's Data Protection Directive (1995),[8] the Act also defines a set of rights concerning personal data, "accruing to individuals and a set of rules for lawful processing on the part of data processors applicable irrespective of sector of application."[9] Arguably, people have "the right not to be researched."[10] Enrollment in research does not make data subjects lose their privacy rights. There is only an accommodation of scientific research as a *public interest*.

The Act could not have contemplated any situation where no law would apply to the processing of personal data in ways detrimental to human or data subjects.

Most of all, as the National Privacy Commission (NPC) puts it, "the rights of the data subject shall be upheld **without compromising research integrity**."[11] To the extent feasible, these rights have to be observed by researchers and research organizations. These rights are so *intertwined* with each other that

[8] In 2018 this was superseded by the General Data Protection Regulation (GDPR). See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) OJ L 119, 4.5.2016, p.6.

[9] Kenny, S., & Korba, L. (2002). Applying digital rights management systems to privacy rights management. *Computers & Security*, 21(7), 648-664.

[10] Sagarin, E. (1973). The research setting and the right not to be researched. *Social Problems*, 21, 52–64.

[11] IRR of Rep. Act No. 10173 (2012), sec. 20 (c). No suggestion, however, is made that "research integrity" is static. There is reason to believe that it is increasingly challenged by technological advancements or that traditional standards of research integrity would at least need revisiting. See, for instance, Gerwin van Schie, Irene Westra & Mirko Tobias Schäfer, "Get Your Hands Dirty: Emerging Data Practices as Challenge for Research Integrity" in Schäfer, M. T., & Van Es, K. (Eds.). (2017). *The datafied society: studying culture through data.* Amsterdam: Amsterdam University Press.

limiting one would tend to undermine the others as well. In cases where research integrity tends to be undermined by granting a particular privacy right, granular adjustments have to be made with the other privacy rights and ensure *not* to compromise research integrity. The law also sets data safety and confidentiality (as well as, effectively, ethics review) as the minimum for allowing the limitation of any privacy rights. To enable a granular balancing of specific privacy rights and the research enterprise, this section seeks to discuss the very research contexts where these rights could be observed.

1.1

Right to be Informed

The right to be informed is a fundamental privacy right, as it empowers the data subject to consider courses of action to protect his own privacy and interests. It signals one's willingness, as a data subject, to provide personal data to a collecting entity. Such data can be accessed, stored, or used by the researchers as long as the data subject gives their permission to do so. Under R.A. 10173, the individual's personal data is treated like his own personal property. In the same way that the use of any sort of property must be done with an owner's consent, personal data should never be collected, processed, and stored by the researcher without the individual's **explicit consent**, unless otherwise provided by law.[12] In case there is any change or alteration to the information previously given to the subject, he should be notified and given an opportunity to withhold consent.

[12] Rep. Act No. 10173 (2012), sec.12.

In operational terms, your research project's **information sheet** to be given out to participants should include the following:

- the purpose of the research,
- what is involved in one's participation in your research,
- the risks and benefits of participation,
- important details of the research, including the name of project, funding source, and sponsoring institution,
- contact details of researchers (or oversight of the project) and how to file a complaint,
- steps in withdrawing participation,
- data utilization plan during the study, storage, dissemination, publishing, and archival, and
- concrete steps the research team takes in maintaining data safety and confidentiality.

The Council of the EU specifies the minimum for "research integrity" to include bars against fabrication, falsification, and plagiarism. Research integrity entails adherence to the ethical principles and professional standards, sound data management, confidentiality, responsible sharing– all essential for the responsible practice of research (Council of the EU Conclusions on Research Integrity, 2011, endnote n°5).

1.2 Right to Access

Once data subjects have given you their consent to use their personal information, they also have the right to access it. Under the Data Privacy Act of 2012, data subjects have the right to obtain from an organization a copy of any information relating to them.[19] It should be provided in an easy-to-access format, accompanied by an explanation in plain language.

Further Discussion

D1.1.1. For many research projects, explicit written consent is a clear indication that the research subject's right to be informed has been respected. However, what about certain studies where getting written consent could adversely affect **research integrity**? (See also the subsection on **Consent** under the Principles of Data Privacy section.) How can research subjects be truly informed?

D1.1.2. *Deception.*[13] Certain studies in sociology,[14] psychology,[15] anthropology,[16] education,[17] applied economics,[18] and other behavioral or social sciences sometimes involve the use of deception or covert methodologies. Such research would otherwise not be possible if the subjects were aware of (a) the researcher's identity, (b) the exact nature of the research being done, or (c) that there was research being done in the first place. These could present a threat to a person's right to be informed. What is the closest thing to respecting the data subject's right to be informed in carrying out research involving active deception, covert methodologies, or withholding of certain information from research participants? Would a research project's **privacy notice** suffice (see Transparency section)?

D1.1.3. *Population Databases.* Population-based studies can be immensely beneficial to researchers working in health and the social sciences. Such studies are essential to the control of life-threatening diseases such as cancer. Using comprehensive government databases can gain fairly reliable social scientific insights into human populations. With the Data Privacy Act in place, how could such population-level studies be affected by potential limitations on the use of such databases for research?

[13] For a general discussion on the methodological issues in the use of deception, see Kimmel, A. J. (2007). *Ethical issues in behavioral research: basic and applied perspectives* (2nd ed). Malden, MA: Blackwell Pub, pp 84-109.

[14] The American Sociological Association (ASA) Code of Ethics states that, "On rare occasions, sociologists may need to conceal their identities in order to undertake research that could not practicably be carried out were they to be known as researchers." American Sociological Association (2018). Code of Ethics 11.4(d). http://www.asanet.org/sites/default/files/asa_code_of_ethics-june2018.pdf

[15] See APA Standard 8.07: "Deception in Research." Deception in psychological research is not used unless there is strong justification for its scientific, educational, or applied value and alternative non-deceptive procedures are not feasible. Debriefing is to be done as soon as is feasible and no later than the conclusion of the data collection. Participants are supposed to be able to withdraw their data. "Ethical Principles of Psychologists and Code of Conduct," 2002, American Psychologist, 57(12), 1060-1073.

[16] The use of participant observation or other unobtrusive methods of research is common in anthropology. Such methods involve at least passive deception or at least non-revelation of the nature of research being done. An argument, however, can be made that despite the "deception," "the spirit of informed consent can be fulfilled without the intrusive and unnecessarily legalistic use of a signed form." See Fluehr-Lobban, C. (1994). Informed Consent in Anthropological Research: We Are Not Exempt. Human Organization, 53(1), 1–10. https://doi.org/10.17730/humo.53.1.178jngk9n57vq685

[17] Fraenkel, J. R., Wallen, N. E., & Hyun, H. H. (2012). How to design and evaluate research in education (8th ed). New York: McGraw-Hill Humanities/Social Sciences/Languages. passim

[18] While many applied economics journals ban the use of deception in experiments, a number of economic publications would still involve deception. Rousu, M. C., Colson, G., Corrigan, J. R., Grebitus, C., & Loureiro, M. L. (2015). Deception in Experiments: Towards Guidelines on use in Applied Economics Research. Applied Economic Perspectives and Policy, 37(3), 524–536. https://doi.org/10.1093/aepp/ppv002

[19] Rep. Act No. 10173 (2012), sec.16 (c).

In a research project involving blood extraction for Complete Blood Count (CBC), for example, denying access to CBC results exhibits disrespect to data subjects. In other research projects, on the other hand, the right to access hardly translates to any straightforward full release of personal information to study subjects. Consider, for instance, a longitudinal study on parenting behaviors and their associations with children's well-being. During the course of the study that would continue to collect data for many years, some parents involved could be asking for their individual parenting scores or "profiles" from the researchers. However, the latter are apprehensive about providing the data, as the release of such highly sensitive, unqualified data is likely to affect the very behaviors they are still in the process of investigating. In this case of an apparent trade-off between potentially undermining research integrity and the full exercise of the right to access, a possible "win-win" solution is for the researchers to provide aggregated data on variables or measures that are unlikely to influence the study subject's future behaviors but are helpful enough to help the parents understand the meaning of their participation in the study.[20]

The data subject's right to access is also intertwined with the right to data portability. Under the law, aside from providing easy access, personal information obtained must be made "data portable" (i.e., personal data capable of being electronically stored and copied any time by the data subject). What is the use of such access rights if the data subjects themselves are unable to take their own information?

[20] Alampay, Liane Peña (personal communication, 16 July 2019).

13

13 A

14

14 A

Further Discussion

D1.2.1. To what extent can your research projects provide access to their participants' own personal data?

Australia's Privacy (Market and Social Research) Code 2014[21] provides exceptions to the granting of the right to access, as follows:

> (a) "the Research Organisation reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
>
> (b) "giving access would have an unreasonable impact on the privacy of other individuals; or
>
> (c) "the request for access is frivolous or vexatious; or
>
> (d) "the information relates to existing or anticipated legal proceedings between the Research Organisation and the individual, and would not be accessible by the process of discovery in those proceedings; or
>
> (e) "giving access would reveal the intentions of the Research Organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
>
> (f) "giving access would be unlawful; or
>
> (g) "denying access is required or authorised by or under an Australian law or a court/tribunal order..." (and 3 more reasons).

Considering these sorts of exceptions to the granting of data subjects' right to access, how feasible is the observance of such right in your own research context?

[21] Office of the Australian Information Commissioner. (n.d.). Privacy (Market and Social Research) Code 2014. Retrieved from https://www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/privacy-market-and-social-research-code-2014

1.3 Right to Data Portability

The right to data portability enables data subjects to move, copy, or transmit personal data easily from one digital environment to another, for whatever purpose they see fit. It is an assurance that data subjects remain "in full control" of their personal data. This right also allows data subjects to manage their personal data with their private devices, and to transmit personal data from one personal information controller [22] to another. It enables the free flow of the subject's personal information across networks and organizations, according to the data subject's preference. This is especially important, as the same data could be reused by different organizations and services. [23]

Further Discussion

D1.3.1. Is the observance of the right to data portability feasible in your research organization?

D1.3.2. Is your project being "research" (and therefore "exempt") ethically sufficient to deny the subject's right to data portability?

D1.3.3. Does data portability apply to data obtained or recorded using analog means?

Definition

7 By "**information controller**" the law refers to a person or organization who controls the collection, holding, processing, or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer, or disclose personal information on his/her behalf. In contrast, "**information processor**" is defined as any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

[22] See section on **Accountability**. Compliance requirements for personal information controllers (PIC) and processors (PIP) are outlined in **Appendix B: Privacy Compliance Matrix.**

[23] Rep. Act No. 10173 (2012), sec. 18

1.4 Right to Object

The person from whom the data was gathered also has the right to object if the personal data processing involved is based on consent or on legitimate interest. When data subjects object or withhold their consent, at any given moment, the researcher must also halt the processing of the subject's personal data, unless the processing is pursuant to a subpoena, for legitimate purposes (contract, employer-employee relationship, etc.) or a legal obligation.[24]

In the EU's General Data Protection Regulation, there are given circumstances when the right to object is less complete, and controllers may be able to continue processing, for instance, if they demonstrate compelling legitimate grounds that override an objector's claims or that the processing is necessary for legal claims or defenses.[25]

Further Discussion

D1.4.1. What if acting on the objection of research participants could irreparably impact the integrity of a researcher's dataset (say, a longitudinal study on a limited subset population)?

D1.4.2. With appropriate safeguards, could an ethics-approved research override a data subject's right to object to the secondary processing of personal data?

[24] Rep. Act No. 10173 (2012), sec. 16.

[25] Mulligan, S. P., Freeman, W. C., & Linebaugh, C. D. (2019). Data Protection Law: An Overview. *Congressional Research Service*, 46. Retrieved from https://fas.org/sgp/crs/misc/R45631.pdf

Right to Erasure or Blocking[26]

Under the law, the subject has the right to "suspend, withdraw or order the blocking, removal or destruction of his/her personal data." The subject can exercise this right upon discovery and substantial proof of the existence of any of the following circumstances: (1) that the subject's personal data is incomplete, outdated, false, or unlawfully obtained; (2) that the data is being used for purposes that the subject did not authorize; (3) that data are no longer necessary for the purposes for which they were collected, (i.e., the researcher does not need the data anymore); (4) that the subject decided to withdraw consent or (5) objects to its processing; (6) that the researcher is processing data unlawfully; (7) that the data concerns information prejudicial to the data subject, unless justified by freedom of speech, of expression, or of the press, or otherwise authorized; or (8) that the subject was a child at the time of collection.[27]

Right to Rectify

The Data Privacy Act also includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. This means that the subject may dispute and have corrected any inaccuracy or error in the data that the researcher holds about him/her. The researcher must act on it immediately and accordingly, unless the request is vexatious or unreasonable. Once corrected, the researcher should ensure the subject's access and receipt of both new and retracted information.

[26] Also known as "the right to be forgotten." For its basis in Philippine law, see Rep. Act No. 10173 (2012), sec. 34 (e); for its intellectual provenance and the European debates surrounding it, see Ausloos, J. (2012). The 'Right to be Forgotten' – Worth remembering? *Computer Law & Security Review*, 28(2), 143–152; and Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, 29(3), 229–235.

[27] Rep. Act No. 10173 (2012), sec. 16 (e).

1.5 Further Discussion

D1.5.1. *Revocation of Consent.* At what junctures could the data subject revoke consent given freely? Could such revocation prove prejudicial to a research project? If so, will you, as a researcher, allow it?

D1.5.2. *Override of right to erasure?* With appropriate safeguards, could an ethics-approved research override a data subject's right to erasure of his own personal data?

Consider an ethics-approved clinical study of a rare disease. A patient has been actively participating in such study for years already when her family decided to immigrate to Australia. She then asked the researchers to drop her from the study and to have all her personal data deleted from the study database and other records. The disease is so rare in the area that it is unlikely the study team could find a suitable replacement. Should such erasure be done?

D1.5.3. *Erasure.* What constitutes an "erasure" of personal data in your information system? If such data is moved to a file that is irreversibly encrypted, does that constitute "erasure"? What would count as erasure in a system (say, blockchain technology) where it would be technically impossible to erase any record because the system is designed to prevent any record erasures at all? What about revoking all access rights to a record, thereby making it invisible to anybody? Is it effectively the same as "erasure"?

Can your research project guarantee complete erasure of personal data if it has an international data sharing agreement or if it has multiple data sources or repositories?

1.6

1.7 Right to Damages & Right to File a Complaint

Further Discussion

D1.6.1. Under what conceivable circumstances could study participants seek to rectify their personal data that the researcher currently holds? Would a research project consider a "grace period" (as part of protocol) beyond which such right is deemed abrogated for the purpose of research?

D1.6.2. With appropriate safeguards to personal data, how do you propose to limit data subjects' access to their personal data in your research?

If data subjects feel that their personal information has been "misused, maliciously disclosed, or improperly disposed" or that any of their data privacy rights have been violated, they have the right to file a complaint. Complaints are to be acted upon within 30 days. If proven, data subjects may claim compensation if they suffered damages due to inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of personal data. [28]

Aside from defining the rights of the data subject, the Data Privacy Act also provides certain limitations to the exercise of these rights. There is leeway if the processed personal information is used only for the needs of scientific and statistical research. It is also imperative that the personal information be held under strict confidentiality and used only for "the declared purpose." [29] However, the "research exemption" clause in the Data Privacy Act of 2012 may not amount to much, insofar as confidentiality and information safeguards are concerned. The law does not sanction breaking confidentiality and breach of personal data, even in research.

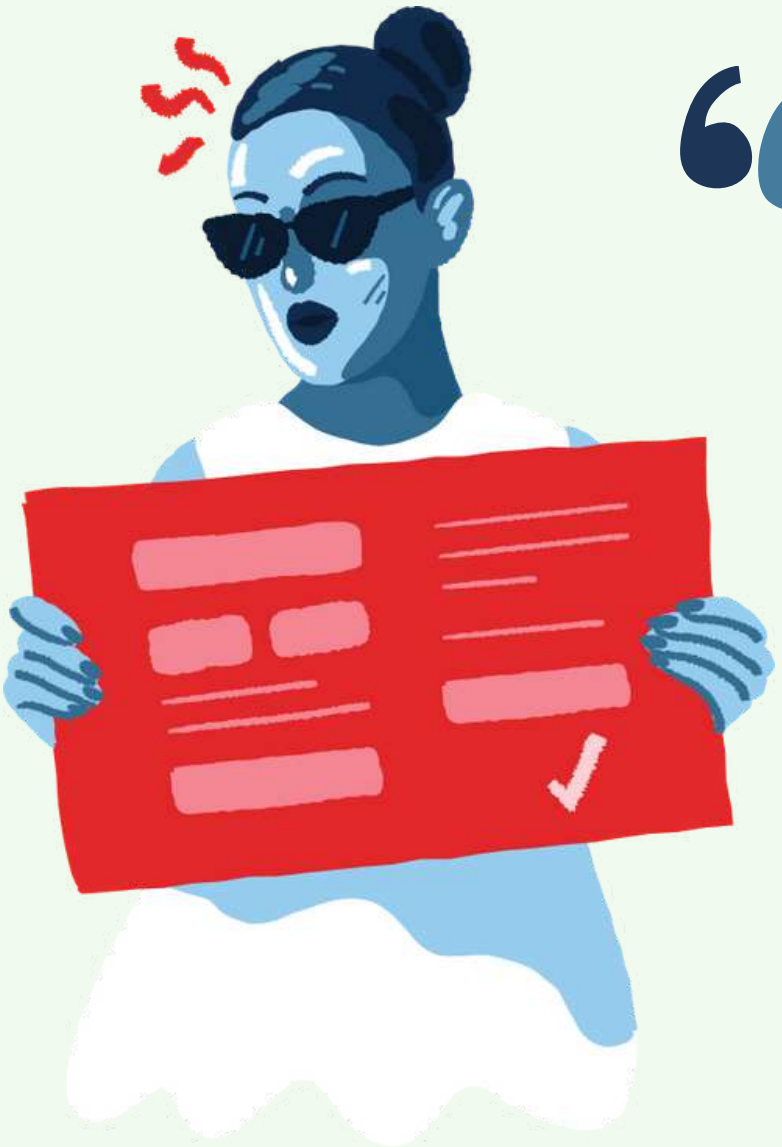
[28] Rep. Act No. 10173 (2012), sec. 16 (f).

[29] IRR of Rep. Act No. 10173 (2016), sec. 37.

Further Discussion

D1.7.1. Is there any complaint mechanism put in place at your institution to handle complaints from data subjects?

There are at least four general principles with respect to the collection and processing of personal data: transparency, legitimate purpose, proportionality, and data quality.[30] All entities covered by the Data Privacy Act and its Implementing Rules must adhere to these principles.



> **The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.**[31]
>
> *(emphasis added)*

02 PRINCIPLES OF DATA PRIVACY

[30] IRR of Rep. Act No. 10173 (2016), sec. 18.

[31] Rep. Act No. 10173 (2012), sec. 11.

2.1

Transparency

The principle of transparency requires that the purpose of processing a person's data should be determined and disclosed before its collection or as soon as practicable.[32] This is the principle behind the right of the data subject to be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the personal information controller, his or her rights as a data subject, and how these can be exercised.[33]

In operational terms, transparency can mean publication of the following in the organization's website or posting them in public areas:

- Privacy Notices
- Data Governance Policies
- Privacy Office Numbers and other Contact Info for Oversight

Privacy notices are an appropriate measure for ALL research. These make more sense especially in studies where consent may not always be obtained. Written in clear and plain language, such notices seek to inform the public and potential data subjects of the nature of an organization's processing activities and the rights available to them. A public notice must include the controller's or the data protection officer's identity and contact information, the intended purposes of the personal information processing, the data retention policy, and, where applicable, whether the data will be transferred to a third party or another country. The notice must indicate the data subject's rights to access, rectification, erasure, and to object to the processing.

Formulating the overall Data Governance of an institution (as opposed to ad hoc, piecemeal considerations of privacy and security issues in diverse research projects) enables researchers and other personnel to effectively navigate through the substance and the technical aspects of privacy and research.

[32] Rep. Act No. 10173 (2012), sec.19 (a) (3).

[33] IRR of Rep. Act No. 10173 (2016), sec. 18 (a).

2.2 Legitimacy of Purpose

This requires that the collection and processing of information must also be compatible with a declared and specified purpose, which must not be contrary to law, morals, or public policy.[34] Personal information must be collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after, collection and later processed in a way compatible with such declared, specified, and legitimate purposes only.[35]

Further Discussion

D2.2.1. Can legitimacy of purpose be the same as "legitimate research"? Can research itself be designated as its own lawful basis for processing of personal data by a research organization (e.g., a survey firm) or as a legitimate interest of the data controller (e.g., employer)?

D2.2.2. Given the requirement for a specific declared purpose to process personal data, are exploratory studies "legitimate"? An exploratory study [36] may focus on a subject with the aim of gaining further insights and not necessarily definitive answers. For instance, you are working on the research question: what are the main factors that contribute to whistleblowers' decision to report to external authorities? In this example, you may start gathering ideas through literature or do exploratory personal data collection that can point to some *potential* factors you are looking for. In other words, can a rather broad purpose of research justify the legitimacy of a research project?

D2.2.3. *Secondary Use of Data.* Should research involving the use of secondary data be allowed, where at the time of data collection only some *broad consent* was used and secondary uses of the data could not be specified? Is processing of personal data for further research purposes allowed, even if such purposes have not been indicated in the *original* consent? If yes, even for purposes that may be incompatible with the purpose indicated in the original consent (but have the potential for new knowledge about "widespread medical conditions" and the "long-term correlation of a number of social conditions" [37])? If not, why not?

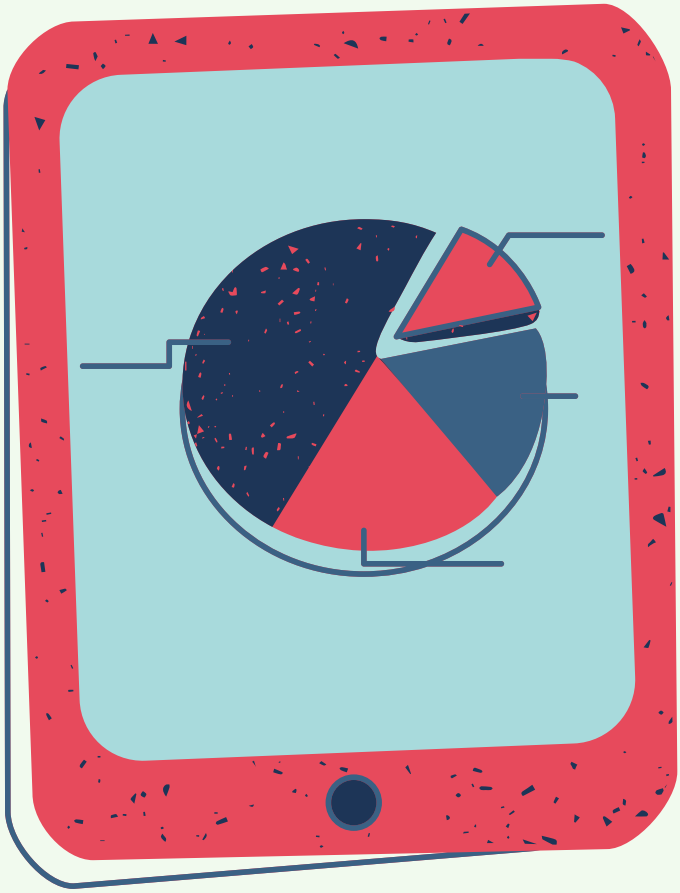
[34] Rep. Act No. 10173 (2012), sec. 18 (b).

[35] Rep. Act No. 10173 (2012), sec. 11 (a).

[36] It is not uncommon to see peer-reviewed, published papers with "exploratory study" in their titles but with no definition of the term in the texts themselves. Many of such papers across disciplines could be demonstrations of the "explorations" that vary in their statements of purpose, deploying diverse methodologies (from the more "open" ethnographic explorations to the more statistical designs). "Potential" is one cognate operative expression: for example, "This exploratory study provides multiple potential future directions for the investigation..." (Sternszus, R., Saroyan, A., & Steinert, Y. (2017). Describing medical student curiosity across a four year curriculum: An exploratory study. *Medical Teacher*, 39(4), 377–382. https://doi.org/10.1080/0142159X.2017.1290793).

[37] Recital 157, GDPR.

2.3 Proportionality



The data subject's information must also prove to be adequate and not excessive in relation to the purposes for which they are collected and processed.[38] The researcher must not collect information beyond the scope of the research.

Further Discussion

D2.3.1. Some studies (e.g., ethnographic) are exploratory and "open" in nature and scope. "Ethnographic fieldnotes, tape-recorded discussions, and information obtained in open-ended interviews may cover a wide range of topics, and not necessarily be limited to the specific focus of investigation."[39] They are hardly predefined. In such cases, how can researchers seek to obtain the "right amount" of information from data subjects when such studies' data collection parameters are not amenable to quantification?

D2.3.2. Does the principle of proportionality mean limitation of data collection in a world of ubiquitous data and apparent willingness of the public to share data (e.g., via social media)?

[38] Rep. Act No. 10173 (2012), sec. 11 (d).

[39] Marshall, P. A. (1992). Research Ethics in Applied Anthropology. IRB: Ethics and Human Research, 14(6), 1. https://doi.org/10.2307/3563851

2.4 Limited Use, Disclosure & Retention

Retention of data must only be for as long as necessary for the fulfillment of the purpose for which the data was obtained or for the establishment, exercise, or defense of legal claims, or for legitimate business purposes, or as provided by law.[40] With proper safeguards and confidentiality protection in place, researcher projects may, however, exercise greater latitude in retaining personal data. With proper de-identification applied to data sets, researchers may keep them for as long as they want.

Further Discussion

D2.4.1. *Limited Use and Retention.* What personal data retention limits do you have for your research?

D2.4.2. *Longitudinal studies.* These are designed to continue for a very long time with potentially indefinite end. Consider, for instance, the Cebu Longitudinal Health and Nutritional Survey, the longest health and nutrition panel study in the country. This is an *ongoing* study of a cohort of Filipino women who gave birth from May 1, 1983, to April 30, 1984, with a current focus on the long-term effects of prenatal and early childhood nutrition and health.[41] Follow-up surveys with selected siblings have been done in the 1990s and 2000s.[42] For this type of research, what policies would you suggest that are consistent with the principle of limited use, disclosure, and retention?

D2.4.3. *Patient Registries.* Maintained for indefinite periods, these databases are meant to be mined for possible answers to legitimate scientific questions. Patient registries can, among others, aid clinical research on rare diseases.[43] They can help facilitate collaboration between researchers and the health industry to address certain medical conditions, benefiting from the accumulation of data or evidence. For such registries to work, however, appropriate design and data elements, written operating procedures, documented methodologies, and appropriate access protocols have to be put in place. How does the principle of limited use, disclosure, and retention apply to patient registries?

D2.4.4. *Retrospective Studies Using Medical Charts.* Conceivably, some legitimate purpose can be had for the use of a training hospital's medical charts for a retrospective study. What privacy rights would need to be observed in that kind of research? Are researchers accessing all the paper medical records directly or just copies with redacted identifiers? How is confidentiality maintained here? Are you only using tabular, de-identified data culled from medical charts? Is your methodology privacy-preserving? Does it justify the potential undermining of the principle of limited use and disclosure?[44]

[40] Rep. Act No. 10173 (2012), sec. 11 (e).

[41] Adair, L., & Popkin, B. (2001). The Cebu longitudinal health and nutrition survey: history and major contributions of the project. Philippine Quarterly of Culture and Society, 29(1/2), 5-37. Retrieved from http://www.jstor.org/stable/29792482

[42] Carolina Population Center. (n.d.). Cebu Longitudinal Health and Nutrition Survey. Retrieved May 2, 2019, from https://cpc.unc.edu/projects/cebu

[43] The Rare Disease Registry is government-mandated, requiring that "all patients diagnosed with rare disease shall be included" in such registry, with no clear opt-out option. "All healthcare practitioners and health care institutions shall be required to report to the Rare Disease Registry based in NIH diagnosed cases of rare disease and provide reports on the status of patients" (Rep Act 10747, Sec. 5&6). In the Philippines, a disease is "rare" if it affects one in every 20,000 individuals or less (Junio, L. (2017, October 19). PGH awaits IRR on rare disease law. Retrieved May 7, 2019, from https://www.pna.gov.ph/articles/1013159). The IRR of RA 10747 defines "rare diseases" as "disorders such as inherited metabolic disorders and other diseases with rare occurrence as recognized by the DOH upon recommendation of the NIH." That excludes "catastrophic (i.e., life threatening, seriously debilitating, or serious and chronic) forms of more frequently occurring diseases" (DOH Memorandum Circular 2017-0039, 23 November 2017, Implementing Rules and Regulations (IRR) of Republic Act No. 10747 entitled "An Act Promulgating a Comprehensive Policy in Addressing the Needs of Persons with Rare Disease," otherwise known as the "Rare Diseases Act of the Philippines"). Worldwide, knowledge and training on rare diseases are scarce (Khosla, N., & Valdez, R. (2018). A compilation of national plans, policies and government actions for rare diseases in 23 countries. *Intractable & Rare Diseases Research*, 7(4), 213–222. https://doi.org/10.5582/irdr.2018.01085).

[44] In the absence of appropriate databases or other secondary sources of information, medical charts are often used to do "retrospective studies." Granted that important institutional requirements like ethics review have already been complied with, methodological concerns are also raised against retrospective research. Are patients' rights really worth derogating for what otherwise might be a methodologically suspect research? See Vassar, M., & Holzmann, M. (2013). The retrospective chart review: important methodological considerations. Journal of Educational Evaluation for Health Professions, 10, 12. https://doi.org/10.3352/jeehp.2013.10.12

2.5 Consent

Consent provides an important legal basis for processing personal data in research (and elsewhere). Once the data subjects have given their consent, the processing of their personal information shall be allowed unless otherwise prohibited by law.[45] While consent is *not the only* legal basis for personal data processing,[46] it appears to be causing the most confusion.

Consent of data subjects refers to any freely given, specific, informed indication of will, whereby the data subjects agree to the collection and processing of personal information about or relating to them. Consent shall be evidenced by written, electronic, or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.[47] The consent explicitness requirement under the law is even made more compelling in the light of the recent enactment of the EU's General Data Protection Regulation (GDPR), the *de facto* international data privacy standards. The GDPR insists that "valid consent for taking data needs to be clear and affirmative (it cannot be silent or 'inferred' by inactivity)."[48] In the context of research, however, the GDPR allows for certain "derogations" or curtailments of the original regulation to accommodate, among others, the exercise of legitimate scientific inquiries.[49] This is especially relevant when we consider how "blanket requirements for explicit consent for the use of individuals' identifiable data" can threaten research integrity. In an observation research, for instance, insistence on explicit consent was found to have biased the results in "disease registers, epidemiological studies, and health services research."[50]

In operational terms, *in addition* to what your ethics committee requires, researchers should include in their Consent Form the following items:

- purpose of the research,
- data retention plan (including archiving and sharing arrangements),
- concrete measures to safeguard the confidentiality of personal data, and
- steps to take in the exercise of one's right to withdraw from the research and the other rights of a data subject.

Consent Template

privacyph.org/consent

[45] Rep. Act No. 10173 (2012), sec. 12 (a).

[46] Other legal bases for personal information processing include contracts, legal obligations, public duties, vital, or other legitimate interests (like medical emergencies). See Rep. Act No. 10173 (2012), sec. 12; IRR of Rep. Act No. 10173 (2016), sec. 19, 20, 21

[47] Rep. Act No. 10173 (2012), sec. 3 (b).

[48] Pels, P., Boog, I., Henrike Florusbosch, J., Kripe, Z., Minter, T., Postma, M., ... & von Poser, A. (2018). Data management in anthropology: the next phase in ethics governance?. *Social Anthropology*, 26(3), 391-413.

[49] Article 89 (GDPR): "Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes." There is also greater latitude on secondary processing and on processing sensitive categories of data (Article 6(4); Recital 50).

[50] Al-Shahi, R., Vousden, C., & Warlow, C. (2005). Bias from requiring explicit consent from all participants in observational research: prospective, population based study. BMJ, 331(7522), 942. https://doi.org/10.1136/bmj.38624.397569.68

The consent document may also indicate the limits of confidentiality, "such as when the researcher is ethically and legally obligated to disclose the identity of the respondent to forestall imminent harm to self or others." [51] Child abuse, substance abuse, violence against women, self-harm, suicide ideation, criminal activities—if such activities are likely to be observed in research and the researcher is required by law to disclose, then the consent document must indicate the possibility of breaking confidentiality.

In many occasions, researchers and ethics committees tend to overemphasize the information disclosure or the "form" aspect of consent. Other elements of consent are equally (if not more) important.

Take understanding. The worst kind of consent are those litanies of legalese that some researchers have been advised to indicate in their consent forms, without any due consideration of their readability. Others would go hyper-creative with their visuals, which tends to overwhelm research participants and knock them out of their own pace of absorbing information and relating to the research situation. Understanding and consent-giving are dynamic processes that tend to do well with conversations. "Having a study team member or a neutral educator spend more time talking one-on-one to study participants appears to be the most effective available way of improving research participants' understanding..." [52]

Further Discussion

D2.5.1. *Verbal Consent,* especially from illiterate and vulnerable individuals or groups. [53] Does their vulnerability abrogate the prospect of obtaining any meaningful consent?

D2.5.2. *Waived Consent.* [54] The 2017 National Ethical Guidelines for Health and Health-Related Research lays down the conditions under which research ethics committees (RECs) could waive the informed consent requirement in *exceptional* cases. Such cases include archival research involving publicly available documents and minimally risky social or behavioral studies that necessitate or justify the use of covert methodologies in data collection. What privacy measures are needed in cases where an ethics committee waives the consent requirement?

Technically, what is really being waived? Is it the consent process itself or just the requirement to obtain a signed informed consent *form* from participants or a *documentation* of the consent process? With appropriate disclosure of relevant information, doesn't *any* research always involve *consent-making* with research subjects, their legal representatives, their advocates, and oversight bodies? Without this *spirit* of the consent process, how else could research be transparent and accountable?

[51] Philippine Health Research Ethics Board (2017). *National ethical guidelines for health and health related research.* Manila: Department of Science and Technology-Philippine Council for Health Research Development.

[52] Flory, J., Emanuel, E. (2004). Interventions to improve research participants' understanding in informed consent for research: A systematic review. *Journal of the American Medical Association,* 292, 1593-1601.

[53] "[A]ny population or group within a society must be considered vulnerable if they lack basic rights and freedoms that form an essential part of choosing the basic course of their life." Zion, D., Gillam, L., & Loff, B. (2000). The Declaration of Helsinki, CIOMS and the ethics of research on vulnerable populations. *Nature Medicine,* 6, 615–617. https://doi.org/10.1038/76174. For the illiterate, thumb marks are possible substitutes for signatures, with attestation from credible witnesses.

[54] See separate discussion on **Standards for Waived Consent**. As it applies to research involving patient or medical records, see also Melton, L. J. (1997). The Threat to Medical-Records Research. New England Journal of Medicine, 337(20), 1466–1470. https://doi.org/10.1056/NEJM199711133372012. For the significance of waived consent in patient registries, see Tu, J. V., Willison, D. J., Silver, F. L., Fang, J., Richards, J. A., Laupacis, A., Investigators in the Registry of the Canadian Stroke Network. (2004). Impracticability of informed consent in the Registry of the Canadian Stroke Network. The New England Journal of Medicine, 350(14), 1414–1421. https://doi.org/10.1056/NEJMsa031697

Further Discussion

D2.5.3. *Informed Consent without Forms.* In some studies involving the use of participant observations, intrusive and unnecessarily legalistic consent forms could threaten the integrity of research.[55] Nonetheless, the spirit of informed consent could still be fulfilled by incorporating the same concerns into the larger research process "that encourages greater openness and disclosure on the part of researchers, empowers voluntary participants in social research, and engenders a more collaborative relationship between researcher and researched."[56]

One way of doing informed consent without forms is through "visual informed consent."[57] This involves the visual capture of a participant's understanding and agreement to participate, especially in situations where "the conventional 'consent form' is so irrelevant as to be a nuisance to all parties."[58]

In your own research, is it appropriate to obtain "informed consent without forms" from your participants? If so, how would you do that?

D2.5.4. *Publicly Available Personal Information.* Secondary research involving publicly available personal data and identifiable biospecimens. Generally, social media data, for instance, are publicly available for analysis or via APIs.[59] Could you fairly assume that the producers or owners of such publicly available social media data would not mind that their information is being processed for research?[60] Is the user's consent via a social media platform's "service agreement" sufficient?

D2.5.5. *Re-consent.* Information obtained from data subjects for a particular study may turn out to be valuable for further studies. If the original consent was clearly limited to only the original study, to the extent it is feasible to re-contact the data subjects concerned, another consent for a follow-up or derivative study might be sought.

Should longitudinal studies involving children seek re-consent once their participants reach adulthood?

However, for cases where re-contact with data subjects is not feasible, an ethics clearance from a duly accredited research ethics committee (REC) is recommended. Are you familiar with any research done with a similar arrangement? Is it justified?

D2.5.6. *Consent in Studies during Emergencies.* What mechanism might be put in lieu of consent in research in emergency

[55] In some studies on language and sexuality, for instance, "institutionalized informed consent procedures may undercut [participants'] agency and expose [them to] symbolic violence." See Mortensen, K. K. (2015). Informed consent in the field of language and sexuality: The case of online dating research. *Journal of Language and Sexuality*, 4(1), 1–29. https://doi.org/10.1075/jls.4.1.01mor

[56] Fluehr-Lobban, 1994.

[57] Lie, R., & Witteveen, L. (2017). Visual informed consent: informed consent without forms. *International Journal of Social Research Methodology*, 20(1), 63–75. https://doi.org/10.1080/13645579.2015.1116835

[58] Wax, M. L. (1980). Paradoxes of 'consent' to the practice of fieldwork. Social Problems, 27, 272–283

[59] A set of rules, routines, protocols, or tools, an application program interface (API) is used by programmers and researchers to access social media data. It specifies how software components interact with each other.

[60] In a study, about 80% of social media users expected to be asked for consent if their social media information is used for research (Williams, M. L., Burnap, P., & Sloan, L. (2017). Towards an ethical framework for publishing Twitter data in social research: Taking into account users' views, online context and algorithmic estimation. Sociology, 51(6), 1149–1168).

Further Discussion

medicine? Responding to medical emergencies, especially when the patient is unconscious and an authorized representative is nowhere in sight, does not require consent. But what about doing studies under that kind of condition? Who could be "waiving" consent, when there is no time to convene the REC?

D2.5.7. *Big Data.* In big data research,[61] researchers are mostly dealing with data types generated not necessarily for research; explicit written consent might not have been considered to begin with. Among the most commonly used big data are administrative data, commercial transaction records, social media data, geospatial data, and images.[62] Such data become available almost as "a matter of course" in contemporary societies. These may include information from transactions with reasonable expectation of privacy. Such data have been put together en masse for analysis, mostly oblivious to consent limitations at data source. Are you familiar with any big data research that might justify the abrogation of the consent requirement?

D2.5.8. *Genetic Studies.*[63] A consent for one's genetic materials or data might give away information on other family members who do not necessarily give consent to the study. Are the privacy concerns of family members (secondary subjects) also being considered? How would you maintain data privacy with this kind of research?

D2.5.9. *Third-party information.*[64] Certain research involving human subjects may implicate other data subjects. For instance, certain psychiatric studies tend to also include information on the mental health of parents and relatives. Research on social determinants of health tends to collect "third-party information" from family, relatives, or friends. It is unlikely that such research is able to get consent from third parties. How do you manage the privacy rights of these third-party individuals who are not even your research participants?

D2.5.10. *Open Consent.*[65] Research subjects who sign up with open consent cannot be guaranteed anonymity, privacy, or confidentiality. Their personal data are stored in publicly accessible databases. While they can withdraw from the research, there is no guarantee that their data can be completely removed, even if they so wish later. Is this situation tenable? Why or why not?

[61] An argument can be made that big data research is not necessarily human subjects research and therefore not subject to research ethics review. For instance, using publicly available online user accounts and profiles, so the argument goes, are mere representations of people, not necessarily the people themselves. Many of these user profiles could also be fake or inactive (Gerwin van Schie, Irene Westra & Mirko Tobias Schäfer, 2017:183ff).

[62] OECD. (2013). *New Data for Understanding the Human Condition: International Perspectives*. Retrieved from http://www.oecd.org/sti/inno/new-data-for-understanding-the-human-condition.pdf

[63] For more discussion on issues in genetic privacy, see, for instance: Taylor, M. (2012). *Genetic data and the law: a critical perspective on privacy protection*. In Cambridge Bioethics and Law. Cambridge ; New York: Cambridge University Press.

[64] For more discussion on issues in genetic privacy, see, for instance: Taylor, M. (2012). *Genetic data and the law: a critical perspective on privacy protection*. In Cambridge Bioethics and Law. Cambridge ; New York: Cambridge University Press.

[65] See, for instance, Personal Genome Project (PGP): www.personalgenomes.org. In this type of study, there is no direct benefit to research participants and the genetic information shared may even harm them. For more discussion on the privacy and consent implications of PGP, see Lunshof, J. E., Chadwick, R., Vorhaus, D. B., & Church, G. M. (2008). From genetic privacy to open consent. *Nature Reviews Genetics*, 9(5), 406–411. https://doi.org/10.1038/nrg2360

2.6 Accountability

The *ultimate* accountability in data privacy lies with the Personal Information Controller (PIC).[66] Each personal information controller is **responsible for personal information under its control or custody**, including information transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.[67]

Further Discussion

D2.6.1. Does your research project indicate clear accountability? Is everyone in the project clear about who are information controllers and processors and data custodians?

[66] Rep. Act No. 10173 (2012), sec. 21 (a).

[67] Rep. Act No. 10173 (2012), sec. 21.

2.7 Security

A research organization must implement reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing. Reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and against human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination, must also be implemented.[68] The determination of the appropriate level of security depends on the nature of the research and the type of data to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices, and the cost of security implementation.[69]

For many people, information security is just perceived as a bureaucratic nuisance or some regulatory hurdle. However, with recent security breaches, businesses could be shut down,[70] health services paralyzed,[71] and personal lives ruined[72]—information security is hardly optional anymore in most facets of modern life and research.

Further Discussion

D2.7.1. What are the security measures that your research requires but fellow researchers are finding to cause inefficiencies or some other unintended, unforeseen negative consequences?

[68] Rep. Act No. 10173 (2012), sec. 20 (b).

[69] Rep. Act No. 10173 (2012), sec. 20 (c).

[70] On May 2, 2018, the National Privacy Commission (NPC) issued an order obliging Wendy's Philippines to inform all the concerned customers whose personal information had been exposed, about the data breach of its website. For this reason, Wendy's had to close their delivery website temporarily. Similarly, the NPC also ordered Jollibee Foods Corporation on May 8, 2018, to shut down its online delivery service due to the security vulnerabilities of its website. The commission reported that the data of approximately 18 million people found in their delivery database were at risk to unauthorized access. Marcelo, P. C. (2018, May 10). JFC shuts delivery websites due to vulnerabilities. *BusinessWorld*. Retrieved May 3, 2019, from https://www.bworldonline.com/jfc-shuts-delivery-websites-due-to-vulnerabilities/

[71] Gordon, W. J., Fairhall, A., & Landman, A. (2017). Threats to Information Security — Public Health Implications. *New England Journal of Medicine, 377(8)*, 707-709. doi:10.1056/nejmp1707212

[72] A high-profile case of personal information breach is that of celebrity physician Hayden Kho's sex video scandal which involved the illicit retrieval of sex videos from Kho's computer and its subsequent distribution online and in the country's pirated DVD market. See Mendoza, C. V. (2012). Balancing of interest in the digital age: Protection of the rights of offended parties and the constitutional rights of the accused in the context of sex scandals. Philippine Law Journal, 86(2), 356-404.

03 CONTEXTUAL ISSUES

Data privacy is *context-sensitive.* Just following a list of requirements to address compliance risks will elude research-specific concerns, including the very impact of privacy on healthcare and other services, research efficiency, selection bias and participant willingness, access to health records and other vital information, and the quality of data sets.[73] Privacy scholar Helen Nissenbaum points to the need to consider such "context-relative informational norms" to maintain contextual integrity and serve as a "benchmark for privacy, yielding assessments that reflect common sentiment and map well onto judgments that privacy has been violated."[74] These informational norms and privacy preferences can vary both between different technologies in the same country and between different countries for the same "technology,"[75] often resulting in "tension…between… the respect for 'local informational norms' and the wish to agree on global informational norms."[76]

Most of all, research is its very own immediate context. While it is important to take stock of the larger cultural, social regulatory context of research, its operational challenges, and impact on human subjects, research seeks its own contextual integrity that goes beyond mere accounting of the risks that come with personal data processing. An effective implementation of privacy policies, therefore, has to be cognizant of these highly contextual concerns to address these challenges that privacy regulation brings to research.

---

[73] IOM (Institute of Medicine). (2009). *Beyond the HIPAA privacy rule: enhancing privacy, improving health through research*. Washington, D.C: National Academies Press, 209-235.

[74] Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books, an imprint of Stanford University Press, 140.

[75] Busch, A. (2015). Privacy, technology, and regulation: Why one size is unlikely to fit all. In B. Rössler & D. Mokrosińska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 303–323). Cambridge University Press, 316.

[76] Busch, 2015:318.

3.1 Operational Challenges

3.1.1 Selection Bias

Compliance with privacy regulation potentially entails selection bias when individuals who give their consent do not accurately reflect the target population. Such unrepresentative or statistically insignificant samples could lead to inaccurate results and reduce its generalizability to the target population.[77] For instance, complicated and lengthy authorization forms have been identified as a significant impediment to the recruitment of data subjects, risking the likelihood of underrepresentation of minority populations.[78] Special attention may be given to obtaining informed consent in social research or clinical trials involving deaf people,[79] persons with cognitive impairment, mental disability or disorder;[80, 81] the illiterate,[82] and other potential data subjects whose condition may put some limitations to the process of obtaining informed consent. Nevertheless, as Rothstein and Shoben (2013) argue, "beneficial scientific ends do not justify oppressive means."[83]

Concerns over selection bias have been exaggerated, as the degree of consent bias in research is below an acceptable level of imprecision, constituting "a reasonable cost for conducting ethically responsible research,"[84] and that the employment of "sound research methodologies" and statistical methods can account for and minimize selection bias.[85]

3.1.2 Timely Access to Health or Other Vital Information

In many instances, timely access to medical records can be a crucial factor in research requiring early contact with patients after diagnosis. Rapid case ascertainment, for instance, involved flipping through patient medical records in cancer registries to contact potential participants for population-based studies. Such a method for recruitment, while ensuring high

[77] Institute of Medicine, 2009:209.

[78] Institute of Medicine, 2009:209-210.

[79] Penn, C., & De Andrade, V. (2017). Informed consent and deafness in South Africa: Guidelines for clinicians and researchers. *South African Journal of Bioethics and Law*, 10(2), 58. https://doi.org/10.7196/SAJBL.2017.v10i2.541

[80] Amer, A. B. (2013). Informed Consent in Adult Psychiatry. *Oman Medical Journal*, 28(4), 228–231.

[81] Van Staden, C. W. (2003). Incapacity to give informed consent owing to mental disorder. *Journal of Medical Ethics*, 29(1), 41–43. https://doi.org/10.1136/jme.29.1.41

[82] Alaei, M., Pourshams, A., Altaha, N., Goglani, G., & Jafari, E. (2013). Obtaining informed consent in an illiterate population. *Middle East Journal of Digestive Diseases*, 5(1), 37–40.

[83] Rothstein, M. A., & Shoben, A. B. (2013). Does Consent Bias Research? *The American Journal of Bioethics*, 13(4), 27–37. https://doi.org/10.1080/15265161.2013.767955

[84] Rothstein & Shoben, 2013:27.

[85] Rothstein & Shoben, 2013:35.

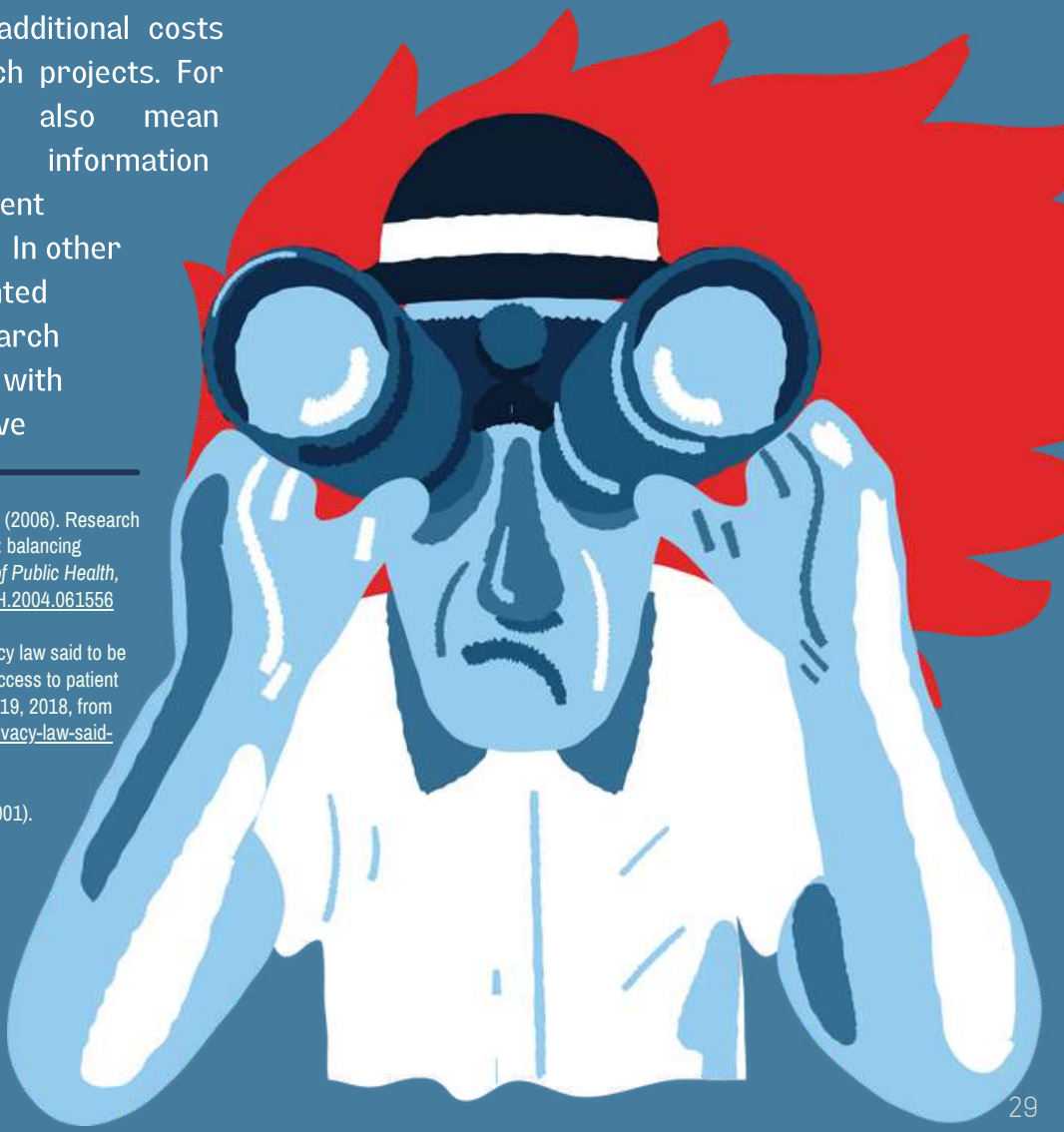
participation rates and, consequently, the validity and generalizability of research findings, involves the risk of invasion of privacy, especially if such sensitive information is misused. [86] Conservative readings of privacy regulation, therefore, can potentially threaten life-saving research that needs to be done within a specific time frame. As one researcher succinctly and grimly puts it, "We study a disease that will kill you in three months. If we wait a year, we won't have any subjects to study." [87]

Where there is access to health or other vital information, it comes too little, too late. Complex approval processes preclude timely and efficient research.

3.1.3
Research Efficiency

Privacy compliance entails additional costs and staff hours for research projects. For many institutions, it can also mean expensive upgrades of information systems, revision of employment contracts, and monitoring. [88] In other countries that have implemented similar privacy regimes, research projects have been burdened with delays and, in some cases, have resulted in the abandonment of some projects. [89] In the case of the United States' sectoral HIPAA Privacy Rule, research recruitment had also been negatively impacted, as "research assistants could no longer approach potential research participants; recruitment was done by hospital staff." [90] In addition, researchers impacted by privacy regulation often find it difficult to gain access to quality anonymized data sets. [91]

Lastly, the fear of incurring criminal liability and legal consequences may lead organizations to impede researcher access to data, as well as make research ethics committees to be overly conservative in their application of privacy provisions in reviewing new proposals. [92]



[86] Beskow, L. M., Sandler, R. S., & Weinberger, M. (2006). Research recruitment through US central cancer registries: balancing privacy and scientific issues. *American Journal of Public Health*, 96(11), 1920–1926. https://doi.org/10.2105/AJPH.2004.061556

[87] Russell, S. (2004, September 26). Medical privacy law said to be chilling medical studies, scientists fight for fast access to patient files. San Francisco Chronicle. Retrieved March 19, 2018, from https://www.sfgate.com/health/article/Medical-privacy-law-said-to-be-chilling-cancer-2691744.php

[88] Protecting patient privacy: striking a balance. (2001). Lancet (London, England), 358(9282), 597.

[89] Institute of Medicine, 2009:214-218.

[90] Institute of Medicine, 2009:218-220.

[91] Institute of Medicine, 2009:231-233.

[92] Institute of Medicine, 2009:235.

3.2 Data Sharing

As data tends to be generated at every digital turn these days, the focus on the sharing of personal information might prove more important than mere data collection. As information scientists Wu et al. (2019) put it, "Investigating how individuals, groups, and businesses deal with information sharing in all types of contexts is critical... to designing privacy-sensitive tools that address the needs and concerns of a wider range of users and communities." [93]

Data sharing among researchers and research institutions is an integral part of the scientific enterprise.[94] Transparency and openness in sharing data helps ensure the scholarly integrity of research output. Data sharing agreements that enable international collaboration are crucial, for instance, to many health-related studies: "having international data is important to study a health problem."

[93] Wu, P. F., Vitak, J., & Zimmer, M. T. (2019). A contextual approach to information privacy research. Journal of the Association for Information Science and Technology, asi.24232. https://doi.org/10.1002/asi.24232

[94] Diverse research practices dictate the extent of data sharing. Sociology: "As a regular practice, sociologists share data and pertinent documentation as an integral part of a research plan" (ASA Code of Ethics). The Inter-university Consortium for Political and Social Research (ICPSR) houses the Data Sharing for Demographic Research (DSDR) that covers a range of activities, including "archiving, preserving, and disseminating data relevant for population studies" (ICPSR. (n.d.). What is DSDR? Retrieved May 31, 2019, from https://www.icpsr.umich.edu/icpsrweb/content/DSDR/about.html).

Further Discussion

D3.1.1. *Selection Bias.* Rothstein and Shoben (2013) argue that the level of selection bias entailed by privacy compliance is acceptable and is a reasonable social cost for respecting the individual's right to privacy. In addition, statistical methods can usually account for this bias. In your experience, are there cases where selection bias becomes unacceptable as a result of privacy or ethics rules?

D3.1.2. *Timely Access to Health Information.* In the Philippine setting, under what conceivable circumstances could privacy compliance hamper the timely access to health information (e.g., cancer registries, rapid case ascertainment)?

D3.1.3. *Additional Costs and Labor.* With your research project, how much do you think will compliance with the Data Privacy Act cost in terms of staff hours and related expenses?

D3.1.4. *Project Abandonment.* Do you have any personal knowledge about research projects abandoned, with privacy or ethics compliance being one of the reasons?

D3.1.5. *Research Recruitment.* How will the Data Privacy Act affect research recruitment and accrual of subjects?

D3.1.6. *Quality of Anonymized Data.* Have you encountered issues in the quality of anonymized or de-identified data sets? If so, what are these?

D3.1.7. *Accessing Data Sets from Organizations.* Do you know of any organization that is reluctant to provide data sets to researchers in light of the Data Privacy Act?

D3.1.8. *Secondary Use.* To what extent can data sets collected primarily for administrative purposes (e.g., student admission, tax payment, land registration, business permits) or collected from financial transactions (e.g., Grab rides, credit card payments, online orders) be used for research (secondary use)?

However, sharing data involving human subjects can pose significant threats to privacy. Formed in 1974, a study group on privacy in research of the British Association for the Advancement of Science (now the British Science Association) expressed concern over the conflation of administrative and research data. The Association notes that while it is common for administrative and research uses to be distinguished,

> "...[t]he same files and the same computers are often used for both [administrative and research data], and data is sometimes put into administrative files for purely research purposes.... [T]his practice is often unnecessary and must be considered unacceptable: the anonymity and security of research data will be protected only by drawing a sharp line between research and administrative data, *both in collection and in use.* Once that separation has been made, it is then possible to look at the two halves separately."[95] [italics supplied]

In the Philippines, the National Privacy Commission only allows data sharing "when there are adequate safeguards for data privacy and security," using "contractual or other reasonable means to ensure that personal data is covered by a consistent level of protection when it is shared or transferred."[96]

Data agreements across state borders will also have to deal with different privacy regimes. For example, the implementation of the HIPAA Privacy Rule in the United States had led to missing data (e.g., age of research participants) in US health research centers collaborating with Dutch counterparts as a result of overly conservative or variable policy interpretations, making it difficult to monitor for selection bias and quality.[97]

With the sharing of personal data between organizations across borders, a data sharing agreement has to spell out the jurisdictional authorities as well as controller and processor commitments relating particular data sets. Such commitments include security (encryption, login, and audit details), data deletion, destruction, or retention.

Further Discussion

D3.2.1. Under what circumstances can a research organization transfer personal data to another country? Can researchers share data without the data subject's consent?

D3.2.2. *Archiving of data in another country.* For the benefit of the international scientific community, data sets are at times archived in foreign facilities. For instance, data from the Cebu Longitudinal Health and Nutrition Survey are available at the UNC Dataverse,[98] a publicly accessible repository, aiding the publication of hundreds of scientific papers.[99] What practical constraints does the current privacy regulation pose to such kind of data sharing practice?

[95] British Association Study Group, 1979:42.

[96] NPC Circular No. 16-02 (2016), sec. 12. This Circular governs data sharing agreements between government agencies and private third parties (and vice versa) "to facilitate the performance of a public function or the provision of a public service."

[97] Institute of Medicine, 2009:228.

[98] See Cebu Longitudinal Health and Nutrition Survey Dataverse (Carolina Population Center, University of North Carolina at Chapel Hill): https://dataverse.unc.edu/dataverse/cebu

[99] Carolina Population Center. (n.d.). Publications — Cebu Longitudinal Health and Nutrition Survey. Retrieved May 2, 2019, from https://dataverse.unc.edu/dataverse/cebu

3.2.1 The Marginalized

Is there strong privacy protection for marginalized individuals and groups in society whose personal data are shared among researchers? The marginalized tend to be researched disproportionately more than the powerful.

3.2.2 Persistence of Sharedness

Data sharing in networked and globalized society is about persistent information. While research subjects have nominal rights to erasure or to be forgotten, data (personal or otherwise) shared across networks and archived redundantly tend to outlast the wishes of their original owners. Destruction of data in one source does not guarantee complete destruction at all. Ownership of data is not the same as access to data.

3.3 Privacy & Filipino Culture

Filipinos are a "highly relational people."[100] While much of research is driven by the scientific question being answered or by methodology and design considerations, actual participation in Philippine research is relational rather than simply transactional.

Privacy, as the right to be "left alone," may prove dissonant in the face of social values like *pakikisama* ("getting along well with others") and Filipinos' tendency to pry into the private lives of others. Especially in rural areas, privacy can be "a matter of definition," ranging from women changing their dress inside their rooms, to "men simply turn[ing] their backs and [facing] the corner" to change clothes.[101] These cultural nuances can potentially erode values of respect for individual privacy and elicit a mixed reception of privacy regulation in the country.

Antonio et al. (2016)[102] highlight two infamous cases that illustrate how such cultural insensitivity to individual privacy concerns might come into play with privacy regulation. The first case was the notorious 2008 Cebu Canister Scandal, where a video documenting the extraction of a metal canister spray from the rectum of a patient

Further Discussion

D3.3.1. *International Collaboration.* Do you have direct knowledge about any issues in doing international collaboration with researchers coping with different privacy requirements (e.g., the EU's GDPR or US HIPAA Privacy Rule and the Philippines' DPA)?

D3.3.2. What other Filipino traits and practices may adversely impact compliance of privacy regulation in research?

D3.3.3. What aspects of research might be affected by the dominance of social media in the Philippines?

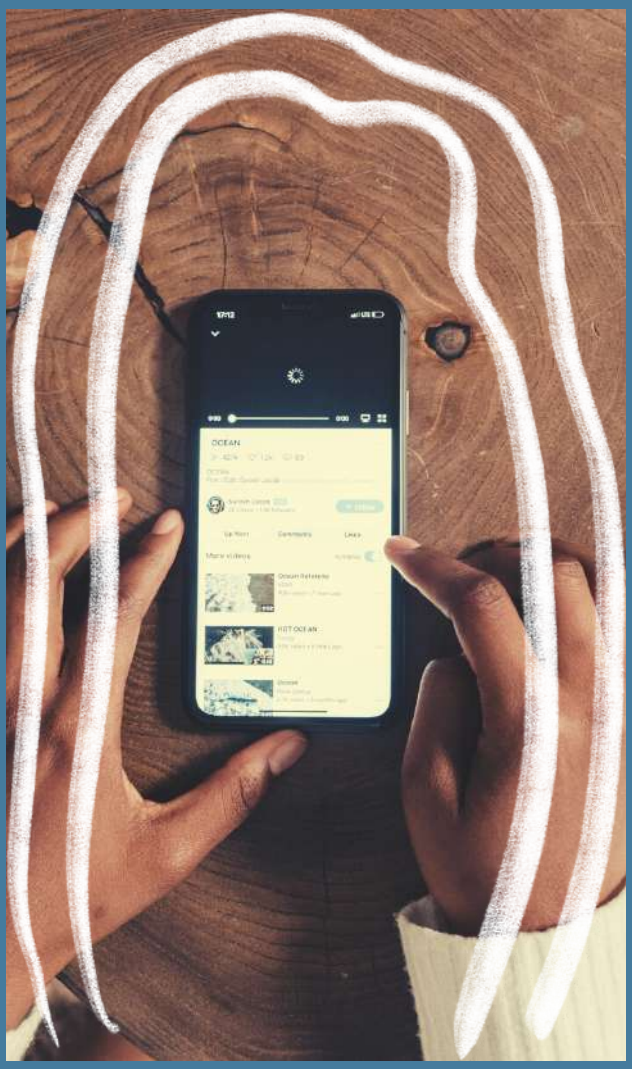
[100] De Leon, F. M., Jr. (2011, July 29). In Focus: The Cultural Matrix of Philippine Traditional Arts. Retrieved March 14, 2018, from http://ncca.gov.ph/about-culture-and-arts/in-focus/the-cultural-matrix-of-philippine-traditional-arts/

[101] Jocano, F. L. (1972). Cultural Idiom and the Problem of Planned Change: A Case Study from a Philippine Municipality. *Asian Studies: Journal of Critical Perspectives from Asia* 10(2), 174.

[102] Antonio, C., Patdu, I., & Marcelo, A. (2016). Health Information Privacy in the Philippines: Trends and Challenges in Policy and Practice. *Acta Medica Philippina*, 50(4), 223–236.

was posted on Youtube without his knowledge and consent. Gawking and jeering hospital staff, including those not directly involved, congregating in the operating room, were also shown in the video. The patient, who was asleep during the medical procedure, was only informed by his barangay captain when the video went "viral." Whoever posted it online was never identified; the hospital staff involved were only penalized with a three-month preventive suspension, the cases filed against them with the Professional Regulation Commission having failed due to a technicality. [103]

The second case is about how sensitive details of then-President Gloria Arroyo's 2009 visit to the Asian Hospital in Manila were leaked to the press. Investigation by the hospital and state authorities revealed that it was non-medical hospital personnel who accessed the President's record and divulged it to a newspaper columnist. Antonio et al. assert that what Arroyo's case highlights is the "possibility of unlimited access to patient files in a centralized electronic medical records database by outsiders who are not directly involved in the care of the patient." They even note that the counsel for the accused physician pointed out that around 76 hospital staff had access to those records. [104] Antonio et al. point to the "pervasiveness of *tsismis* (gossip) in



Filipino culture" despite the legal and ethical safeguards put in place. [105] Aggravating the privacy situation is the high ICT and social media penetration rate, not only in the country, but across Southeast Asia. [106] Such technological developments have only been increasing since 2008, "[outpacing] policy and practice."

[103] Antonio et al., 2016:230-231.

[104] Antonio et al., 2016:231.

[105] Antonio et al., 2016:232.

[106] Kemp, S. (2017, February 16). Digital in Southeast Asia in 2017. We Are Social. Retrieved July 16, 2021. https://wearesocial.com/special-reports/digital-southeast-asia-2017

3.4 The Research Context

Context is multidimensional, and research is also its own context. When researchers insert themselves into different social or data situations, they are expected to "read" them correctly. Each situation has its own contextual integrity that people are emotionally or personally invested in. It is not merely the sharing of personal information per se that upsets people, but the breaking of its contextual integrity.[107] In social media research, for instance, part of the context could be that of researchers belonging to the same network as that of some data subjects or that they have common "friends" on the platform. In this situation, just because the researcher is able to access the profile and other personal information of the data subject, it cannot be assumed that the data are "publicly available" nor that the data sources do not care about their privacy.

No two research projects are the same. With all the relationships (perceived or real) formed around research-related interactions, a research project also tends to define the limits of data utilization. As privacy researchers Zook et al. put it,

> ***Just because something has been shared publicly does not mean any subsequent use would be unproblematic. Looking at a single Instagram photo by an individual has different ethical implications than looking at someone's full history of all social media posts. Privacy depends on the nature of the data, the context in which they were created and obtained, and the expectations and norms of those who are affected. Understand that your attitude towards acceptable use and privacy may not correspond with those whose data you are using, as privacy preferences differ across and within societies.***[108]

[107] Nissenbaum, H. F. (2010). *Privacy in context: technology, policy, and the integrity of social life.* Stanford, Calif: Stanford Law Books.

[108] Zook, M., Barocas, S., Boyd, D., Crawford, K., Keller, E., Gangadharan, S. P., ... Pasquale, F. (2017). Ten simple rules for responsible big data research. PLOS Computational Biology, 13(3), e1005399. https://doi.org/10.1371/journal.pcbi.1005399

04 PRIVACY & WELFARE PROTECTION IN RESEARCH

4.1 Compliance[110]

To protect the privacy and welfare[109] of participants in research, extra care and safeguards must be put in place in handling personal data. In doing so, organizations will have to undergo compliance. Privacy compliance champions in the organization have to account for various aspects of research, including: the information life cycle, privacy by design, security, and data protection officer. Research ethics review by duly accredited bodies helps ensure that the welfare of participants, above and beyond privacy rights, has been well considered.

Formal institutional structures and mechanisms have to be in place for the protection of human and data subjects. They are not incompatible with the exercise of researchers' academic freedom, freedom of thought or inquiry.

Compliance can be part of an overall strategy to manage research quality and risks. For greater efficiency in the deployment of resources, privacy and ethics compliance can dovetail with Quality Management certification efforts of the organization. Even without such formal efforts, however, the institution could well adopt essentially the same strategy, minus the onerous fees associated with formal quality management certification. The ICH-GCP

[109] Promoting welfare in research is not about handing out dole-outs (or pejoratively "welfare"). With research ethics, however, the minimum is about not making research participants worse off due to research activities. That includes privacy rights being respected.

[110] See also Appendix B: Privacy Compliance Matrix.

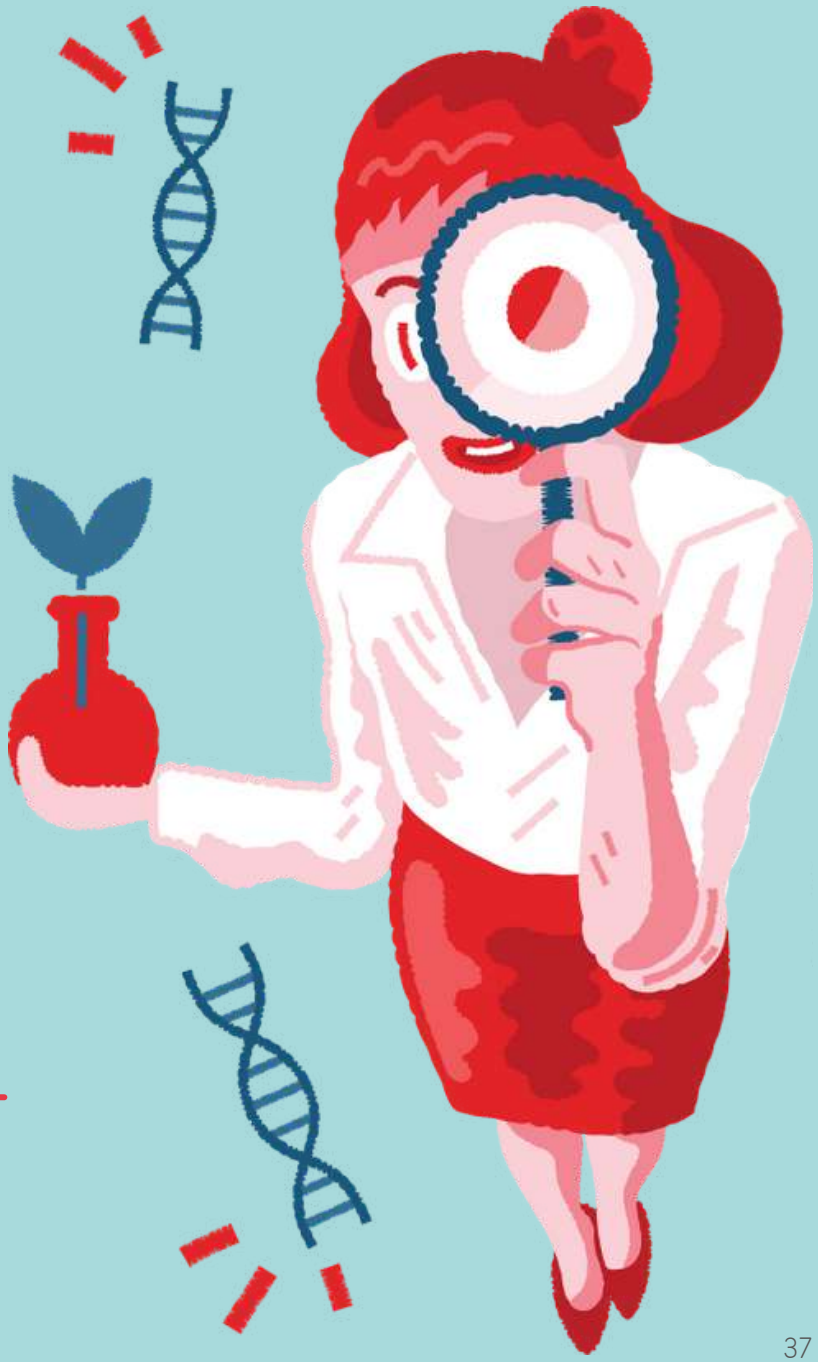
Guideline, for instance, mandates a systematic approach to quality assurance and control "proportionate to the risks inherent in the [clinical] trial and the importance of the information collected." [111]

These days, a risk-based approach to research entails the identification and evaluation of critical processes and information, of privacy and other risks that the research and study subjects are exposed to, and of the treatment and control of such risks as well as communicating, reporting, and reviewing them.

4.1.1 Privacy Compliance

As a general rule, research organizations *qua* personal information controllers are covered by privacy compliance requirements. Especially for entities with at least 250 employees or processing personal data of at least a thousand individuals, privacy compliance is to be treated with greater urgency.

However, in the exercise of freedom of speech, of expression, or of the press, personal information processed for journalistic, artistic, or literary purposes is exempt from *certain* data privacy constraints.[112] Information controllers and processors are certainly not exempt. The "research exemption" clause in the Data Privacy Act of 2012 is *not* a blanket authority for research organizations to dodge privacy regulations altogether. Only functions that directly relate to research would be covered by such exemption but these are *still* subject to security and confidentiality controls as well as other applicable laws. For instance, insofar as these organizations would collect personal information from their own employees, need to have an inventory of informational risks, and need to report information breaches, they are definitely covered by the privacy regulations.



[111] Guideline, I. H. (2016). Integrated addendum to ICH E6 (R1): Guideline for good clinical practice E6 (R2). Current Step, 4, 1–60. In ICH-GCP, the Sponsor ensures the effective Quality Management of clinical trial.

[112] IRR of Rep. Act No. 10173 (2016), sec. 5 (b).

In this light, organizations are better off using the NPC's five (5) "pillars" of compliance as a guide here.

Pillar 1: Appointment of a Data Privacy Officer

Pillar 2: Conduct of Privacy Impact Assessment

Pillar 3: Institution of Privacy Management Program

Pillar 4: Implementation of Privacy & Data Protection Measures

Pillar 5: Establishment of Breach Reporting Procedures

4.1.1.1 Compliance on the Data Processing: Organization Side

4.1.1.1.1 Appointment of a Data Protection Officer (DPO) [113]

A business entity appoints a DPO to be accountable for compliance. Publicly notarized, the DPO appointment needs to be filed with the NPC. The DPO initiates or facilitates the conduct of Privacy Impact Assessments (PIA) for the whole institution and research projects. DPOs' skill sets should include the ability to champion and negotiate for privacy measures in the organization, without losing sight of the obligation to comply with the law.

Your DPO does not have to be a lawyer. However, he has to possess specialized knowledge or expertise relevant to privacy or data protection. A sufficient understanding of processing operations and information systems and the needs for data security and privacy would constitute good DPO qualities.

DPO Duties and Responsibilities

privacyph.org/dpo

In some cases, a Compliance Officer for Privacy (COP) performs some of the functions of a DPO, for instance, for an organization or entity with branches, sub-offices, or any other component units. Especially for large organizations, COPs are the focal persons needed to extend the reach of the DPO.

4.1.1.1.2 Conduct of Privacy Impact Assessment [114]

The Privacy Impact Assessment (PIA) is a legally mandated exercise at the level of the organization but not necessarily for a particularly small-scale research.[115] It is about taking

[113] Rep. Act No. 10173, sec. 21; IRR of Rep. Act No. 10173 (2016), sec. 50; NPC Circular 16-01; NPC Advisory 17-01.

[114] Rep. Act No. 10173, sec. 20(c); IRR of Rep. Act No. 10173 (2016), sec. 29; NPC Advisory 17-03.

[115] Here is where the "research exemption" clause in the Act could come in handy for individual and small-scale research groups. See, for instance, "Data Protection" in Denscombe, M. (2014). The good research guide: for small-scale social research projects (5. ed). Maidenhead: Open University Press, 317ff. Locally, processing the personal data of over 1000 individuals or over 250 employees is a trigger for the proper conduct of PIA.

stock of the informational risks that your organization has. Its components include: ownership, stakeholder involvement, privacy risk inventory, controls and measures framework, sign-off from decision-makers, and an implementation plan. Ownership refers to the ownership of systems (e.g., an electronic medical record (EMR) system, student enrollment system, or other information systems), procedures (e.g, colonoscopy, venipuncture, hiring procedure, etc.), programs (e.g., vaccination program, recruitment program, etc.), projects (e.g., research project, livelihood project, etc.), and administration (e.g., human resources, accounting, budget, etc.) [116] that process personal data. Stakeholder involvement ensures broad buy-in and mandate of the PIA exercise. Part of the PIA process is an inventory of privacy risks that should be managed with appropriate, adequate controls and measures. Once done, the PIA becomes the baseline information for the formulation and implementation of a privacy management program.

A good PIA helps information controllers and processors to evidence that they have well profiled the privacy risks that their organization and research are exposed to, and have met their broader data protection obligations.

Ordinarily, a university researcher does not have to worry about conducting a PIA; that is the job of the university's DPO. It's another story, however, if the researcher is the project leader of a study, especially if such study has greater than minimal risks. This researcher may have to facilitate at least an inventory of personal data involved in the project.

Privacy Impact Assessment Worksheets

privacyph.org/piaworksheets

Early in the information life cycle (see **Information Life Cycle** section), before you start collecting data for your project, program, system, or any information processing activity, consider the need to conduct a PIA as an integral part of your project (or activity) planning and development.

4.1.1.1.3 Institution of Privacy Management Program [117]

This plan or program ensures that privacy principles are imbibed in all aspects of your organizational life: operations, human resources, customer service, etc. The program should also include provisions for privacy notices to the public, data management, [118] data sharing, compliance monitoring, security clearances for data handlers, and privacy training.

[116] This classification scheme for dividing privacy concerns into systems, projects, programs, procedures, and administration is a matter of convenience. Certainly, overlaps are likely. For instance, an organization can have a project that involves the development and deployment of a system that collects personal information. Procedures or processes could make up a system, too. The point of the exercise is to be able to cover comprehensively the bases of privacy risks.

[117] Rep. Act No. 10173, sec. 11-15; IRR of Rep. Act No. 10173 (2016), sec. 21-23, 43-45; NPC Circulars 16-01, 16-02.

[118] For concerns from anthropologists on data management, see Pels, P., Boog, I., Henrike Florusbosch, J., Kripe, Z., Minter, T., Postma, M., Richards-Rissetto, H. (2018). Data management in anthropology: the next phase in ethics governance? *Social Anthropology*, 26(3), 391–413. https://doi.org/10.1111/1469-8676.12526

Privacy Management Plan

privacyph.org/mgt

4.1.1.1.4 Implementation of Privacy and Data Protection Measures

A good practice is to codify the implementation of privacy and data protection measures in a form of an Organizational Privacy Manual that everyone in the organization can refer to and follow. The manual guides everyone in the organization in carrying out their duties and responsibilities, with special consideration to data privacy. The manual is a direct translation of privacy requirements in organizational and operational terms, ensuring that data subjects are apprised of their rights through privacy notices and the consent processes, and that up-to-date data protection measures or controls are being observed.

In the formulation of your Organizational Privacy Manual, it helps to think of this as a combination of outputs in the use of tools like the Privacy Management Plan (PMP) Template and Privacy by Design (PbD) Guidelines and, for health research, the Health Privacy Code currently being passed through appropriate government channels.

In addition to specific physical, organizational, and technical security measures that your organization seeks to implement, the manual may also include:

- protocols of your breach response team,
- protocols for inquiries and complaints,
- annexes (like privacy notices, consent forms, access request form, and request for correction form).

4.1.1.1.5
Establishment of Breach Reporting Procedures

A breach is to be reported within 72 hours upon knowledge of the incident. To address breaches systematically, use the Breach Management Questionnaire as a template. Answers to such questionnaire will formulate your organization's **response policy procedure**. With a designated breach response team, conduct a breach drill at least once a year.

Breach Management Questionnaire

privacyph.org/breachform

With the Five Pillars as a guide, privacy compliance should not be hard to achieve. While an apparent non-compliance may not automatically mean violation of the privacy law, the progression from simple to gross negligence would likely guarantee violation of privacy regulation. A complaint from interested parties could also lead to such determination.

4.1.1.1.6
Registration of Information Processing Systems

Personal information controllers (PIC) or processors (PIP) employing at least 250 persons or processing at least 1000 records involving sensitive personal information, are mandated to register their data processing systems, as provided by sections 5 (c) and (d) of NPC Circular No. 17-01. The registration shall include the following:

(a) the organization's purpose or mandate;
(b) all existing policies relating to data governance, data privacy, and information security, and other documents that provide a general description of privacy and security measures for data protection;
(c) attestation on certifications obtained by PIC, PIP, relevant personnel processing personal data;
(d) brief description of data processing system or systems:
  (i) name of the system;
  (ii) purpose or purposes of the processing;
  (iii) whether processing is being done as a PIC, PIP, or both;
  (iv) whether the system is outsourced or subcontracted (to include the name and contact details of the PIP);
  (v) description of the categories of data subjects and their personal data;
  (vi) recipients or categories of recipients to whom the personal data might be disclosed; and
  (vii) whether personal data is transferred outside of the Philippines;
(e) notification regarding any automated decision-making operation.

4.1.1.2 Compliance Check [119]

On the regulatory side, the NPC is empowered to audit privacy compliance in relation to personal data processing activities, including research. [120] "Compliance Check" is defined as the systematic and impartial evaluation [121] of a Personal Information Controller (PIC) or Personal Information Processor (PIP), conducted to determine whether activities that involve the processing of personal data are being carried out in accordance with the standards [122] mandated by the Data Privacy Act and the issuances of the Commission.[123]

In order to ensure compliance with the Data Privacy Act, the NPC may opt to employ various modes of Compliance Checks,[124] including:

(1) Privacy Sweep [125]
(2) Documents Submission [126]
(3) On-Site Visit [127]

4.1.2 Ethics Compliance

The research participant's welfare is the prime concern of research ethics review. In research, such review is also a prerequisite to data privacy compliance. Human subjects protection and data protection are complementary mechanisms to promote the rights and welfare of study participants. For guidance on Research Ethics Review, please refer to the following documents:

- 2017 National Ethical Guidelines for Health and Health-Related Research

- Code of Ethics in Social Science Research

and

- SSERB Guidelines for Ethical Research in the Social Sciences

For an ethics committee to approve a research proposal, at the least the following criteria need to be considered: [128]

- risks to research participants are minimized or are reasonable in relation to anticipated benefits;
- equitable selection of study subjects;
- their informed consent is obtained to the extent required; and
- protection of the privacy of study subjects and the confidentiality of data.

[119] Rep. Act No. 10173, sec. 7-7(q) ; IRR of Rep. Act No. 10173 (2016), sec. 8, 9(d).

[120] IRR of Rep. Act No. 10173 (2016), sec. 49(e).

[121] NPC Circular No. 02-18 (2018), sec. 3(d).

[122] Rep. Act No. 10173 (2012) ; IRR of Rep. Act No. 10173 (2016).

[123] NPC Circular No. 02-18 (2018).

[124] NPC Circular No. 02-18 (2018), sec. 4.

[125] NPC Circular No. 02-18 (2018), sec. 4(a).

[126] NPC Circular No. 02-18 (2018), sec. 4(b).

[127] NPC Circular No. 02-18 (2018), sec. 4(c).

[128] See 45 Code of Federal Regulations 46.111 "Criteria for IRB approval of research."

For better integration of privacy protection in research ethics reviews, the research ethics committee (REC) should consider regular representation from the Data Protection Officer (DPO).

While such a committee expects to find an Ethical Considerations section in research proposals, it should also prescribe to include a **Data and Privacy Management Plan** section in study protocol submission from research proponents precisely to address privacy concerns in research. Increasingly, data management and data privacy are governance and accountability issues that funding agencies, universities, and international journals would seek researchers to address. Putting them under one particular section in a research proposal is a practical consideration before a research ethics committee.

4.1.2.1 Risk Assessment & Minimization

Risks to research subjects are physical, psychological, social, economic, dignitary, or privacy-related. These risks are non-mutually exclusive. The goal of research ethics review is to facilitate the mitigation of risks that the research may introduce to these human subjects. The threshold for ethics approval is usually "minimal risk" defined as "a classification of risk in research where the probability and magnitude of harm or discomfort anticipated in the proposed research are not greater, in and of themselves, than those ordinarily encountered in daily life or during the performance of **routine physical or psychological examinations** or tests."[129] The benchmark risk exposures here are those of daily life and routine procedures. In research data privacy protection, would your stakeholders going below similar levels of exposure to privacy risks be good enough?

The challenge, however, is not simply about the determination per se of risks based on some objective standards—notwithstanding the *supposedly* accepted daily life and routine exams criteria. Such risks are not just lying around waiting to be discovered. It is also about the capacity of research ethics committees to understand them and respond in a timely manner. There is an expected uncertainty to the process of risk assessment whose objects are moving and are context- and time-sensitive.

Consider, for instance, a research on "Tastes, Ties, and Time" (T3) involving the use of Facebook data. A Harvard University institutional review board (IRB) approved the research protocol concerned. "It is [the IRB's] job to ensure that subjects' rights are respected, and we think we have accomplished this," maintains a T3 researcher.[130] On another occasion, the same researcher noted that the ethics approval was granted "because we don't actually talk to students, we just accessed their Facebook information."[131] The Research Ethics Committee (or the IRB) must have thought they had gotten a good handle of the privacy risks involved. In 2008, T3 researchers publicly released their data comprising 1700 multi-year profiles of students at a supposedly anonymous northeastern American University. Despite all the measures indicated in an ethics-approved protocol to ensure privacy and confidentiality, the source of the dataset was quickly identified, using only T3's publicly available codebook and some public comments made

[129] Philippine Health Research Ethics Board. (2017). *National Ethical Guidelines for Health and Health-Related Research 2017*. Taguig, Metro Manila: Department of Science and Technology - Philippine Council for Health Research and Development, 255.

[130] Kaufman, J. (2008). Michael—We did not consult... [Blog comment]. michaelzimmer.org Retrieved June 5, 2019, from http://michaelzimmer.org/2008/09/30/on-the-anonymity-of-the-facebook-dataset/

[131] Kaufman, J. (2008). Considering the sociology of Facebook: Harvard Research on Collegiate Social Networking [Video].: Berkman Center for Internet & Society, as cited in Zimmer, M. (2010). "But the data is already public": on the ethics of research in Facebook. Ethics and Information Technology, 12(4), 313–325. https://doi.org/10.1007/s10676-010-9227-5

about the research. [132] With the dataset source now known and with the public availability of the dataset itself, certain people could link at least some unique attributes on the dataset with other available personal information, thus making T3 research subjects vulnerable to further privacy attacks.

In this light, the research ethics committee is part of the risk equation. Not being able to see privacy risks is itself risky. In overestimating some risks and underestimating others, and in making impossible requests from researchers, an ethics committee could unintentionally encourage obfuscation rather than transparency. In response to "one-size-fits-all," context-insensitive review procedures and criteria, researchers could behave less ethically than they otherwise would. [133]

On the other hand, it is unreasonable to believe that research ethics committees could fully address all privacy risks in any given research project. It is a setup for failure when, to begin with, expectations of research ethics committees are disproportionate to their budgets, training, and other institutional support. Accountability in risk assessment and response has to match ownership of information systems, processes, procedures, and programs. Even in research, "who's the information controller?" remains the primary question. The committee helps with the risk oversight but the primary responsibility of risk accounting and response remains with information controllers and the very institution enabling the processing of personal information.

Further Discussion

D4.1.2.1. *Disaster Research.* Research ethics review pays special attention to the vulnerable whose unique vulnerabilities (privacy ones included) tend to be amplified in disaster situations. One of the proposals to facilitate disaster research is to obtain "proactive pre-disaster collaborative engagement" with your research ethics committee and to have pre-approved standard protocols, plans, and instruments for, say, competence assessment on disaster-affected research subjects' decision-making as well as capacity to give consent. [134, 135] Such kind of approval could be contingent on certain oversight and reporting requirements. How much of this proposal is feasible in your own research context?

In disaster areas where resources could be scarce, how do you propose to secure the confidentiality of data?

D4.1.2.2. *Privacy Risk Standard.* In research ethics review, ethics committees are supposed to know what counts as "minimal risk" to research subjects, being the threshold for approval. How does this translate to privacy risks? In big data research, for instance, "Would online photos or social media data scraping pose minimal risk to the subjects? Which research designs and objectives can be sought to minimize risks?" [136]

[132] Zimmer, M. (2010). "But the data is already public": on the ethics of research in Facebook. Ethics and Information Technology, 12(4), 313–325. https://doi.org/10.1007/s10676-010-9227-5

[133] cf. Glasius, M., de Lange, M., Bartman, J., Dalmasso, E., Lv, A., Del Sordi, A., … Ruijgrok, K. (2018). Research, Ethics and Risk in the Authoritarian Field. https://doi.org/10.1007/978-3-319-68966-1

[134] Packenham, J. P., Rosselli, R. T., Ramsey, S. K., Taylor, H. A., Fothergill, A., Slutsman, J., & Miller, A. (2017). Conducting Science in Disasters: Recommendations from the NIEHS Working Group for Special IRB Considerations in the Review of Disaster Related Research. Environmental Health Perspectives, 125(9), 094503-. https://doi.org/10.1289/ehp2378

[135] To just assume that disaster survivors have impaired decision-making capacity is inaccurate. Generally, even those with acute stress disorder and posttraumatic stress disorder do not possess diminished capacities (Rosenstein, D. L. (2004). Decision-making capacity and disaster research. Journal of Traumatic Stress, 17(5), 373–381. https://doi.org/10.1023/B:JOTS.0000048950.36359.a2).

[136] Prosperi, M., & Bian, J. (2019). Is it time to rethink institutional review boards for the era of big data? Nature Machine Intelligence, 1(6), 260–260. https://doi.org/10.1038/s42256-019-0059-7

4.1.2.2 Standards for Waived Consent

The requirement for a signed informed consent form may be waived by a research ethics committee for certain cases, including:

- research that does not involve human participants nor samples,
- research or protocols (such as evaluation and quality tests) that do not have more than minimal risks,
  - no disclosure of the participants involved in a survey, interview, non-participant observation, or their responses on it,
- research using publicly available documents,[137]
- research that uses the method of naturalistic observation (covert methodology) in data collection, provided that:
  - use of covert method is thoroughly justified,
  - there is a defined plan for data use, and
  - there is a mechanism in place to ensure confidentiality and anonymity.

In addition, partial waiver or alteration may be approved by the REC, given that:

- the research is no more than minimal risk,
- no adverse effect on the rights and welfare of human subjects,[138]
- research cannot be practically carried out without such waiver or alteration, and
- participants will be debriefed after the study.[139]

---

[137] Philippine Health Research Ethics Board. (2018). National Ethical Guidelines for Health and Health Related Research 2017, 38-39. Department of Science and Technology-Philippine Council for Health Research and Development. Retrieved from https://ethics.healthresearch.ph/index.php/phoca-downloads/category/4-neg?download=98:neghhr-2017

[138] Except perhaps the data subject's right to be informed and other related privacy rights.

[139] The American Psychological Association recommends that the debriefing procedure should explain to participants how the deception was carried, what its purpose was, and how it was necessary, having considered the alternatives (APA, 1984. *Ethical principles in the conduct of research with human participants*. American Psychological Assoc.).

In other words, consent is not absolutely required in research, ethically or legally. Ethics compliance and the consideration of research integrity could provide for better appreciation of the leeway in privacy compliance.

On the other hand, while certain studies are candidates for waiver of the informed consent requirement, data privacy protection even in such kind of studies remains to be enforced. In retrospective medical chart reviews, for instance, it is not always feasible to contact patients for their consent. A researcher doing a retrospective study involving patient records may argue that such a study is minimally risky and that patient records are routinely being examined for internal quality improvement or assurance at the hospital, as well as for reportorial and insurance-reimbursement purposes. Such justification could persuade the REC to grant a consent waiver. However, with heightened attention to data privacy concerns, such research may not be acceptable in situations where the only option to make such research possible is to give researchers unhampered access to the medical records section of the hospital.

Research Proposal Review Tips

privacyph.org/researchreviewtips

4.2 Information Life Cycle[140]

Consider whether it is necessary to collect and hold that much personal information in order to carry out your functions and activities. Plan how personal information will be handled by embedding privacy protections into the design of your organization's information handling practices. Assess the risks associated with the collection of personal information due to a new act, practice, or change to an existing project or as part of business as usual. Take the appropriate steps and put into place strategies to protect the personal information that you hold. Lastly, de-identify or destroy personal information when it is no longer needed.

To systematically address privacy concerns in the data life cycle, use the Privacy Management Plan template.

Privacy Management Plan

privacyph.org/mgt

Researchers must be mindful of how they use shared personal data by adopting appropriate safety measures against potential threats to privacy.

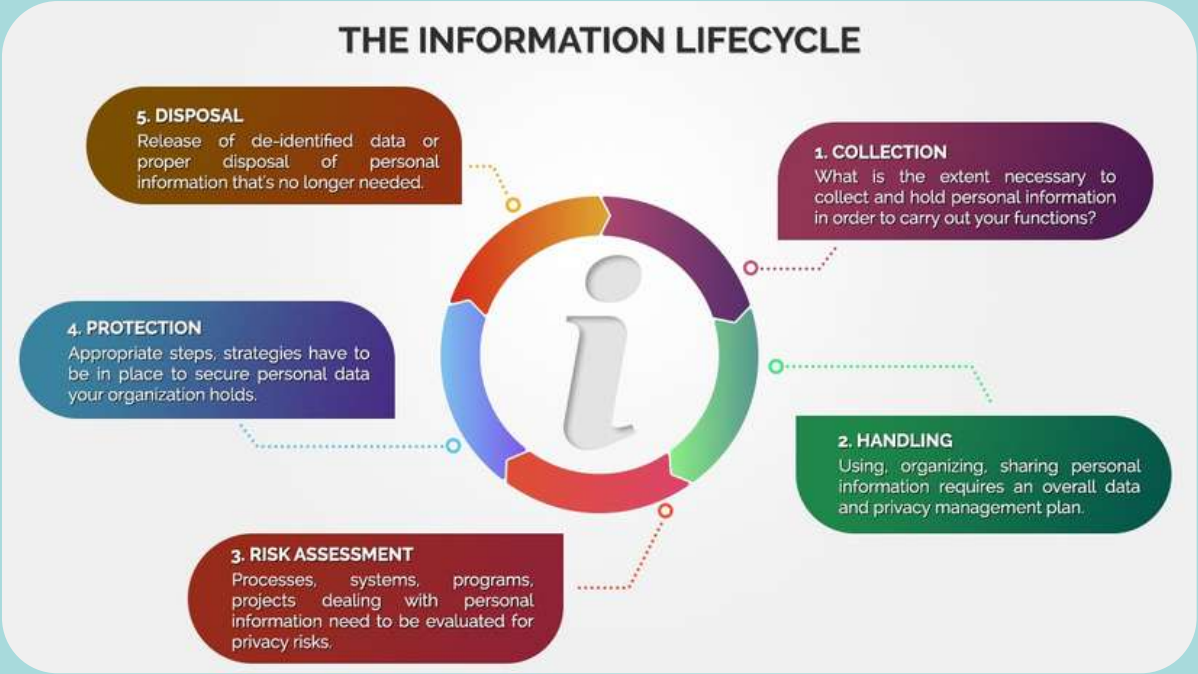


Figure 1. *Securing personal information in its life cycle.*[141]

[140] Office of the Australian Information Commissioner. (2018). Guide to securing personal information: 'Reasonable steps' to protect personal information. Retrieved 15 March 2019, from https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

[141] cf. the Office of Australian Information Commissioner's (OAIC) "Guide to securing personal information."

4.3 Privacy by Design Approach

The concept of Privacy by Design (PbD) in research sets a data-processing environment that respects privacy and data protection in a comprehensive way. Given a diversity of design options, one should always choose the one that makes privacy as the *default* setting. PbD compels heads of institutions, project leaders, researchers, officers, and developers to make privacy protection an integral part of their operations, procedures, technologies, and information architectures. See "PbD in Research" Guidelines as a starting point to implement your own measures for embedding privacy in your research organization.

"PbD in Research" Guidelines

privacyph.org/pbdresearch

Privacy Impact Assessment Worksheets

privacyph.org/piaworksheets

Further Discussion

D4.2.1. *Periodic risk assessments.* The IRR and the National Privacy Commission mandate organizations to conduct a periodic Privacy Impact Assessment (PIA). Besides the organizational assessment once a year, how often in between should you have PIAs? Do you have a clear sense of your current privacy risk profile?

4.3.1
Intersection between Privacy & Security

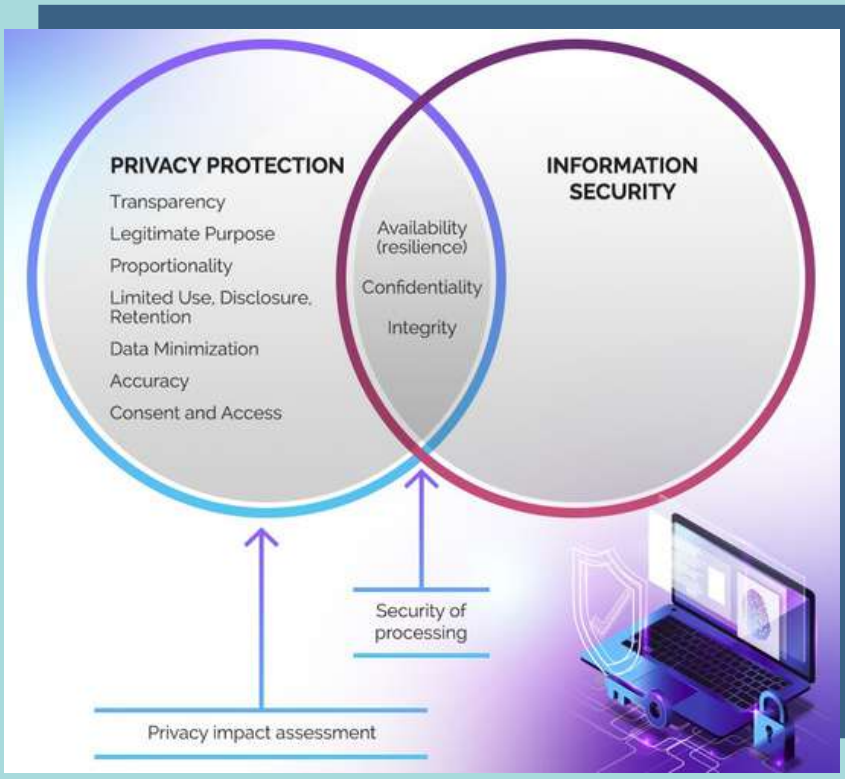


Figure 2. *The privacy-security overlap.*[142]

An information security adage states that there is no privacy without security. Some people, however, tend to confuse that claim to mean security is equal to privacy or that security guarantees privacy. There is significant overlap between the two (see Figure 2) but they are not the same. In research (as in any productive endeavor), there is a trade-off between security and utility. The more security measures an organization puts into an information system, the less useful and accessible it tends to be. If a system is not useful at all, privacy becomes a non-starter. "Privacy by Design" would still maintain proportionality in security: the more sensitive the information is, the more security it should have.

[142] cf. Data Protection Working Group. (2017). Risk Assessment and Data Protection Impact Assessment. Bitkom e.V. Retrieved from https://www.bitkom.org/sites/default/files/file/import/170919-LF-Risk-Assessment-ENG-online-final.pdf.

4.3.2 PbD and Awareness of Privacy Risks

It takes some time to imbibe data privacy consciousness. Hence, a willful attention to privacy risks must be made, however exaggerated it tends to be at the beginning. Some highlights of penalty categories and range of fines and imprisonment are as follows.

- *Accessing Personal Information and Sensitive Personal Information Due to Negligence.*[143]
  - **Personal Information.** For persons who, due to negligence, provided access to personal information without being authorized under the Data Privacy Act or any existing law will be penalized with imprisonment ranging from one to three years and a fine of five hundred thousand pesos up to not more than two million pesos.[144]
  - **Sensitive Personal Information.** For persons who, due to negligence, provided access to sensitive personal information a penalty of imprisonment ranging from three to six years and a fine of five hundred thousand pesos up to not more than four million pesos shall be imposed.[145]

- *Unauthorized Access or Intentional Breach.*[146] The act also penalizes persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information are stored. The Data Privacy Act provides for a penalty of imprisonment ranging from one to three years and a fine of not less than five hundred thousand pesos but not more than two million pesos.[147]

---

[143] Rep. Act No. 10173 (2012), sec. 26 ; IRR of Rep. Act No. 10173 (2016), sec. 53.

[144] Rep. Act No. 10173 (2012), sec. 26(a) ; IRR of Rep. Act No. 10173 (2016), sec. 53(a).

[145] Rep. Act No. 10173 (2012), sec. 26(b) ; IRR of Rep. Act No. 10173 (2016), sec. 53(b).

[146] Rep. Act No. 10173 (2012), sec. 29 ; IRR of Rep. Act No. 10173 (2016), sec. 56.

[147] Rep. Act No. 10173 (2012), sec. 29 ; IRR of Rep. Act No. 10173 (2016), sec. 56.

[Processing]

- *Unauthorized Processing of Personal Information and Sensitive Personal Information.* [148]
  - **Personal Information**. Individuals who process personal information without the consent of the data subject, or without being authorized under the Data Privacy Act or any existing law will face the penalty of imprisonment ranging from one to three years and a fine of not less than five hundred thousand pesos but not more than two million pesos will also be imposed. [149]
  - **Sensitive Personal Information**. A heavier penalty shall be imposed on persons who process sensitive personal information without the consent of the data subject, or without being authorized under the Act or any existing law. These individuals would face imprisonment ranging from three to six years and a fine of not less than five hundred thousand pesos but not more than four million pesos. [150]

- *Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes.* [151]
  - **Personal Information.** A penalty of imprisonment ranging from one year and six months to five years and a fine of five hundred thousand pesos up to one million pesos shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under the Act or under existing laws. [152]
  - **Sensitive Personal Information.** A penalty of imprisonment ranging from two to seven years and a fine of five hundred thousand pesos to not more than two million pesos shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under the Act or under existing laws. [153]

[148] Rep. Act No. 10173 (2012), sec. 25 ; IRR of Rep. Act No. 10173 (2016), sec. 52.

[149] Rep. Act No. 10173 (2012), sec. 25(a) ; IRR of Rep. Act No. 10173 (2016), sec. 52 (a).

[150] Rep. Act No. 10173 (2012), sec. 25(b) ; IRR of Rep. Act No. 10173 (2016), sec. 52(b).

[151] Rep. Act No. 10173 (2012), sec. 28 ; IRR of Rep. Act No. 10173 (2016), sec. 55.

[152] Rep. Act No. 10173 (2012), sec. 28(a) ; IRR of Rep. Act No. 10173 (2016), sec. 55(a).

[153] Rep. Act No. 10173 (2012), sec. 28(b) ; IRR of Rep. Act No. 10173 (2016), sec. 55(b).

Concealment

- *Concealment of Security Breaches Involving Sensitive Personal Information.*[154] In 72 hours upon knowledge of a security breach, an organization should notify the NPC. Concealment, whether by omission or intentionally, is punishable by imprisonment of up to five years and a fine of up to one million pesos.[155]

Disposal

- *Improper Disposal of Personal Information and Sensitive Personal Information.*[156]
  - **Personal Information.** Individuals who knowingly or negligently dispose, discard, or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection shall also be penalized. A penalty of imprisonment ranging from six months to two years and a fine of not less than one hundred thousand pesos but not more than five hundred thousand pesos shall be imposed.[157]
  - **Sensitive Personal Information.** For persons who knowingly or negligently dispose, discard or abandon the sensitive personal information of an individual in an area accessible to the public or has otherwise placed the sensitive personal information of an individual in its container for trash collection, a penalty of imprisonment ranging from one to three years and a fine of not less than one hundred thousand pesos but not more than one million pesos shall be imposed on.[158]

---

[154] Rep. Act No. 10173 (2012), sec. 30 ; IRR of Rep. Act No. 10173 (2016), sec. 57.

[155] Rep. Act No. 10173 (2012), sec. 30 ; IRR of Rep. Act No. 10173 (2016), sec. 57.

[156] Rep. Act No. 10173 (2012), sec. 30 ; IRR of Rep. Act No. 10173 (2016), sec. 57.

[157] Rep. Act No. 10173 (2012), sec. 27 ; IRR of Rep. Act No. 10173 (2016), sec. 54.

[158] Rep. Act No. 10173 (2012), sec. 27(b) ; IRR of Rep. Act No. 10173 (2016), sec. 54(b).

[Disclosure]

- *Malicious Disclosure.*[159] Any personal information controller or personal information processor, or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or sensitive personal information obtained by him or her, shall be subject to imprisonment ranging from one year and six months to five years and a fine of not less than five hundred thousand pesos but not more than one million pesos.[160]

- *Unauthorized Disclosure.*[161]
  - **Personal Information.** Any personal information controller or personal information processor, or any of its officials, employees, or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one year to three years and a fine of not less than five hundred thousand pesos but not more than one million pesos.[162]
  - **Sensitive Personal Information.** Any personal information controller or personal information processor, or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three years to five years and a fine of not less than five hundred thousand pesos but not more than two million pesos.

[159] Rep. Act No. 10173 (2012), sec. 31 ; IRR of Rep. Act No. 10173 (2016), sec. 58.

[160] Rep. Act No. 10173 (2012), sec. 31 ; IRR of Rep. Act No. 10173 (2016), sec. 58.

[161] Rep. Act No. 10173 (2012), sec. 32 ; IRR of Rep. Act No. 10173 (2016), sec. 59.

[162] Rep. Act No. 10173 (2012), sec. 32(a) ; IRR of Rep. Act No. 10173 (2016), sec. 59(a)

COMBINATION OF ACTS

Any combination or series of acts defined above shall make the person subject to imprisonment ranging from three years to six years and a fine of not less than one million pesos but not more than five million pesos.

4.4 Security

4.4.1 Physical Security

Know the data format. The format, whether digital or paper-based physical, helps determine the appropriate **storage type and location** for your data. Whether virtual or physical, the storage facility must be secure. Papers or physical documents bearing personal data shall be stored in **locked filing cabinets,** access keys to which shall be entrusted to authorized personnel. Digital or electronic documents containing personal data shall be stored in computers, portable disks, and other devices, provided either the document or the device where it is stored is protected by **passwords or passcodes.** Computers, portable disks, and other devices used shall be **encrypted** with the most appropriate encryption standard.

When it comes to access and security clearances, only authorized personnel and the Personal Information Processor (PIP) may access the personal data stored; they may not share, disclose, or distribute the personal data unless with the **consent** of the data subject. To monitor the people who access the data, all those who enter and access the room where the personal data is stored must **register in the logbook,** which shall indicate the date, time, duration, and purpose of each access. For digital access, an audit trail should be put in place.

Maintenance of confidentiality is a constant concern. In some privacy-compliant facilities, no one is allowed to bring their own personal or access storage devices when processing any personal data.

4.4.2 Technical Security Measures

There are three types of privacy breach:

(i) **Availability breach** – data loss due to accidental or unlawful destruction of personal data;

(ii) **Integrity breach** – the unauthorized, unwanted alteration of personal data; and,

(iii) **Confidentiality breach** – the unauthorized disclosure of or access to personal data.

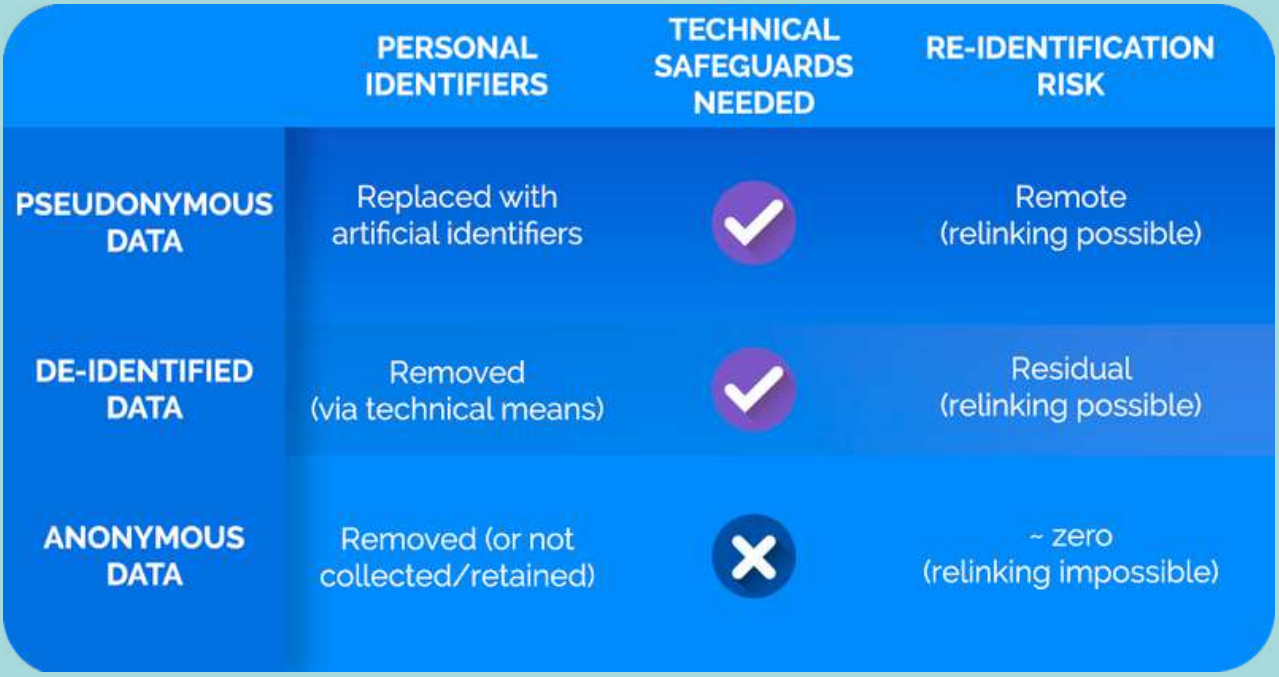


Table 1. *Differences among pseudonymous, de-identified, and anonymous data.*

Here is how to respond to privacy breaches:

Breach Management Questionnaire

privacyph.org/mgt

At least once a year, using current definitions, vulnerability scanning of online assets must be conducted. Business continuity drills must also be done at least once a year. Providers hosting personal data stored in the cloud need to be compliant with ISO:IEC 27018. AES 256-bit is the encryption standard for digitized personal data at rest or in transit.[163]

Specifically for research, one way to implement technical measures on data sets is to use pseudonymization, "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual."[164] Note, however, that pseudonymization (including techniques like key coding) is short of anonymization and is still subject to data privacy regulation. Technically, it is also different from de-identification (discussed in greater detail in the **Confidentiality and De-Identification** section). Table 1 details the main

[163] NPC Circular No. 16-01 (2016).

[164] Article 4(3b), GDPR.

differences among pseudonymous, anonymous, [165] and de-identified data. Only anonymous data have practically zero re-identification risks. Relinking such data to source personal identifiers is impossible. Both pseudonymous and de-identified data would need technical safeguards.

Monitor for security breaches. Maintain and keep an updated Data Privacy Tracker, containing a log of all privacy-related incidents, complaints, and requests from data subjects, access requests, and all agreements on data sharing and outsourcing. You can also run security vulnerability scans periodically to detect outdated applications, misconfigured machines, and malwares, among others. Use an intrusion detection system to monitor security breaches and to be alerted of any attempt to interrupt or disturb the information system. Examine firewall logs regularly or run security analytics to determine whether your machines may have been compromised.

Use essential security software and applications. Procure and install antivirus, antimalware software for all devices where personal data are stored that regularly access the Internet. The Compliance Officer for Privacy (COP), if any, or the head of the institution, should ensure that the antivirus software is updated and that a system check is done periodically. To ensure the compatibility and data security of the software applications, the COP or the head of the institution shall ensure that the applications have been reviewed and evaluated by authorized personnel or PIP(s) concerned before their utilization in computers and devices.

Have a regular assessment and evaluation of the effectiveness of security measures. If the use of any software application is found to be a security risk that may disturb or interrupt the normal operations of your network, the PIPs shall notify the end user of such risk and the software application shall immediately be uninstalled.

Encrypt, authenticate, and employ other technical security measures. Encryption is important, whereby the processed personal data, most especially the sensitive ones, shall be encoded into scrambled text using algorithms that render it unreadable unless a cryptographic key is used. Passwords or passcodes used to access personal data should be of sufficient strength to deter password attacks. Encryption and authentication must be accompanied by other technical security measures that can keep your software security tools up-to-date.

[165] Note, however, that in some studies, like oral history, certain participants may not want to be anonymized and may even look forward to seeing their names publicized. Suggesting that you are changing their names for their privacy might cause them to be upset. Silverman, D. (2017). Doing qualitative research (Fifth edition). London Thousand Oaks, California: SAGE Publications Ltd, 184.

4.4.3 Organizational Security Measures

Organizational security measures are needed for the smooth employment of the security system that your institution has put in place.

Further Discussion

D4.4.1. Is data accountability well thought out in your research organization? Does it allow you to determine who is responsible for possible losses caused by a data breach?

D4.4.2. Is there any documentation on your individual and team roles for data privacy in your organization? Are you clear about your tasks as personal information controller, processor or data custodian?

D4.4.3. The US National Institutes of Health requested "an indexed CD-ROM of the Cebu [Longitudinal Health and Nutrition Survey] data and documentation so that these data can be stored adequately and be readily available for future generations of scholars... [S]ubsequent rounds of CLHNS data have been made available to other scholars via the World Wide Web..." [166] What security measures have to be put in place of these kinds of archival and data sharing practices?

D4.4.4. *Online research.* For many disciplines, online research (aka "Internet research" [167]) is inescapable. Many people inhabit the online world. For experimental psychologists, for instance, the Internet is an inexpensive natural laboratory that enables them to collect enormous amounts of data with minimal efforts. Certain social and behavioral phenomena only exist online.[168] How do you maintain confidentiality in online research? What appropriate administrative, organizational, or technical safeguards are needed for particular Internet research?

D4.4.5. *Health Data.* Do you accord extra physical, organizational, and technical safeguards to health data? Given that health information tends to attract the most cyber criminals, do you put more attention to it than any other types of sensitive personal information? There could be some inherent sensitivity to health data. On the dark web, a single patient's complete health records can fetch for several hundreds of dollars, while other types of sensitive personal information cost much less. [169] Does the value cyber-criminals attach to health information merit special consideration in security?

[166] Adair, L., & Popkin, B. (2001). The Cebu longitudinal health and nutrition survey: history and major contributions of the project. *Philippine Quarterly of Culture and Society*, 29(1/2), 5-37. Retrieved from http://www.jstor.org/stable/29792482

[167] Internet Research "utilizes the Internet to collect information through an online tool...; studies about how people use the Internet...; and/or, uses of online datasets, databases, or repositories." Buchanan, E. A., & Zimmer, M. (2018). Internet Research Ethics. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Winter 2018). Retrieved from https://plato.stanford.edu/archives/win2018/entries/ethics-internet-research/

[168] Myers, A., & Hansen, C. H. (2012). Experimental psychology (7th ed). Australia; Belmont, CA: Wadsworth Cengage Learning. See also Kraut R et al (2004). Psychological research online: Report of board of scientific affairs' advisory group on the conduct of research on the Internet. *American Psychologists*, 59(2): 105-117.

[169] Trustwave. (2017). The value of data: a cheap commodity or a priceless asset. Retrieved from https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf

Having key personnel is important. There must be a person who shall be responsible for overseeing the compliance of the institution with the Data Privacy Act of 2012, its IRR, other pertinent laws and government issuances on data privacy.

Hold workshops/training on data privacy. Members of any institution who will use the personal data for any purpose shall be briefed on their obligations under the Data Privacy Act. The institution shall try to hold privacy and data protection workshops/training sessions at least once a year for personnel who handle

the personal data. Any memorandum shall be distributed to inform the members of the institution of the most current government issuances on data privacy.

Have confidentiality and non-disclosure agreements. All personnel who have access to the personal data shall hold such data under strict confidentiality even after the personnel has left the institution for whatever reason. Non-disclosure agreements can be done through contracts between the data subject and the institution.

DPO Duties and Responsibilities

privacyph.org/dpo

05 CONFIDENTIALITY & DE-IDENTIFICATION

Confidentiality helps maintain people's trust in human subjects research and science. The need to keep personal data confidential cannot, therefore, be overemphasized. In cases where such information needs to be shared or released, technical de-identification should be given utmost importance to maintain the trust of the data givers. De-identification enables researchers to make secondary use of data sets with previously identifiable personal information. Most of all, *proper* de-identification or anonymization puts your work outside the purview of data privacy regulation.

Non-disclosure Agreement. Traditionally, non-disclosure agreements (NDA) have been used to protect sensitive information in organizations. Data privacy requirements, however, extend beyond "disclosure." Processing (not just disclosure) of personal data is the coverage of privacy regulation. Hence, NDAs may no longer suffice. Employees or staff working as information processors should be bound by the privacy policies that are reflected in employment contracts, terms of reference, data sharing agreements, company manuals, training programs, and human resource on-boarding and off-boarding protocols.

De-identification. Functional de-identification considers the whole of the data situation, i.e., both the data and the data environment. When we protect privacy and confidentiality, we are in essence hoping to ensure that de-identified data remains de-identified once it is shared or released within or into a new data environment; therefore, functional de-identification has to consider all relevant aspects of this situation. On the next page is Data61's **De-Identification Decision Framework** (DDF)[170] that seeks to provide safeguards for data sharing and release.

De-Identification Decision Framework

[170] O'Keefe, C. M., Otorepec, S., Elliot, M., Mackey, E., & O'Hara, K. (2017, September 18). The De-Identification Decision-Making Framework. Retrieved from https://publications.csiro.au/rpr/download?pid=csiro:EP173122&sid=DS3

The Data Situation Audit and its components will help you identify and frame the issues relevant to your own context, while the Risk Analysis and Control and its components require you to consider the technical processes in order to both assess and manage the disclosure risk associated with your data situation. Lastly, the Impact Management and its components identify the measures that should be in place before you share or release data. It helps you communicate with stakeholders, ensure that the risks associated with your data are negligible, and work out what you should do in the event of an unintended disclosure or security breach.

Data Situation Audit

1. *Describe your data situation.* Your data situation includes ALL data, people, infrastructure, and governance that make up your environment. Often there's more than one data situation involved, such as if the data is being transferred from one organization to another or being released as open data.

2. *Understand your legal responsibilities.* Does your dataset contain personal information? Or is it de-identified? What controls need to maintain confidentiality?

3. *Know your data.* Conduct a high-level examination of your data, focusing on the data type, features, and properties. Know well your dataset's subjects, variables, quality, and age.

4. *Understand the use case.* In determining the use case for your data you need to understand three things: (i) the reason for wishing to share or release your data, (ii) the groups who will access your data, and (iii) the intention of these groups as they use your data.

5. *Meet your ethical obligation.* Considerations here include consent, transparency, stakeholder engagement, and data governance. Does your research require an ethics approval?

Risk Analysis and Control

6. *Identify the processes you will need to assess disclosure risk.* This is the four-part process for assessing disclosure risk. The first two procedures are always necessary, while the third and fourth may or may not be required depending on the conclusions drawn after conducting the first two:

(a) Incorporation of your top-level assessment to produce an initial specification.

(b) An analysis to establish relevant plausible scenarios for your data situation. When you undertake a scenario analysis, you are essentially considering the how, who, and why of a potential breach.

(c) Data analytical approaches. You will use data analytical methods to estimate risk given the scenarios that you have developed under Procedure (b).

(d) Simulate attacks using 'friendly' intruders who'll try to force your system to disclose personal information not intended to be shared.

7. *Identify the disclosure control processes relevant to your data situation.* Disclosure control processes essentially attend to either or both of the two elements of your data situation: the data and its environment. If your risk analysis in Component 6 suggests that you need stronger controls, then you have two (non-mutually exclusive) choices: (a) reconfigure the data environment or (b) modify the data, including possibly reducing the amount of data under consideration.

Impact Management

8. *Identify who your stakeholders are and plan how you will communicate with them.* Effective communication can help build trust and credibility, both of which are critical to difficult situations where you need to be heard, understood, and trusted. You will be better placed to manage the impact of a disclosure if you and your stakeholders have developed a good working relationship.

9. *Plan what happens next once you have shared or released the data.* Monitor the data environment once you have shared or released your data. Keep a registry of all the data you have shared or released, including a description of the associated data environment(s); and compare proposed share and release activities to past shares and releases to account for the possibility of linkage between releases that could lead to a disclosure.

10. *Plan what you will do if things go wrong.* Sometimes, even when you follow the best practice, things can go wrong. It is essential to put in place mechanisms that can help you deal with the rare possibility of a disclosure or relinking. Such measures include having: a robust audit trail, a crisis management policy, and adequately trained staff.

Sharing of De-identified Data with Collaborators and Analysts. To illustrate attendant privacy issues and concerns, as a research data set moves from one type of environment to another, you need to look at your options in relation to data availability, access, utilization, and safety.

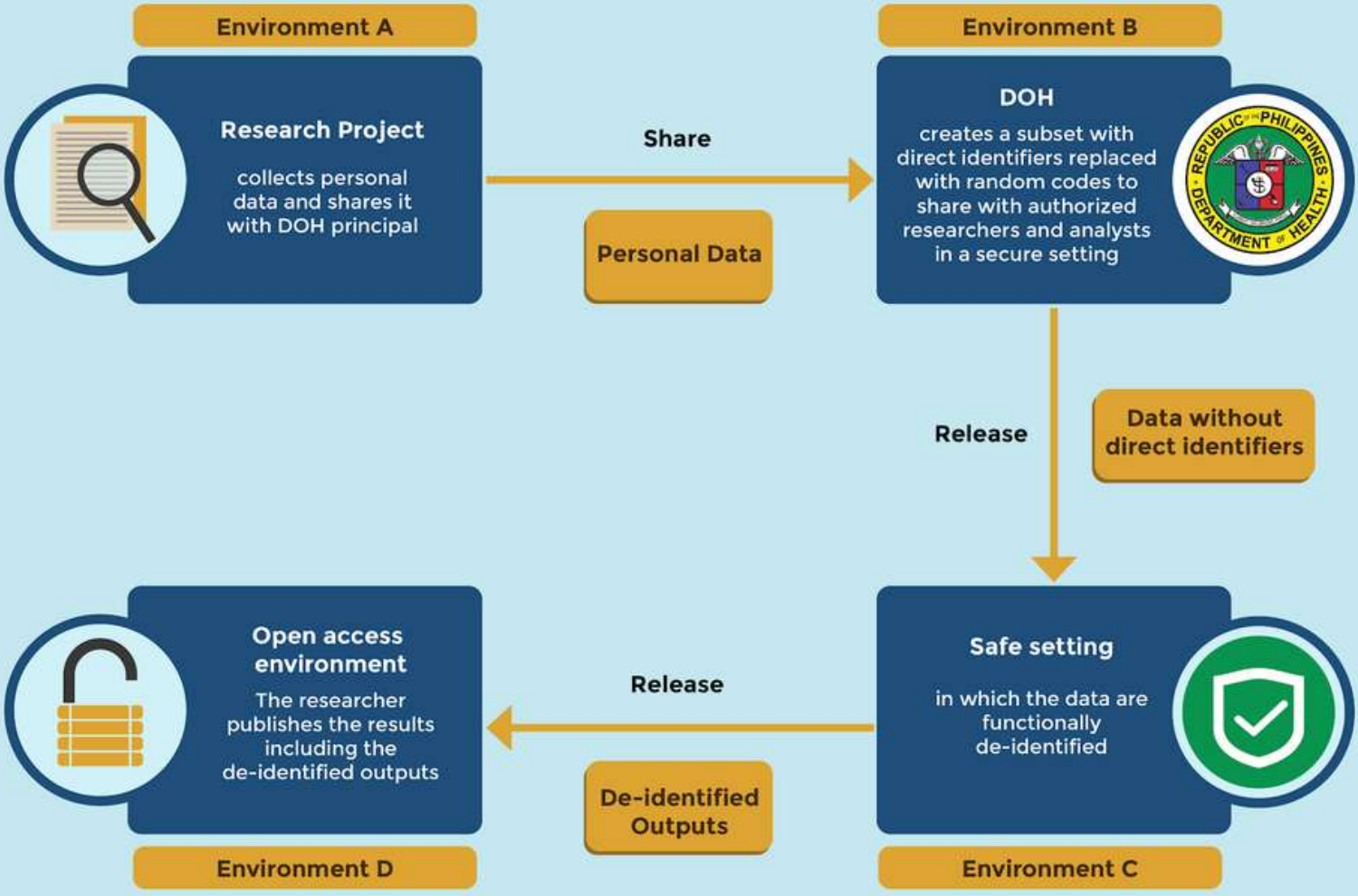
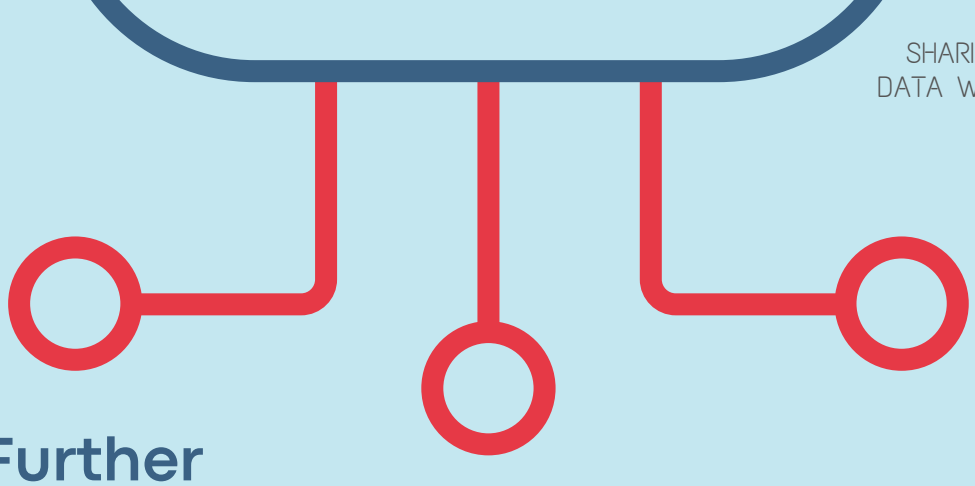


Figure 3. *Illustrative example of the utilization of de-identification in different data environments*

Before research is published, the personal data set to be released undergoes a series of de-identification. While health studies have utility, it is important to uphold the confidentiality and anonymity of the participants. When planning, data collection should be precise and answer the scientific question and their objectives. And, on the research proper, they must only retain the necessary data and properly dispose of those that are not. After collection, data is shared with another organization (in this case, the DOH) and they would provide their de-identification method appropriate to their standards. Direct identifiers will be eliminated or transformed into pseudonyms. Indirect identifiers remain as is. The pseudonymous data will then be examined by another entity to check whether the data is rendered not identifiable. Both direct and indirect identifiers are subjected to various de-identification measures. Only when there is little to no risk of the subjects being identified can research data be published and available to the public.

Release of De-identified Data Sets through Public Archives and Publications. Look out for privacy issues and concerns in archiving supposedly de-identified data sets using public repositories. Many published articles in online journals now come with the data sets used in research. Personal identifiers could leak; secondary attributes could potentially point to identities of research participants. Metadata in such public archives or publications could be problematic if they risk revealing personal data or risk identifying the specific context or other background information that could lead to the participants' identities being inferred.



Further Discussion

D5.1. What sorts of data do you have that need de-identification? If you conduct de-identification with your data set, what is it for? Will you also be sharing your data?

D5.2. What contextual features could render your data set resistant to de-identification?

D5.3. *Patient Registries and Electronic Health Records.* These two have different but complementary foci. Allowing the linkage between the two could boost not only clinical practice but also health research. The use of both registries of rare or common medical conditions and "capillary networks recording the daily clinical practice" (Electronic Health Records) [171] for both clinical and research purposes could prove beneficial to society. What possible measures of confidentiality can be implemented in such a scenario? Are you personally familiar with a similar project? If so, how is confidentiality observed there?

D5.4. *Biorepositories.* If your project involves the archival of human biospecimens, [172] what protections have you put in place to maintain the confidentiality of their identifiable data? How would you design the repository that might link personal information with the specimen? How would you address data degradation and format concerns over time? Are roles for access, sharing, release, and destruction of data clearly defined by your protocols? Do you have a Data Use Agreement (DUA) or, in some cases involving third parties or foreign institutions, a Material Transfer Agreement in place? [173] Do you feel the need to have your data protection plan explicitly reviewed and approved? [174]

---

[171] Tavazzi, L. (2019). Big data: is clinical practice changing? European Heart Journal Supplements, 21(Supplement_B), B98–B102. https://doi.org/10.1093/eurheartj/suz034

[172] US National Cancer Institute defines "biospecimen" as "samples of material, such as urine, blood, tissue, cells, DNA, RNA, and protein from humans, animals, or plants. Biospecimens are stored in a biorepository and are used for laboratory research. If the samples are from people, medical information may also be stored along with a written consent to use the samples in laboratory studies" (National Cancer Institute. (2011, February 2). NCI Dictionary of Cancer Terms. Retrieved May 9, 2019, from National Cancer Institute website: https://www.cancer.gov/publications/dictionaries/cancer-terms)

[173] For more privacy and confidentiality considerations involving biorepositories, see National Comprehensive Cancer Network. (2019). NCCN Points to Consider on the Best Practices for Biorepositories, Registries and Databases. Retrieved May 9, 2019, from https://www.nccn.org/clinical_trials/RepositoriesBestPractices.aspx. For alternative models or design considerations, see USC Office for the Protection of Research Subjects. (n.d.). Five Models for Biorepositories. Retrieved May 9, 2019, from https://oprs.usc.edu/files/2017/05/biobank-diagram-7.5.11.pdf

[174] Chin, W. W. L., Wieschowski, S., Prokein, J., Illig, T., & Strech, D. (2016). Ethics Reporting in Biospecimen and Genetic Research: Current Practice and Suggestions for Changes. PLOS Biology, 14(8), e1002521. https://doi.org/10.1371/journal.pbio.1002521

POSTSCRIPT

Privacy protection, in research projects or elsewhere, is not a stand-alone exercise. We have the research ethics review process as a complementary activity to protect and advance the rights and welfare of individuals who are simultaneously data and research subjects. Ethical standards are both foundational and aspirational elements of research: without ethics, privacy compliance in research may tend to be a meaningless chore. As such, to be both ethical and compliant, researchers, project leaders, and ethics reviewers may follow the Principles of Data Privacy as a guide in navigating the complexities of dealing with privacy and confidentiality issues.

Ultimately, scientific research is an exercise in freedom of thought. Thus, no researcher would want privacy regulators (or anyone, for that matter) to micromanage their work. These days, however, mastering the principles informing the answers to privacy questions and acquiring new privacy-enhancing analytical and computational skills are a must for researchers and project leaders. Even more so, sharing such principles and skills with the Philippine research community is consistent with a high level of maturity and accountability that should make scientific research a truly self-regulating, reflexive enterprise.

As the Further Discussion portions running throughout the five sections of this Primer might suggest, privacy issues and concerns in research involving human participants go beyond what we can humanly cover in this Primer (privacyph.org/primer), its companion Toolkit (privacyph.org/toolkit), and Online Course (privacyph.org/course). Many such issues are moving targets that necessitate the revision of this Primer sooner rather than later. Technologies (including those used in research) also move fast, requiring periodic updates to this work.

While the orientational and practical goals of this Primer are rather modest, we cannot help but wonder how else we could help Philippine researchers focus more on their work and less on regulatory concerns. In this day and age, however, scientific research and regulation are increasingly intertwined. Many researchers will continue to find gaps between what we have managed to articulate in this Primer and the complexities involved in their projects. Further analytical and additional computational skills (e.g., in the use of de-identification applications) might be expected of them down the line.

While many of the questions raised in the Further Discussion segments might simply remain "academic" for many researchers and stakeholders, we hope just the same that discussions to explore the diverse, multi-layered, context-sensitive challenges of privacy will continue. Appendix C provides some Case Vignettes for Privacy in Research (with Discussion Questions) that could serve as further prompts toward this purpose.

Despite criticism of privacy regulations for being potentially obstructive, scientific research, as a *public good,* must continue to be pursued with sustained vigor and rigor, without undermining the rights and welfare of its research participants.

APPENDIX A

SUMMARY OF TOOLS & TEMPLATES

1. Breach Management Questionnaire
   privacyph.org/breachform
2. Consent Template
   privacyph.org/consent
3. DPO Duties and Responsibilities
   privacyph.org/dpo
4. Privacy Management Plan
   privacyph.org/mgt
5. Privacy Impact Assessment Worksheets
   privacyph.org/piaworksheets
6. 'PbD in Research' Guidelines
   privacyph.org/pbdresearch
7. Research Proposal Review Tips
   privacyph.org/researchreviewtips

APPENDIX B

PRIVACY COMPLIANCE MATRIX

Privacy Compliance Requirements & Tools

	DPO Appoint-ment	Registration of Data Processing Systems	Privacy Impact Assessment	Privacy Management Program	Organi-zational Privacy Manual [175]	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_0618.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 Responsi-bilities	N/A	PIA Worksheets	Privacy Management Plan (PMP) Template	PMP Template + PbD Guidelines	Breach Response Questionnaire	N/A

[175] 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.

APPENDIX C

CASE VIGNETTES FOR PRIVACY IN RESEARCH

	Privacy Rights	Principles of Data Privacy	Contextual Issues	Privacy and Welfare Protection	Confidentiality and De-identification
privacyph.org/case1 Case 1 **Prevalence of XDR TB in Region 17**	1.1 Right to be Informed 1.4 Right to Object	2.2 Legitimacy of Purpose 2.3 Proportionality	3.1.2 Timely Access to Health or Other Vital Information 3.2 Data Sharing	4.1.2 Ethics Compliance	D5.3. Patient Registries and Electronic Health Records
privacyph.org/case2 Case 2 **Preemptive Intervention Against Depression**	1.1 Right to be Informed 1.2 Right to Access	2.1 Transparency 2.4 Limited Use, Disclosure & Retention 2.5 Consent	3.4 The Research Context	4.1.2 Ethics Compliance	
privacyph.org/case3 Case 3 **Machine Learning and Sexual Assault**	1.5. Right to Erasure or Blocking Sec 1.7 Right to Damages and Right to File a Complaint	2.2 Legitimacy of Purpose 2.5 Consent	3.2.2. Persistence of Sharedness		
privacyph.org/case4 Case 4 **Teenage Suicides in Barangay Tangwayan**		2.6 Accountability 2.7 Security	3.2 Data Sharing 3.4 The Research Context		5.0 De-Identification Decision Framework: Data Situation Audit, Risk Analysis and Control
privacyph.org/case5 Case 5 **Drugs and Workshops in Talisay**	1.1 Right to be Informed	2.5 Consent	3.2 Data Sharing 3.4 The Research Context		5.0 De-Identification Decision Framework: Data Situation Audit, Risk Analysis and Control
privacyph.org/case6 Case 6 **Facial Recognition and Crime Prevention at Malaya**	1.1 Right to be Informed	2.1 Transparency 2.2 Legitimacy of Purpose	3.1.3 Research Efficiency	4.1.1.1.4 Privacy Management Plan 4.1.2 Ethics Compliance	
privacyph.org/case7 Case 7 **COVID-19 Surveillance**	1.1 Right to be Informed	2.1 Transparency 2.4 Limited Use, Disclosure & Retention 2.5 Consent		4.1.2 Ethics Compliance	5.0 De-Identification Decision Framework: Impact Management

AUTHORS

Peter A. Sy is Chairman of the Privacy Experts Group, eHealth Initiative, Department of Health (DOH)/Department of Science and Technology (DOST), and of the University of the Philippines Diliman Ad Hoc Committee on Open Data. He is an Associate Professor at the Department of Philosophy, College of Social Sciences and Philosophy, University of the Philippines, Diliman. A co-founder of the UP Social Innovations Lab (upsilab.org). Sy is also part of the training team of the Philippine Health Research Ethics Board (PHREB). He has been Program Director (2011-2014) of the Ethical, Legal, Social Issues (ELSI) Program, Philippine Genome Center; a research consultant at the Public Assessment of Water Services (PAWS), National Engineering Center; and Research Fellow at the UP Center for Integrative and Development Studies and at the School of Public Health, Harvard University. His current research interests and projects are in the areas of data privacy, open data, research ethics, and digital humanities. Correspondence: psy@up.edu.ph

J.C. Navera studies library and information science (archives and records management track) at the University of the Philippines Diliman.

Katrina R. Tan is currently writing her Master's thesis in Philosophy at the University of the Philippines Diliman. She graduated magna cum laude from the same institution with a Bachelor's degree in Philosophy in 2018. Her research interests include logic, ethics, and philosophy of language.

Fatima Nicolas is currently studying law at the University of the Philippines, where she also graduated cum laude with a Bachelor's degree in Philosophy.