*International Journal of Open-Access, Interdisciplinary & New Educational Discoveries of ETCOR Educational Research Center (iJOINED ETCOR)*

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
Website: https://etcor.org

iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577

The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

# Patient Data Privacy Laws in the Medical Technology Profession: Philippines and Australia Reviewed

David Timothy De Guzman[1]*, Jamie Dimaano[2], Zelene DJ Adrianne Dy[3], Kristine May Filart[4], Sophie Nicolette Franco[5], Jarred Jones Gara[6], Mary Danielle Garcia[7], Miguel Joaquin Garcia[8], Maria Erika Ysabela Javier[9]
[1, 2, 3, 4, 5, 6, 7, 8, 9] Department of Medical Technology, Faculty of Pharmacy,
University of Santo Tomas, Manila City, Philippines
*Corresponding Author e-mail: *davidtimothy.deguzman.pharma@ust.edu.ph*

**Received**: 27 April 2024 **Revised**: 28 May 2023 **Accepted**: 29 May 2023

**Available Online**: 29 May 2023

**Volume III (2024), Issue 2, P-ISSN – 2984-7567; E-ISSN - 2945-3577**

***Abstract***

**Aim:** The protection of patient data stands as a cornerstone of ethical and responsible medical practice (Nass, Levit & Gostin, 2009). With this, this comprehensive review that intends to embark on a comparative exploration of patient data privacy laws within the medical technology profession, with a specific focus on drawing parallels of regulatory framework between the Philippines, a third-world country, and Australia, a representative first-world country.

**Methodology:** The selection and search criteria used a comprehensive electronic search of related literature published between January 1, 2000, and November 5, 2023.

**Results:** First-world nations such as Australia frequently exhibit more developed and sophisticated legal arrangements for patient data privacy. Meanwhile, in the Philippine context, this comparative lens facilitates a recognition of best practices and possible areas for improvement in upholding and safeguarding data privacy.

**Conclusions:** With promising laws put into place, it is concluded that protecting privacy is a priority not just in developed countries but also in developing countries, with the same objective of safeguarding people's privacy from further data breaches. If new situations emerge and data breaches potentially compromising patient privacy arise, these laws must be amended as necessary to avoid further damage and improve security.

***Keywords:*** Data Privacy Law, Medical Technology, Patient, Philippines, Australia

## INTRODUCTION

In the ever-advancing landscape of healthcare, protecting patient data is a cornerstone of ethical and responsible medical practice (Nass, Levit & Gostin, 2009). With that in mind, this comprehensive review takes a unique approach by comparing Patient Data Privacy Laws within the Medical Technology profession in two distinct contexts: the developing country of the Philippines and the developed country of Australia. This comparative exploration aims to draw parallels between the regulatory frameworks of these two countries, shedding light on the challenges and best practices in both settings.

The imperative for stringent patient data privacy laws within the Medical Technology profession is rooted in the increasing digitization of healthcare systems (Theodos & Sittig, 2021). As technological innovations continue to enhance patient care, the simultaneous risk of unauthorized access, data breaches, and exploitation of sensitive information amplifies. Coupled with the lack of updated legislation, a critical gap indeed exists between technological advancements, consumer informatics tools, and privacy regulations (Theodos & Sittig, 2021). Hence, patient data privacy laws emerge as a critical response to these challenges, ensuring the confidentiality and security of medical information. Beyond legal compliance, these regulations underscore the ethical responsibility of medical technologists to safeguard patient trust and uphold the sanctity of personal health data.

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

This review closely examines the patient data privacy laws in the Philippines, particularly the impact of the Data Privacy Act of 2012, juxtaposed against the regulatory landscape of a first-world country. The comparative analysis aims to unravel the nuances that differentiate these legal frameworks, shedding light on the level of stringency, comprehensiveness, and adaptability to emerging technologies.

First-world countries often showcase more mature and evolved legal structures for patient data privacy, driven by advanced technological infrastructure and a heightened consciousness of data protection (UNCTAD, 2020). This comparative lens serves as a conduit for identifying best practices and potential areas of enhancement within the Philippine context. Through this examination, the study aspires to contribute valuable insights to the global discourse on patient data privacy, fostering a deeper understanding of the ethical imperatives that underpin the Medical Technology profession on both local and international scales.

**Objectives**

This article aimed to compare patient data privacy laws within the medical technology profession in two distinct contexts: the developing country of the Philippines and the developed country of Australia. Specifically, this review addressed the following questions:

1. What are the parallels between the regulatory frameworks of the two mentioned countries in terms of patient data privacy laws?
2. What are the challenges faced by these countries in their respective patient data privacy laws?

**METHODS**

**Selection and Search Criteria**

**A. Article**

A comprehensive electronic search encompassing related literature published between January 1, 2000, and November 5, 2023, was conducted using Google Scholar, the National Library of Medicine, PubMed Central, and Scopus. The wide gap in accepted publication years was to allow laws published more than ten years ago. The following key terms and their combination and synonyms were used: "data protection," "patient privacy," "laws/regulations," "medical technology," "first-world country," "third-world country," "Philippines," and "Australia." The search strategy included reference lists of the articles gathered from the initial search. The consolidated literature was screened through their abstracts to include only those focused on and/or related to patient data privacy laws of the Philippines and Australia in the medical technology field. Out of all the searched articles, only 19 were deemed relevant and used.

**B. Country**

BakerHostetler (2019) reports that healthcare has the leading number of cybersecurity breaches, emphasizing the need for law and regulation enforcement to mitigate attacks and breaches that may corrupt rapport between patients, physicians, and hospitals. The latest United Nations Conference on Trade and Development (UNCTAD) data reveals that only 66% of nations worldwide safeguard the data and privacy of their citizens, with the relevant laws of developing countries trailing behind developed countries at 63% as opposed to the latter's 89%. (UNCTAD, 2020). Thus, one developing country and one developed country were chosen for comparison regarding laws, policies, and/or regulations related to data and privacy, especially in healthcare, specifically in the field of medical technology.

**Developing Country.** The Philippine jurisprudence pertinently acknowledges and protects the privacy of health information, thereby decreeing that independent practitioners and institutions should uphold such obligation. However, there is a lack of existing policy frameworks addressing access to health information by non-health-related professionals, use of health information for non-health-related purposes, and collection, storage, and use of electronically derived health information (Antonio, Patdu, & Marcelo, 2016). With such gaps in the country, the Philippines was chosen as the third-world country to be compared in the study.

**Developed Country.** Developed countries listed by UNCTAD were narrowed down according to their respective data and privacy laws (UNCTAD, 2014). Out of the 43 listed countries, the European Union 15 (notably Sweden and

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

Germany), Canada, Australia, and Japan were deemed to have the strictest laws against data and privacy. A search of laws related to key terms "healthcare," "medical technology," and "patients" disclosed the Swedish Patient Data Act of Sweden, Patient Data Protection Act of Germany, Personal Health Information Protection Act of Ontario, Canada, and Act of Protection of Personal Information of Japan (Bärkås, et al., 2021; Cavoukian, 2004; McLennan, et al., 2022; Saeki, 2022). Moreover, there is a distinct interest in Australia with its own government-assembled National Health and Medical Research Council (NHMRC), declared that privacy revolving around health information was its priority issue in mid-2003 (Thomson, 2004). With talks of the Privacy Act 1988, including the Health Records Information Privacy Act 2002 that was based on thirteen Australian Privacy Principles (APPs), some of which deal specifically with handling protected health information, being under review to bring privacy laws of Australia into refinement, Australia was selected as the first world country to be compared in the study.

## RESULTS AND DISCUSSION

### Data Privacy Laws in the Philippines

#### A. Overview of the Data Privacy Law

Republic Act 10173, or the Data Privacy Act of 2012, protects the individual personal information in both information and communications systems of both government and private entities.

#### B. Penalties/Fine.

Under the Republic Act 10173, Chapter VIII states the following penalties for violations that occurred under data protection.

**Section 25.** *Unauthorized Processing of Personal Information and Sensitive Personal Information* — this provision focuses on situations wherein individuals or entities process personal information without proper authorization or consent from the party. This provision refers to handling personal information without the data subject's permission or authorization under the data privacy law. The provision is designed to protect the privacy and rights of individuals by penalizing those who engage in the unauthorized processing of personal information.

Any act of unauthorized processing of any personal and sensitive information is subject to imprisonment for one (1) to three (3) years. Furthermore, anyone found guilty of unauthorized processing must pay a fine amounting to not less than five hundred thousand pesos (Php. 500,000.00) but not more than two million pesos (Php. 2,000,000.00)

**Section 26.** *Accessing Personal Information and Sensitive Personal Information Due to Negligence* — this provision outlines the legal consequences of accessing any personal and sensitive personal information due to negligence. Any individual found guilty of doing such an act will be imprisoned for one (1) to three (3) years. Moreover, a specified fine of not less than five hundred thousand pesos (Php. 500,00.00) but not more than two million pesos (Php. 2,000,000.00) will be imposed.

Furthermore, a subsection specifically addresses accessing sensitive personal information, and the imprisonment term is more severe, ranging from three (3) to six (6) years. Moreover, a higher monetary fine of not less than five hundred thousand pesos (Php. 500,000.00) but not more than four million pesos (Php. 4,000,000.00) is imposed.

The severity of consequences is higher for sensitive personal information, reflecting the increased importance and potential harm associated with mishandling more sensitive data.

**Section 27.** *Improper Disposal of Personal Information and Sensitive Personal Information* — this section aims to protect personal and sensitive information from unauthorized access by penalizing individuals who dispose of such information improperly.

Any individual found guilty of knowingly or negligently disposing, discarding, or abandoning personal information in a manner accessible to the public or in a container for trash collection will be subject to penalties. The

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

imprisonment of such an act will range from six (6) months to two (2) years, and a fine of not less than one hundred thousand pesos (Php. 100,000.00) but not more than five hundred thousand pesos (Php. 500,000.00) is imposed on those found guilty of improperly disposing of personal information.

Moreover, a subsection is added to address the improper disposal of sensitive personal information wherein the improvement is increased to one (1) to three (3) years with a higher monetary fine of not less than one hundred thousand pesos (Php. 100,000.00) but not more than one million pesos (Php. 1,000,000.00).

The penalties are designed to deter individuals from negligent or international actions that could compromise the security and integrity of an individual's information. The severity of the consequences is heightened for sensitive personal information, reflecting the increased potential harm associated with mishandling such sensitive data.

**Section 28.** *Processing of Personal Information and Sensitive Information for Unauthorized Purposes* — any individual found guilty of processing information for purposes not authorized by the data subject or not authorized under the law is subject to imprisonment and monetary penalties.

The imprisonment term ranges from one (1) year and six (6) months to five (5) years. Furthermore, a monetary fine of not less than five hundred thousand pesos (Php. 500,000.00) but not more than one million pesos (Php. 1,000,000.00) is imposed on those guilty of processing personal information for unauthorized purposes.

Moreover, stricter penalties are imposed for the unauthorized processing of sensitive personal information. The imprisonment for anyone found guilty will range from two (2) years to seven (7) years. Furthermore, a higher monetary fine of at least five hundred thousand pesos (Php. 500,000.00) but not more than two million pesos (Php. 2,000,000.00) is specified.

This provision emphasizes the importance of obtaining proper authorization for processing personal information and reinforces consequences for violations to deter any unauthorized activities.

**Section 29.** *Unauthorized Access of Intentional Breach* — this provision aims to deter and penalize individuals who intentionally and unlawfully breach systems storing personal and sensitive information. Unauthorized access includes breaking into data systems and violating data confidentiality and security.

Individuals who knowingly and unlawfully break into any systems storing personal and sensitive data will face imprisonment for one (1) year to three (3) years.

Furthermore, an individual found guilty must pay a fine of not less than five hundred thousand pesos (Php. 500,000.00) but not more than two million pesos (Php. 2,000,000.00).

**Section 30.** *Concealment of Security Breaches Involving Sensitive Personal Information* — this provision applies to individuals who, after becoming aware of a security breach and the obligation to notify the regulatory body as outlined in ***Section 20 (F)***, intentionally or through omission, conceal the information.

Those found guilty are subject to imprisonment for one (1) year and six (6) months to five (5) years. Furthermore, a fine of not less than five hundred thousand (Php. 500,000.00) but not more than one million pesos (Php. 1,000,000.00) is applied. This provision is designed to prevent and penalize the intentional or negligent concealment of security breaches involving sensitive personal information. It further emphasizes the importance of timely and truthful disclosure in a security incident involving personal and sensitive information.

**Section 31.** *Malicious Disclosure* — this provision addresses the malicious disclosure of personal information by individuals, specifically personal information controllers, personal information processors, or their officials, employees, or agents. The section applies to all individuals involved in managing or processing personal information who, with

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

malice or in bad faith, disclose unwarranted or false information regarding any personal or sensitive personal information they have obtained.

Those found guilty of maliciously disclosing false or unwarranted information face legal consequences. The imprisonment term ranges from one (1) year and six (6) months to five (5) years. Furthermore, a monetary penalty of not less than five hundred thousand pesos (Php. 500,000.00) but not more than one million pesos (Php. 1,000,000.00) is specified.

This provision protects individuals' privacy and reinforces the importance of responsible handling and disclosure of personal information.

**Section 32.** *Unauthorized Disclosure* — this provision addresses the unauthorized disclosure of personal and sensitive personal information by individuals, including personal information controllers, processors, or their officials, employees, or agents.

This provision applies to individuals who, without the data subject's consent, disclose personal information not covered by the immediately preceding section (Section 31).

Those found guilty will face imprisonment from one (1) year to three (3) years and will pay a fine not less than five hundred thousand (Php. 500,000.00) but not more than one million pesos (Php. 1,000,000.00).

Furthermore, a subsection specifically addresses the unauthorized disclosure of sensitive personal information that entails stricter and more severe consequences. Any person found guilty will be imprisoned for three (3) years to a maximum of five (5) years. Moreover, a fine of not less than five hundred thousand pesos (Php. 500,000.00) but not more than two million pesos (Php. 2,000,000.00) is specified.

**Section 33.** *Combination or Series of Acts* — this provision entails individuals involved in a combination or series of acts, as defined in Sections 35 to 32 of the law. These sections encompass offenses related to personal data protection, including unauthorized processing, access, disclosure, and other related actions.

Individuals found guilty of engaging in a combination of acts violating the specified sections are subject to a more severe penalty, such as imprisonment for a minimum of three (3) years to six (6) years. Furthermore, a fine of not less than one million pesos (Php. 1,000,000.00) but not more than five million pesos (Php. 5,000,000.00) is imposed.

**Section 34.** *Extent of Liability* — this provision entails extending liability for various entities and individuals involved in offenses related to unauthorized processing, access, disclosure, and other violations of personal data protection.

- **Corporation, Partnership, or Juridical Person:**
  If the offender is a corporation, partnership, or any juridical person, the penalty will be imposed upon the responsible officer who participated in the Act or through gross negligence that allowed the omission of the crime.

- **Juridical Person:**
  If the offender is juridical, the court can revoke or suspend any of its rights under this Act.

- **Alien Offender**
  If the offender is an alien or a foreign individual, in addition to the prescribed penalties, deportation is applied without further proceedings may occur after serving the penalties

- **Public Official or Employee:**

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

If the offender is a public official or employee found guilty of acts penalized under Sections 27 and 28 of this Act, in addition to the prescribed penalties, the individual shall be granted perpetual or temporary absolute disqualification from office.

This provision emphasized that accountability extends beyond individual offenders to responsible officers of corporations or juridical persons. The comprehensive approach aims to ensure accountability and deterrence across various entities and individuals involved in mishandling personal and sensitive information.

**Section 35.** *Large-Scale* — this provision covers the offenses applicable to the term "large-scale" in the aspect of unauthorized processing, access, disclosure, and other violations of personal data protection.

The maximum penalty provided for the scale of penalties for these offenses will be imposed when the personal information of at least one hundred (100) persons is harmed, affected, or involved as a result of the actions mentioned in the preceding sections.

This provision introduces an additional criterion for determining the severity of penalties for personal data protection offenses. When the action specified in the previous section of the law involves at least one hundred (100) persons, the maximum penalty will be imposed within the prescribed scale of penalties.

**Section 36.** *Offense Committed by Public Officer* — this section applies to crimes related to personal data protection committed by a public officer, as defined in the Administrative Code of the Philippines.
An accessory penalty is prescribed for public officers found guilty of offenses related to data protection. The accessory penalty consists of the disqualification from occupying any public office for a term double the criminal penalty imposed.

This section is a significant and specific consequence for public officers, aiming to hold them accountable for any violation related to the mishandling or unauthorized processing of personal information.

**Section 37.** *Restitution* — this section refers to the concept of restitution for any aggrieved party and specifies that the principles of the New Civil Code of the Philippines shall govern the restitution.
Restitution is restoring or compensating an aggrieved person or party for any harm, loss, or damages they have suffered.

**C. Violations in the Philippines**

The pandemic has seen an explosion in medical records, from test results and vaccine records to hospitalizations; much medical data should be shared and kept securely (Mamidi, 2022). However, that is not always the case; perhaps the most prominent cases of data privacy violations in the field of medical technology have emerged during the COVID-19 pandemic. Some countries followed international laws and local regulations to protect users' privacy in handling patient data pertaining to COVID-19, but other countries did not comply with these requirements, which resulted in privacy breaches (Alshawi et al., 2022). Having the disease came with the stigma that the patient is a walking biohazard even after the patient recovers, so they only disclose their condition to medical practitioners. However, given the novel situation, prompt and immediate measures must be taken to prevent the increase in cases, starting at the patient identification phase. To further expedite the delivery of healthcare to COVID-19 patients, the Integrated Bar of the Philippines (IBP), the Philippine Medical Association (PMA), and the Philippine College of Surgeons (PCS) issued a joint statement requesting individuals with COVID-19 and patients under investigation (PUI) to "voluntarily waive" the confidentiality of their medical condition (Cepeda, 2020). They have cited Article III, Section 3 of the Code of Ethics of the Medical Profession, which states physicians shall keep "highly confidential" whatever is disclosed to their patients "except when required by law, ordinance, or administrative order in the promotion of justice, safety, and public health," and further backs this with the Department of Health's Health Privacy Code Implementing the Joint Administrative Order No. 2016-0002, which states that "in case of emergency, where time is of the essence, disclosure may be made even without court order." Further, the Data Privacy Commission and the Department of Justice affirm the validity of the joint statement. While the public has been urged to waive the confidentiality of their condition, the decision is still ultimately up to them and

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

not mandated by law. Should an individual be forced to waive their confidentiality based on this joint statement, the offending party could be tried for and subject to the penalties or fines stated in sections 25, 28, 32, and 33 of R.A. 10173.

Although various associations and organizations have urged the public to disclose their condition to medical professionals, unauthorized disclosure of COVID-19 patients' identities continued. Dizon (2020) reports that from March to May 2020, the National Privacy Commission (NPC) investigated 22 complaints of privacy breaches involving more than 150 COVID-19 patients, as well as PUIs. At least 7 of these cases were committed by people who had access to the patients' information, while the culprits in the rest were third parties, including ordinary citizens. The offending parties varied from private individuals to corporations or entities, from a hospital staff who took a picture of a death certificate of a PUI and forwarded it to their department group chat, causing it to be spread in several group chats, to local governments themselves disclosing the identities of their patients in their official social media page to expedite contact tracing efforts, which was what the local government of Cagayan did. There also was a case in which a local radio station in Baguio disclosed private information about COVID-19 patients on social media, in which the complainants sued under Republic Act 11332 or the Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act in relation to Republic Act 10175 or the Cybercrime Prevention Act of 2012 (Cimatu, 2020). While this case and those aforementioned may be subject to the penalties or fines of R.A. 11332 and R.A. 10175, they also are criminally liable under the provisions of R.A. 10173. If such cases were to move forward in court and are found guilty, the defendants could face fines of up to the millions or imprisonment of up to seven years.

Despite these heavy consequences, there are still many data privacy offenders in medical technology. One reason, as stated, is that it could expedite processes and shorten turnaround time, such as in the case of divulging patient information on social media to quicken contact tracing. Another reason is that it could be simply because of a lack of knowledge that what these offenders were doing was wrong in the first place. Hence, medical technologists and even other professionals in the medical field, should undergo trainings or seminars to further advance their knowledge in data privacy as this has become an integral part of our healthcare system in the 21st century.

**Data Privacy Laws in Australia**

The advancement of technology and the capacity to access nearly everything with a single tap on a screen has resulted in privacy issues. One area that could not avoid the circumstances was health or medical services. As the patients' data is held in these so-called technologies with systems accessible over the internet, the risk of this information being leaked or breached increases. As a result, countries enacted legislation to restrict the use of these technical breakthroughs to safeguard patients' personal information and their medical histories.

**A. Overview of the Data Privacy Law**

The Privacy Act 1988 was passed in the Australian Parliament in 1988 and went into effect the following year. This law concerns the security of persons' personal information, including its collection, storage, use, and dissemination. This Act includes 13 Australian Privacy Principles (APPs) that can provide privacy protection for information obtained, maintained, and disclosed while imposing requirements on organizations and agencies. This was expanded and amended throughout the next few years when revisions were required due to the circumstances and further data breaches that conflicted with people's privacy.

Health service providers, including hospitals, practitioners, and other health allied professions, were governed by the Privacy Act of 1988. It focuses on the security and confidentiality of patients' data, except for cases where the data must be provided with legitimate access.

Section 6, Part II, Division I of the Privacy Act of 1988 defines health, genetic, and biometric information as sensitive information. The State or Territory health authority is the authority in charge of the state or territory's health services. The law elaborated on health information, which includes data concerning an individual's disability, illness, or injury, as well as other personal information required for providing health services. Genetic information was also included in the health information as it can predict the individual's health and its genetic relatives. Additionally, health service was expounded; the law describes it as the activities that are performed that are connected to an individual's health and aim to improve, assess, diagnose, treat, and other health-related activities.

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

In addition to the Privacy Act of 1988, the My Health Records Act 2012 safeguards an individual's privacy. This Act indicates the functions and role of the My Health Record system. It serves as a registration framework for individuals, organizations, and healthcare providers and a privacy framework regulating information in health record systems.
According to the My Health Records Act 2012, a My Health Record is a healthcare recipient's record of information managed by the system operator and comprises information for registration and other health-related data of the entity.

**B. Privacy Act of 1988 Penalty**
Under the Privacy Act of 1988, Section 6, Part II, Division 1, the enforcement body is the one that will impose a sanction, or a penalty based on the law. According to the Crimes Act 1914, there are penalty units, which indicates that a "penalty unit" is equivalent to $275.

This section focuses on the penalties or fines related to the healthcare system. Under Section 13D, Part III-Information Privacy, Division 1-Interferences with Privacy discusses offenses with their corresponding penalty.

For serious and repeated interferences with privacy, an entity makes an action that causes serious interference with an individual's privacy and is repeatedly done with the same individual or others; this causes a civil penalty of 2,000 penalty units.

**C. My Health Records Act 2012 Penalty and Imprisonment**
In the My Health Records Act 2012, civil penalties, which are also aligned with the Privacy Act of 1988, are expounded. This Act includes penalties and civil penalties. Criminal penalties include imprisonment and fines for a recorded criminal conviction, while civil penalties are monetary fines that do not involve criminal court processes.

Under My Health Record Act 2012 Section 59 Part 4-Collection, use and disclosure of health information included in a healthcare recipient's My Health Record, Division 1-Unauthorized collection, use, and disclosure of health information included in a healthcare recipient's My Health Record.

A penalty of imprisonment for five years, or 300 penalty units, or both, can be given to an unauthorized individual who collected health information on the My Health Record System and unauthorized disclosure of the health information with this individual's knowledge of his or her offense. If the person is liable for the civil penalty regarding the offense mentioned above, there will be a civil penalty of 1,500 penalty units. If the health information is obtained and used for prohibited purposes, there will be a civil penalty of 1,500 penalty units. For the secondary unauthorized disclosure, the person will face a penalty of imprisonment for five years of 300 penalty units and/or a civil penalty of
1,500 penalty units.

**D. Violations in Australia**
A recent case emerged in November 2023 that was filed against Australian Clinical Labs Limited due to a data breach in their company in February 2022. This case was filed by the Australian Information Commissioner in the Federal Court of Australia. The breach happened specifically in the company acquired by the Australian Clinical Labs Limited in December 2021, Medlab Pathology or 'Medlab,' wherein Medlab found out that a third party accessed their IT or information systems. At first, it was said that no evidence showed any patient data being extracted. Australian Cyber Security Center (ACSC), an agency in the country's government, stated that it was a ransomware incident. It has come to their knowledge, in June 2022, that Medlab patient data was found in the dark web. The company reported it to the Office of the Australian Information Commissioner, and on October 27, the amount of damage caused by the breach emerged. Approximately 223,000 individuals were affected, with 17,500 medical and health records, 28,000 credit card details, and 128,000 Medicare numbers.

The allegations were as follows: (1) the company did not take any appropriate actions from May 2021 to September 2022 to protect their patient's information, (2) they breached the s26WH of the Privacy Act to analyze if there is a possible data breach and remedy it within 30 days, (3) and they did not notify the OAIC as soon as the

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

possibility of a data breach surfaced. However, the company denies the allegations as their security measures are stable. The maximum penalty for the case is 2.2 million dollars.

According to Hunton Andrews Kurth, there are two reasons for this case's significance. First, this is only the second time a case like this has been filed since 2014. Second, it shows the prioritization of the regulators to resolve cybersecurity issues.

**Conclusion**

The introduction of technology to healthcare has redefined Medical Technology in many ways, one of which is in the context of patient data privacy. The advancement of technology opened various pathways that led to the modernization of patient data-keeping and the automated storage of it.

The studies presented information regarding privacy issues concerning health and medical services. It is important to note that chances of breaches are heightened now that these so-called technologies limit the patients' data in a system that has its own flaws. While they are incredibly convenient in this day and age, they come with significant risks. Hence, in order to protect patients' private information and medical records, a number of nations have passed laws limiting the bounds of these technological advancements within a safe range of use. However, there is currently no policy structure in place to handle the following issues: non-health-related professionals' access to health information, the use of health information for non-health-related objectives, and the gathering, storing, and utilization of health information derived digitally.

Due mainly to their modern technology infrastructure and increased awareness of data protection, first-world nations such as Australia frequently exhibit more developed and sophisticated legal arrangements for patient data privacy. Within the Philippine context, this comparative lens facilitates a recognition of best practices and possible areas for improvement. The penalties are intended to dissuade people from careless acts that can jeopardize the confidentiality and security of personal data.

With the promising laws put into place, it can be concluded that protecting privacy is a priority not just in developed countries but also in developing countries, with the same objective of safeguarding people's privacy from further data breaches. If new situations emerge and data breaches potentially compromising patient privacy arise, these laws must be amended as necessary to avoid further damage and improve security.

**Recommendations**

Engaging stakeholders, such as patients, legislators, medical professionals, and technological specialists is essential. Surveys, interviews, and focus groups can determine how well people understand these rules, what obstacles they have in complying with them, and what needs improvement. Assessing the accurate compliance rates among medical facilities in both nations is essential. It is crucial to evaluate how these rules are implemented and if they successfully address new developments in technology and healthcare. Finding the holes and suggesting fixes or additional policies to provide thorough coverage is essential. Comparative effect analyses will demonstrate how well patient data privacy regulations protect private information and stop data breaches. This can draw attention to problem areas and strengthen the culture of accountability among healthcare professionals. Examining potential global partnerships between Australia and the Philippines in the healthcare domain can promote best practice sharing, information sharing, and improved data privacy protocols. Healthcare personnel should have access to continual education and training that emphasizes their ethical obligations while managing patient information and ensures they comply with changing legal requirements. Understanding how public attitudes affect the application and adoption of patient data privacy legislation in various cultural contexts can be gained by conducting cross-cultural analyses.

It is imperative to create ethical guidelines and best practices tailored to the Medical Technology industry, considering the unique legal systems in both nations. This will help practitioners maintain ethical standards as they

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

navigate legal boundaries. Integrating technology into healthcare has revolutionized Medical Technology, particularly in managing patient data privacy. The My Health Records Act 2012 outlines stringent penalties, aligning with the Privacy Act of 1988, for unauthorized collection, use, or disclosure of health information. Nations like Australia exhibit robust legal frameworks for patient data protection, offering lessons for improvement globally. These laws must evolve to address emerging threats and ensure patient privacy amid technological advancements. Upholding privacy is not solely a developed nation's priority; it is essential globally, necessitating continuous legislative updates to safeguard sensitive health information.

Finally, starting public awareness efforts to teach patients their rights regarding data privacy in healthcare would enable them to protect their personal health information actively and will support the implementation of more stringent privacy regulations. These ongoing initiatives will have a significant impact on the conversation about patient data privacy, international cooperation, and the advancement of moral behavior in the field of medical technology in a variety of sociocultural contexts.

## REFERENCES

Alshawi, A., Al-Razgan, M., AlKallas, F. H., Suhaim, R. a. B., Al-Tamimi, R., Alharbi, N., & AlSaif, S. O. (2022). Data privacy during pandemics: a systematic literature review of COVID-19 smartphone applications. PeerJ, 7, e826. https://doi.org/10.7717/peerj-cs.826

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. DOI: 10.47895/amp.v50i4.760

BakerHostetler. (2019). Managing Enterprise Risks in a Digital World: Privacy, Cybersecurity, and Compliance Collide. 2019 Data Security Incident Response Report. Retrieved from https://f.datasrvr.com/fr1/019/33725/2019_BakerHostetler_DSIR_Final.pdf

Bärkås, A., Scandurra, I., Rexhepi, H., Blease, C., Cajander, Å., & Hägglund, M. (2021). Patients' Access to Their Psychiatric Notes: Current Policies and Practices in Sweden. *International Journal of Environmental Research and Public Health, 18*(17), 9140. DOI: 10.3390/ijerph18179140

Cavoukian, A. (2004). *A Guide to the Personal Health Information Protection Act.* Information and Privacy Commissioner, Ontario.

Cepeda, M. (2020, April 5). Coronavirus patients urged to waive confidentiality: 'Being diagnosed not a crime, stigma.' *Rappler*. https://www.rappler.com/nation/257036-coronavirus-patients-urged-waive-confidentiality-being-diagnosed-not-crime-stigma/

Cimatu, F. (2020, September 26). In Baguio, COVID-19 patients sue radio station, netizens for disclosing info. *Rappler*. https://www.rappler.com/nation/baguio-covid-patients-sue-radio-station-facebook-users-disclosing-information/

*Chapter 2*. (2017, March 27). https://www.aph.gov.au/parliamentary_business/committees/senate/economics/whitecollarcrime45th/report/c02

CRIMES ACT 1914 - SECT 4AA Penalty units. (n.d.). http://www5.austlii.edu.au/au/legis/cth/consol_act/ca191482/s4aa.html

Dizon, N. (2020, June 28). Unauthorized disclosure of COVID-19 patients' identities continues. *Rappler*. https://www.rappler.com/newsbreak/in-depth/264851-unauthorized-disclosure-covid-19-patients-identities-continues-npc/

ETCOR Educational Research Center Inc.
SEC Reg. No. 2024020137294-00
Sta. Ana, Pampanga, Philippines
Website: https://etcor.org
iJOINED ETCOR
P - ISSN 2984-7567
E - ISSN 2945-3577
The Exigency
P - ISSN 2984-7842
E - ISSN 1908-3181

LLP, H. A. K. (2023, November 15). Australian Privacy Regulator Sues in Data Breach Case. Privacy & Information Security Law Blog. https://www.huntonprivacyblog.com/2023/11/15/australian-privacy-regulator-sues-in-data-breach-case/

Mamidi, S. (2022, April 12). Protecting healthcare data during the COVID-19 pandemic. Security Magazine. Retrieved from https://www.securitymagazine.com/articles/97406-protecting-healthcare-data-during-the-covid-19-pandemic

Nass, S. J., Levit, L.A., & Gostin, L,O. (2009). Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. *National Academies Press (US).* Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK9579/

McLennan, S., Rachut, S., Lange, J., Fiske, A., Heckmann, D., & Buyx, A. (2022). Practices and Attitudes of Bavarian Stakeholders Regarding the Secondary Use of Health Data for Research Purposes During the COVID-19 Pandemic: Qualitative Interview Study. *Journal of Medical Internet Research, 24*(6), e38754. DOI: 10.2196/38754

*My Health Records Act 2012*. (n.d.). https://www.legislation.gov.au/Details/C2021C00475

*My Health Record legislation and governance*. (n.d.). Australian Digital Health Agency. https://www.digitalhealth.gov.au/about-us/policies-privacy-and-reporting/my-health-record-legislation-and-governance

Office of the Australian Information Commissioner. (n.d.). *History of the Privacy Act*. OAIC. https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/history-of-the-privacy-act

Saeki, S. (2022). Impact of the "Amendments to the Act of the Protection of Personal Information" to Global Health Research Conducted in Japanese Medical Facilities. *Journal of Epidemiology, 32*(9), 438). DOI: 10.2188/jea.JE20220141

Theodos, K. & Sittig, S. (2021). Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply. *Perspect Health Inf Manag.18*(Winter): 1I. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7883355/

Thomson, C. (2004). *The Regulation of Health Information Privacy in Australia: A description and comment.* National Health and Medical Research Council Privacy Committee.

United Nations Conference on Trade and Development. (2020). Data and privacy unprotected in one third of countries, despite progress. Retrieved from https://unctad.org/news/data-and-privacy-unprotected-one-third-countries-despite-progress