Angeles University Foundation
College of Nursing
Summer Term – A.Y. 2024-2025
2009 Angeles City, Philippines
Website: www.auf.edu.ph / Email: registrar@auf.edu.ph

RA 10173:

Data Privacy Act of 2012

Submitted by:

Alonzo, Aleah Sheree D.

Betita, Junie Marie

Bulario, Maria Yvette

Catacutan, Keesha Noreen C.

De Guzman, Christian Joshe

Enriquez, Samantha Anne M.

Galang, Wilena-Owe

Manalastas, Ramon Luis P.

Marimla, Jhon Dominic

Regala, Katherine G.

Tan, Marv Joshua P.

BSN 2-B

Group 6

INTRODUCTION

In today's digital era, where information is easily stored, shared, and accessed through electronic systems, protecting personal data, specifically in the healthcare field, has become more important than ever. The Philippine Republic Act No. 10173, or the Data Privacy Act of 2012, was established to uphold every individual's right to privacy by regulating the collection, handling, and safeguarding of personal and sensitive information in both public and private sectors. Within clinical settings, this law is vital in maintaining the confidentiality of patient health records and ensuring that such data is accessed only by authorized individuals for legitimate medical purposes. As future healthcare professionals, nursing students must understand the principles and responsibilities mandated by this law to practice ethically, uphold patient trust, and avoid legal violations. This report emphasizes the significance of every chapter of RA 10173 and its valuable contribution in the nursing profession, focusing on its practical applications, ethical implications, and the role of nurses in protecting patient data across various healthcare environments.

BODY

CHAPTER I - GENERAL PROVISIONS

The Data Privacy Act of 2012 is a law that aims to protect every individual's right to privacy, particularly in the handling of personal information. It promotes the responsible use of information and communications technology to support innovation and national development while ensuring that both government and private institutions secure the personal data they manage. The law defines key terms such as the National Privacy Commission, data subject, consent, personal and sensitive personal information, personal information controller, and processor. It also outlines the rights of individuals regarding their data, including the rights to access, correct, erase, and file a complaint. Special care is required when handling sensitive information, such as health records, religious beliefs, and government-issued identification numbers.

The Data Privacy Act applies to all forms of personal information processing by individuals and organizations, whether in the Philippines or abroad, as long as they use equipment in the country or have a presence such as a branch or office. However, it does not cover information related to public officials' roles and functions, service contractors with the government, financial benefits from government agencies, journalistic or artistic content, official duties of public authorities, specific financial regulations or data gathered from foreign residents under their own country's laws. The law also upholds the protection given to journalists under Republic Act No. 53, allowing them to keep their sources confidential. Additionally, the Act applies to foreign entities if the personal data involved concerns Filipino citizens or residents, or if the entity has a connection to the Philippines, such as doing business in the country or collecting data through local operations.

CHAPTER II - THE NATIONAL PRIVACY COMMISSION

This chapter of the Data Privacy Act establishes the National Privacy Commission (NPC), an independent government agency responsible for implementing and enforcing data privacy laws in the Philippines. The NPC ensures organizations comply with the law, handles complaints about data privacy violations, investigates cases, and can issue orders to stop harmful data processing. It also coordinates with other government agencies and international bodies to improve data protection. The NPC is led by a Privacy Commissioner and two Deputy Commissioners, all experts appointed by the President, and supported by a Secretariat made up mostly of experienced government personnel. The Commission keeps all personal information confidential and has the authority to propose new privacy laws, assist both public and private sectors, and ensure the country meets global data protection standards.

CHAPTER III - PROCESSING OF PERSONAL INFORMATION

The Chapter III of the Data Privacy Act of 2012 provides definite rules of how one should handle one's personal information, focusing on transparency, lawful purpose, and data minimization. It requires that personal data must be collected for specific, legal reasons and used fairly and accurately. The law emphasizes that the gathered information must not be excessive and should be kept only as long as necessary and aligned with the intended purpose. Moreover, data processing of personal information is only allowed when it is not against the law and when certain conditions, like informed consent or legal obligation, are met. However, when it comes to sensitive information such as health records and legally confidential details, stricter rules are applied and can only be used with proper consent or as long as there are strong measures to protect the data. When it comes to third parties handling the personal data, the original organization still remains accountable for ensuring privacy. More than that, the law protects private and confidential communications, meaning that any sensitive information obtained improperly cannot be used as legal evidence.

In hospital settings, Chapter III of the Data Privacy Act of 2012 plays an essential role in guiding how nurses handle patients' personal and sensitive information. As part of their daily care, the nurses are legally and ethically obligated to uphold the principles of transparency, legitimate purpose, and proportionality when collecting and using patient data, such as names, medical histories, and diagnoses. This means information must only be gathered for specific medical purposes, shared only with authorized personnel, and kept accurate and relevant. Informed consent is deemed necessary, especially in cases of obtaining sensitive information such as mental or sexual health records. Even when hospitals outsource services, they remain accountable for protecting patient confidentiality. Furthermore, nurses are also required to uphold the confidentiality of private conversations between patients and healthcare providers, and such information must not be shared unless there is a valid legal basis for doing so. For

example, if a nurse discloses a teenage patient's diagnosis of a sexually transmitted infection to an unauthorized staff member or discusses it in a public area where others can hear, this constitutes a breach of patient confidentiality and clearly violates this chapter. Thus, the resolution would involve reporting the breach to the hospital's Data Protection Officer, issuing an apology to the patient, and undergoing retraining on privacy protocols to prevent recurrence. In total, this chapter brings importance to the nurse's duty to protect patient privacy, thereby strengthening trust and maintaining professionalism in the provision of healthcare services.

CHAPTER IV - RIGHTS OF THE DATA SUBJECT

This chapter is all about the right of the subject to inform his or her information that will or has been processed. In entering the data in a system, all the information must have been provided such as the nature and purpose of the data, how it will be processed, who will receive it, how long it will be stored, and the identity of the data controller. Moreso, the subject has the right to reasonably access his or her information that includes the content of the information that is being processed, the sources where it was obtained, who will receive the information, how will the information be used, the reasons for the disclosure of the information, the date where the information affects the subject, and whether automated systems were used in decisions affecting them.

However, the subject may dispute if there is inaccuracy or error in the information and an immediate correction; unless there is an unreasonable request. Once corrected, both the prior recipients and the new recipients of the erroneous data must be informed; provided that the previous recipients of the data must be informed. They also have the right to block, remove, or delete their personal data if it is incomplete, outdated, false, unlawfully obtained, or no longer necessary. Additionally, they are entitled to

compensation for any damages resulting from the misuse or inaccuracy of their personal information.

These rights may be exercised by the lawful heirs or assigns of a data subject in cases where the individual is deceased or incapacitated. Moreover, data subjects have the right to data portability, allowing them to obtain and transfer their data in an electronic, structured, and commonly used format. However, these rights do not apply when personal information is used solely for scientific or statistical research without affecting the data subject, or when data is collected for criminal, administrative, or tax investigations. In such cases, strict confidentiality must still be maintained, and the data must be used only for its stated purpose.

As student nurses, when we conduct a case study on a patient, it is our ethical and legal responsibility to explain why we are collecting their personal and medical information. This is not only for academic purposes but also to contribute to the improvement of healthcare practices and add to the body of nursing knowledge. In doing so, we must always secure the patient's informed consent through a properly documented consent form. This consent form should clearly state the purpose of the data collection, how the information will be used, who will have access to it, and how it will be stored and protected. Also, ensuring that their data is handled responsibly, ethically, and in compliance with the law. This legal safeguard protects both the data subject (the patient) and the data user (the student or institution), promoting trust, transparency, and accountability in handling sensitive information within the healthcare setting.

CHAPTER V - SECURITY OF PERSONAL INFORMATION

Personal information controllers are responsible for the implementation of reasonable and appropriate security measures which may include organizational, technical, and physical measures in order to protect the personal information from

accidental or unlawful destruction, alteration, disclosure, or misuse. To determine the level of security that will be provided, the sensitivity of the data, risks involved, size and complexity of the organization, current best practices, and cost of implementation must be taken into consideration. These measures must include the protection of computer networks, a clear security policy, systems for detecting vulnerabilities, and regular monitoring to prevent and respond to security breaches. If the third party will handle the personal information, the personal information controllers must ensure that the third party follows the same security measures. Any persons involved in the information must maintain strict confidentiality even if the employment contract ends.

In the event of data breach that involves the sensitive personal information that could lead to identity fraud or serious harm, the PIC must immediately notify both the National Privacy Commission and the affected individuals. The notification must have the description of the nature of the breach, the data involved, and the actions taken to address it. Notification may be delayed only if necessary for investigation or system recovery. The Commission may exempt or postpone notification if it's not in the public or data subject's best interest, or if it would interfere with an ongoing criminal investigation.

For example, in a hospital, data and other information are needed to be collected which includes sensitive data such as a patient's name, medical history, and lab results. The law requires the hospital to protect this information by having proper policies, securing physical files, and using technology like passwords and encryption. If a hospital fails to do this, like if a nurse posts a patient's chart online, it breaks the law and can face penalties.

CHAPTER VI - ACCOUNTABILITY FOR TRANSFER OF PERSONAL INFORMATION

Accountability in the Data Privacy Act of 2012 places a strong emphasis on the responsibility of organizations when transferring personal data to third parties. In

essence, the act of sharing an individual's personal information with another entity does not absolve an organization of its responsibility for ensuring the protection and proper use of that information. The original organization, which is known legally as the personal information controller, is still accountable for how that data is used and protected. The law ensures that when data crosses organizational or even national boundaries, the same standards of privacy and security must be maintained. This is essential in a world where data is constantly moving across systems and borders.

Section 21, which outlines the Principle of Accountability, goes even further by placing a clear, ongoing obligation on organizations to actively safeguard personal information. It is insufficient for companies and institutions to merely assert compliance with the law; they must demonstrate it through clear processes, employee training, and concrete actions. If a breach happens, the organization can't simply point fingers at another party; it needs to show that it did everything it reasonably could to protect the data. This principle is about more than just legal risk, it's about fostering a culture of respect for privacy and ensuring that people's trust isn't taken for granted. In an age where data is one of the most valuable resources, accountability is what keeps organizations from treating it carelessly.

This is especially important in hospital settings, where personal information includes not just names or contact details but deeply sensitive medical records and histories. Hospitals frequently share data with laboratories, insurance companies, partner clinics, and government agencies. Each transfer of information is a potential weak link if not handled properly. That's why hospital administrators must take extra care in choosing who they share data with, how that data is transferred, and what protections are in place. Staff members, from physicians to billing clerks, must recognize that data privacy is not solely an information technology concern; it is an

integral component of patient care. If a hospital fails to safeguard patient data, it risks not only legal consequences but also losing the trust of the very people it exists to help.

CHAPTER VII - SECURITY OF SENSITIVE PERSONAL INFORMATION IN GOVERNMENT

This chapter highlights how critical it is for government agencies to protect sensitive personal information (SPI) in their possession. Government databases often hold highly personal details, including everything from financial data to medical records, making them an obvious target for misuse or breaches. This chapter recognizes that the responsibility for safeguarding this information is not merely a technical task; it is a leadership issue. It is about accountability at the highest levels of government agencies and about ensuring that every person who interacts with this data understands the gravity of handling it properly. In a world where data leaks and cyberattacks are no longer rare but expected, this chapter serves as a crucial safeguard for citizens' trust in public institutions.

Sections 22 through 24 lay out specific responsibilities for protecting sensitive personal information within the government. Section 22 makes it clear that the heads of government agencies are personally responsible for ensuring that proper safeguards are in place. This responsibility cannot be delegated entirely to IT departments or mid-level staff. Section 23 requires strict control over which agency personnel can access sensitive personal information; access should be limited only to those whose job duties require it, and appropriate security clearances must be enforced. Section 24 ensures that even when government work is outsourced to private contractors, these contractors must follow the same stringent privacy and security requirements as the agencies themselves.

In a hospital setting, particularly in a public or government-run hospital, these principles are not merely theoretical; they are critically practical. Hospital administrators must take personal responsibility for ensuring that patient records are protected. Not everyone on staff should be able to access sensitive patient data; this access must be limited to those who directly need it for patient care or essential hospital operations. Additionally, when hospitals engage third-party service providers, such as outsourced billing companies or IT contractors, those vendors must also be contractually and practically bound to meet the same data privacy standards. A failure to do so can result not only in legal consequences but in serious harm to patient trust and well-being. For healthcare providers, protecting patient information is more than a matter of compliance; it is an extension of the ethical duty to do no harm.

CHAPTER VIII - PENALTIES

Penalties are defined as the consequences or punishments imposed when specific rules or laws are violated. These may include sanctions such as fines or imprisonment. This chapter outlines the penalties that may be applied to individuals who commit violations under the stated regulations.

Unauthorized processing of personal and sensitive information is the act of using, collecting, storing, or sharing the information without the permission or consent of the owner. Unauthorized processing of personal information is punishable by imprisonment ranging from one year to three years and a fine ranging from Php500,000.00 to Php2,000,000.00. Unauthorized processing of sensitive information is punishable by imprisonment of three to six years and a fine of Php500,000.00 to Php4,000,000.00.

Accessing personal information and sensitive personal information due to negligence is the act of unintentional information disclosure due to lack of self awareness of the surrounding environment or failure to follow the proper protocols.

Negligence accessibility to personal information is punishable by imprisonment of one year to three years and a fine of Php500,000.00 to Php2,000,000.00. While negligence, accessibility to sensitive information will receive imprisonment of three to six years and a fine ranging from Php500,000.00 to 4,000,000.00.

Improper disposal of personal information and sensitive personal information is the act of disposing or discarding information that still allows it to be read or retrieved such as throwing it in a trash bin without shredding or destroying it. Improper disposal of personal information will receive imprisonment of six months to two years and a cash fine ranging from Php100,000.00 up to Php500,000.00. While improper disposal of sensitive information will have imprisonment of one to three years and a cash fine of Php100,000.00 to Php1,000,000.00.

Processing of personal information and sensitive personal information for unauthorized purposes is the act of using, collecting, or sharing information without proper authorization or consent, especially done outside the scope of the original purpose. Unauthorized processing personal information will receive imprisonment for one year and six months up to five years and a fine of Php500,000.00 to Php1,000,000.00. Unauthorized processing sensitive information will get imprisonment of two years to seven years and a fine of Php500,000.00 up to Php2,000,000.00.

Unauthorized access or intentional breach is the act of accessing personal and sensitive information without the consent of the owner. The form of punishment includes imprisonment of one to three years and a fine of Php500,000.00 to Php2,000,000.00. Concealment of security breaches involving sensitive personal information is the act of having knowledge of a security breach and failing to notify the commission either intentionally or unintentionally will still be held accountable under the law. The form of punishment will be imprisonment of one year and six months up to five years and a cash fine of Php500,000.00 to Php 1,000,000.00. Malicious Disclosure is the act of

disclosing unwarranted or false information used for the purpose of harming the person. The form of punishment will be imprisonment of one year and six months up to five years and a cash fine of Php500,000.00 to Php1,000,000.00.

The unauthorized disclosure of personal information is a serious violation of an individual's right to privacy. Specifically, this occurs when personal data is shared with third parties without the explicit consent of the data subject, thereby breaching the provisions of the law. Consequently, offenders face penalties of one to three years of imprisonment and fines ranging from Php500,000.00 to Php1,000,000.00. On the other hand, the disclosure of sensitive personal information, such as health records, individual affiliations, or other critical identifiers, is treated even more severely under the Act. As a result, violators may be punished with imprisonment of three to five years and fines between Php500,000.00 and Php2,000,000.00.

Moreover, the Data Privacy Act imposes stricter penalties when multiple violations occur, whether simultaneously or sequentially, emphasizing the importance of compliance. Offenders in such cases face three to six years of imprisonment and fines ranging from Php1,000,000.00 to Php5,000,000.00. The law also holds corporate officers liable for enabling or negligently allowing such violations, subjecting them to penalties and the suspension or revocation of corporate rights. Similarly, public officials who commit violations under the Act may face temporary or perpetual disqualification from holding office.

In cases involving large-scale violations affecting 100 or more individuals, the Act mandates the application of the maximum penalty to ensure accountability. Additionally, public officers committing these offenses in their official capacity face disqualification from public office for a period double the length of the criminal sentence. In the last section, victims of data privacy violations are entitled to restitution, in accordance with the provisions of the New Civil Code.

CHAPTER IX - MISCELLANEOUS PROVISIONS

Chapter IX acts as the backbone of the Data Privacy Act, ensuring that the law is properly followed, enforced, and implemented effectively across all sectors. It provides a guide on how to interpret the law and requires detailed implementation guidelines by the National Privacy Commission (NPC).

In a hospital setting, this means following clear rules such as obtaining proper consent, securing patient data, handling breaches responsibly, and ensuring hospital staff understand their roles in protecting privacy. These organizations must submit reports to demonstrate compliance, while the law also provides funding for the NPC to guide, monitor, and investigate enforcement efforts. For example, hospitals are given one year to make necessary changes, like appointing Data Protection Officers and improving data systems. Even if part of the law is invalidated or voided, the rest remains effective.

This chapter as a whole serves as the foundation that keeps the Data Privacy Act law adaptable and enforceable, ensuring that personal information is treated as a legal and ethical responsibility and that institutions stay updated with current privacy standards.

CONCLUSION

In conclusion, the Philippine Republic Act No. 10173, or the Data Privacy Act of 2012, is a vital law that safeguards individuals' personal and sensitive information, including patient information in healthcare. In the field of nursing, this law is essential for ensuring privacy, confidentiality, ethical practice, and patient trust. Hence, by understanding and applying the concept of RA 10173, the nurses can protect patient privacy, prevent data breaches, and uphold professional standards in the corners of clinical settings.

AUF Honor Code

As an Angelenean who lives by the core values of pagiging mabuti, magaling at may malasakit sa kapwa, I hereby commit that I complete my academic work with integrity. This means that I shall accomplish my academic work without receiving or giving unauthorized assistance. My work also observes scholarly and intellectual standards, rules on proper citation of sources, and appropriate collection and use of data.

Reference: Republic Act 10173 - Data Privacy Act of 2012. (2024, July 22). National Privacy Commission. https://privacy.gov.ph/data-privacy-act/#w25