are mandated by law to get the patient's consent. The security and confidentiality of patients' personal information must also be ensured by healthcare providers by means of appropriate safeguards [10].

Patients have the right to view and update their personal data, including their health information, under the PDPA. In some situations, patients have the right to request that their personal data be destroyed or anonymized.

The PDPA also creates a legal framework for Indonesian personal data protection in addition to these measures. To oversee the PDPA's implementation and enforcement, the law establishes the Personal Data Protection Commission as a data protection authority. Healthcare providers and other organisations who transgress the terms of the PDPA may be subject to investigations, penalties, and other enforcement actions by the commission [11].

Here are some takeaways as to how PDPA helps in protecting the healthcare industry in Indonesia:

- Privacy protection for patients: The PDPA offers a thorough framework for the protection of personal data, including information on health. By requiring healthcare providers to get patients' permission before collecting, using, or revealing their personal information, this can aid in protecting patients' privacy.
- Promoting data sharing: The PDPA can aid in promoting data sharing between healthcare providers and other system stakeholders. By enabling more precise and thorough medical records, this can result in better patient care and better health outcomes.
- Increasing data security: Under the PDPA, healthcare providers must put in place the proper security measures to guard against unauthorized access, use, or disclosure of personal information. This can lessen the possibility of data breaches and safeguard patients' private health information.
- Promoting trust: The PDPA can aid in fostering trust between patients and healthcare professionals by establishing a clear framework for the protection of personal data. Better health outcomes may result from more patient engagement and involvement in their own care.
- Overall, by promoting patient privacy, encouraging data sharing, improving data security, fostering trust between patients and healthcare providers and improving patient outcomes by establishing a clear legislative framework for data protection, the PDPA can significantly support Indonesia's healthcare sector.

B. Difficulties and Concerns Regarding Data Protection in the Indonesian Healthcare Sector:

Despite the regulations in place, there are several challenges and issues related to data protection in the health sector in Indonesia. Some of these challenges include:

- Lack of knowledge: Patients' and healthcare practitioners' ignorance of their rights and responsibilities regarding data protection is one of the major difficulties. Healthcare providers could not completely comprehend their obligations to protect personal data, and many patients might not be aware of the risks and repercussions of data breaches. This can lead to non-compliance with regulations, mismanagement of personal data, and inadequate protection of sensitive information [13].
- Lack of resources: It is possible that many healthcare organisations lack the staff, infrastructure, and technology required to put in place comprehensive data protection procedures. Maintaining accurate and full records, preventing unauthorised access to personal data, and effectively handling data breaches may become difficult as a result. This can also leave personal data vulnerable to cyber-attacks and data breaches.
- Limited regulatory enforcement: Although Indonesia has laws in place to protect personal information in the health industry, their application may not always be guaranteed. For regulatory agencies to effectively monitor and enforce compliance with data protection requirements, there can be a shortage of resources or experience.
- Cultural considerations: In some circumstances, cultural considerations could make it more difficult to protect patient data. Due to cultural or religious views, patients may be reluctant to divulge sensitive medical information, which can make it difficult for healthcare providers to gather accurate and full data [12].

In general, overcoming these difficulties and problems with data privacy in the healthcare industry in Indonesia will call for a multifaceted strategy including participants from all facets of the healthcare system. This could involve stepping up awareness and education initiatives, allocating more funds, and stepping up regulatory enforcement.

C. Analysis of Data Protection Law in Health Sector sin Indonesia:

A thorough legal framework for the protection of personal data, including health data, in the healthcare industry is provided under Indonesia's Personal Data Protection Law. All data controllers and processors, including healthcare providers and other organisations that handle personal data in the medical field, are subject to the law.

The key principles of the Personal Data Protection Law in relation to the health sector include:

The requirement that data controllers and processors get consent from individuals before collecting, using, or disclosing their personal data, including health information, is one of the most crucial legal principles. This means that before collecting, using, or disclosing patients' health information, healthcare professionals must have their express consent.

- Limitation on use: Personal information, including health information, may only be handled for clear, acceptable, and legal objectives. Only those purposes that have been explicitly disclosed to patients and are

required for the delivery of healthcare services may be collected and used by healthcare professionals.

- Data minimization: Healthcare providers must make sure they only gather and use the bare minimum of personal information—including health information—to accomplish the particular goals for which the information is being gathered and processed.
- Security: Healthcare providers must put in place the proper security measures to guard against unauthorised access, use, or disclosure of personal data, including health data. The confidentiality, integrity, and availability of health data must always be maintained by healthcare practitioners.
- Healthcare providers must make sure that personal information, including health information, is not stored any longer than is required for the particular objectives for which it was gathered and processed.
- Data subject rights: The law outlines a number of data subject rights, including the right to access and update personal information, the right to object to the processing of personal information, and the right to request the deletion of personal information under specific conditions.
- Accountability: Healthcare providers are responsible for their data processing actions and are required to keep records of such actions. To make sure that their data processing activities comply with the law, they must also perform routine reviews [14].

Indonesia's health sector has significant challenges related to data privacy. A thorough legal framework for the protection of personal data, including health data, is provided under the Personal Data Protection Law. The law specifies unambiguous guidelines for the handling of personal data, protects data subjects' rights, and creates a supervisory authority to uphold the law. Concerns like knowledge, consent, security, data retention, data subject rights, data breach response, and supervision still need to be addressed in relation to data protection. Healthcare providers in Indonesia can enhance the privacy and security of personal data, including health data, and boost public confidence in the healthcare system by putting best practises and recommendations for data protection in the health sector into practice [15].

3. Health Data Protection in Canada

There are two federal laws in Canada regarding personal data protection, applicable to public and private sectors. “The Privacy Act, 1985”, which regulates a person’s right to access and correct information, only applies to federal government institutions. The “Personal Information Protection and Electronic Documents Act (PIPEDA), 2000”, regulating collection, usage and disclosure of personal information applies to private-sector organizations and federally-regulated businesses.

Apart from the federal laws, Canada’s ten provinces and three territories also have separate legislation protecting personal data and personal health data. Each of them has separate public-sector laws which apply to them, instead of the Privacy Act, 1983. PIPEDA, 2000 applies to 10 of the provinces and territories of Canada, while the other three have separate private-sector laws that are substantially similar to the federal law.

Before going into protection of health data in Canada, it is pertinent to put forward what is understood by personal information and personal health information. Both the federal laws define personal information in their own ways. However, in general, personal information may be considered to refer to any information of an ‘identifiable person’. Such information may be in the form of

- Race, Nationality or Ethnicity, Religion, Colour, Age, status of marriage
- Educational, Medical, Criminal or Employment history, financial information
- Any identifying number or symbol
- Address, Fingerprints, Blood type
- Personal opinions or views etc.

Office of the Privacy Commissioner of Canada provides advice and information for protection of personal information, while also enforcing the two federal laws in the country.

A. Protection of Health Data in Canada

PIPEDA, 2000 is all-encompassing inasmuch as it refers to ‘personal health information’ in Section 2 of the Act. Personal health information, according to PIPEDA, 2000, refers to

- Information of physical or mental health
- Information of any health service
- Information concerning donation or examination of body part or bodily substance
- Information collected in the course of providing health service
- Incidental information

Sub-clauses (d) and (e) to Section 2(1) also bring information collected in the course or incidentally, respectively for the provision of health services, into the scope of the Act. It can therefore, be inferred that the provisions of the Act for the protection of personal data also applies to protection of personal health data, except where it has been explicitly excluded [16].

Section 5(3) of PIPEDA, 2000 states that an organisation is only permitted to gather, utilise, or share personal data when it is considered as appropriate by a reasonable person. Section 6.1 of the same establishes the importance of valid consent regarding collection, use or disclosure of such information and Section 7 lists out the situations wherein information may be collected, use and disclosed without

valid knowledge or consent of the person. Section 9 also regulates access to information to a person if information regarding third person may be disclosed through that.

On breach of any provisions of the above Act, the court, upon investigation, may order the organisation to correct its practices, publish a notice in this regard and award damages to the aggrieved persons.

Furthermore, most of the provinces have their separate laws to regulate and protect health information. We shall consider them one by one.

- Alberta- Alberta's separate legislation for the protection of health data is the "Health Information Act".
- British Columbia- British Columbia protects health data via the "E-Health (Personal Health Information Access and Protection of Privacy) Act".
- Manitoba- The separate legislation of Manitoba is the "Personal Health Information Act".
- New Brunswick- New Brunswick protects health data through "Personal Health Information Privacy and Access Act".
- Newfoundland and Labrador- The separate legislation is called "Personal Health Information Act".
- Northwest Territories- The health data is protected by "Health Information Act".
- Nova Scotia- Nova Scotia's separate legislation to protect health data is "Personal Health Information Act".
- Ontario- "Personal Health Information Protection Act" protects health data in Ontario.
- Saskatchewan- "Health Information Protection Act" protects health data in Saskatchewan.
- Yukon- Yukon's separate legislation is "Health Information Privacy and Management Act".

Each of the above laws regulate the collection, use and disclosure of health information and many of them are actually substantially similar to PIPEDA, 2000. Nunavut, Prince Edward Island and Quebec do not have a separate legislation dedicated to protection of health data [17].

Recently, e-health has developed into a major area of deliberations and discussions. Research by Richard C. Alvarez has shown that e-health can lead to collection, processing and maintenance of health information for various uses like providing health services. He has specifically mentioned Infoway, an independent, not-for-profit health corporation and its mission to facilitate the development and adoption of electronic health information systems which also, strictly incorporates standards of confidentiality and protection of health information. Several Health Information Networks have also been mandated by different provinces and territories like Newfoundland and Labrador, Saskatchewan and Alberta to connect provincial hospitals, nursing homes, physicians, pharmacists, and healthcare providers.

Research has also established how rapid technological change and advancement like Big Data and Artificial Intelligence is creating more and more information and thus, the protection of such information becomes important. Thus, revolutionizing technological advancements may threaten privacy of health data. While Canadian framework for data protection, especially health data protection is fairly open to data sharing for research and other appropriate use, there is pressure to strengthen laws. Thus, data protection laws in Canada must attempt to reach to a perfect balance of safeguards and engagement through data sharing, taking responsibility and accountability for the same. In 2022, the Digital Charter Implementation Act, also known as Bill C-27 was introduced in the Canadian Federal government which still is in the draft stage and awaits assent. If that bill is passed, it would bring the Consumer Privacy Protection Act (CPPA) which would replace PIPEDA, 2000 and would also bring a separate tribunal into existence for such matters.

4. The New Framework of Data Protection in India

Earlier, India had introduced the Health Data Management Policy in 2020. The draft policy included creating a system of personal and medical records which would be voluntary and based on consent. However, it was criticized for allowing access of health data to private entities. The Government then released the revised version of Health Data Management Policy of 2022 which addressed these issues. A Personal Data Protection Bill was also introduced in 2019. This bill was highly criticized, with many raising concerns about privacy [18].

India has passed a comprehensive act on data protection- the Digital Personal Data Protection (DPDP) Act, 2023 which was notified in August 2023 but has not come into force yet. It shall be supplemented by rules to be issued by the central government in due course of time. A Data Protection Board of India shall also be established as an adjudicatory body. The DPDP Act is applicable to any data identifiable with the data principal. It also applies to all kinds of digital personal data and not only special categories. However, removing the distinction between sensitive personal data and other data may turn out to be disadvantageous and may create risks since health data is no longer considered sensitive data. Moreover, it also raises concerns of usage of artificial intelligence in the case of data management. For an illustration, Section 2(g) of the DPDP Act, 2023 mentions "consent manager" which can be any person registered with the above-mentioned Board. Also, Section 2(s) mentions that a person can be an "artificial juristic person" as well.

Article 22 of the Regulation Number 20 of 2016 on Personal Data Protection in Electronic Systems by Minister of Communication and Informatics of the Republic of

Indonesia provides certain requirements to be complied with for transferring data outside of the country. The parties must-
a. Be in coordination with the Ministry or officials / institutions that are authorised to do so; and
b. Implement the provisions of laws and regulations on cross-border Personal Data exchange.

Canada does not explicitly regulate or prohibit cross-border transfer of data. If the personal information is being used for the purpose it was originally collected for under the PIPEDA, 2000, then this personal information may be transferred to an organization outside of the jurisdiction [19].

On the transnational flow of data, the DPDP Act, 2023 in India gives unilateral powers to the Government to restrict flow of data.

6. Conclusion

The National Strategy on Artificial Intelligence that was published by the Government of India has been a major driver in artificial intelligence's continued expansion into digital health solutions, which have recently started to be implemented. Digital interventions open the door to the accumulation of enormous amounts of data, which artificial intelligence systems that employ mathematical algorithms can then use to attempt to make sense of these complicated and extensive datasets. Some algorithm-based mental health apps have been reported to use AI; however, the basic conflict between the significance of permission and data reduction as stated in Indian data protection frameworks like the Sri Krishna report makes this type of intervention ecology untenable. By acquiring significantly more information about an individual's private life from them, linking Aadhaar to these systems can make them more intrusive. The setting and features of both the person and the condition can cause health data points to differ, which can make it difficult for AI systems to draw meaningful relationships between the two. Because there is a lack of knowledge, education, and organization to perform the right to informed choice in the vast bulk of healthcare situations in India, obtaining meaningful consent is already difficult. As a result, obtaining consent can become even more difficult if medical evidence is instantaneously fed into an AI system. Even though data are often directly linked in ways which are not easily recognizable, or since the impacts are not completely understood, it's going to be challenging for people living with medical problems to perceive and/or exercise their own consent in these types of situations. This will also be the case for the family members of these individuals.

In conclusion, the examination of data protection regulations in the healthcare sectors of Indonesia and Canada underscores the critical importance of balancing technological advancements with robust privacy measures. Both nations are navigating the complex landscape of digital health, aiming to harness its benefits while safeguarding patients' sensitive information. While Canada's well-established legal framework showcases a commitment to data security, Indonesia is actively adapting its regulations to keep pace with the evolving e-health landscape. As these countries work towards enhancing healthcare services through digital means, it is evident that comprehensive data protection measures are integral to fostering trust among patients, healthcare providers, and stakeholders. However, the journey towards optimal data protection is ongoing, requiring continuous adaptation to the dynamic nature of technology and the ever-changing healthcare environment.

References

[1] K.S. Bagot, S.A. Matthwes & M. Mason, Current, Future and Potential Use Of Mobile And Wearable Technologies And Social Media Data In The ABCD Study To Increase Understanding Of Contributors To Child Health, 32, Dev. Cogn. Neurosci.,121-129, (2018)

[2] Global Strategy on Digital Health 2020-2025, https://www.Who.Int/Docs/Default-Source/Documents/Gs4dhdaa2a9f352b0445bafbc79ca799dce4d.Pdf (Last Visited:12/02/2023).

[3] Oracle India, https://www.Oracle.Com/In/Big-Data/What-Is-Big-Data/ (Last Visited:12/02/2023).

[4] Vasanthi Vara, Better Data Collection and Convenience For Remote Monitoring Of Patients The Main Benefits Of Using Digital Health Technologies In Clinical Trials, Clinical Trials Arena, (Last Visited: 12/02/2023) https://Www.Clinicaltrialsarena.Com/News/Better-Data-Collection-Main-Benefit-Of-Digital-Technologies-In-Clinical-Trials/

[5] At A Glance: Data Protection And Management Of Health Data In Indonesia, 2023, lexology.com/library/detail.aspx?g=1c823558-17b0-4e91-844a-82e746a80883#:~:text=Currently%2C%20Indonesia%20does%20not%20have,data%20protection%20for%20electronic%20systems.(last visited: 28/04/2023)

[6] Cahyani Endahayu & Reagen Mokodompit, Indonesia: New medical records regulation — what's new? Global Compliance News (2022) ,https://www.globalcompliancenews.com/2022/12/20/https-insightplus-bakermckenzie-com-bm-healthcare-life-sciences-indonesia-new-medical-records-regulation-whats-new_12162022/ (last visited: 28/04/2023)

[7] Personal Data Protection (PDP) Law of Indonesia, Cpl.Thalesgroup. Com, https://cpl.thalesgroup.com/compliance/apac/indonesia-personal-data-protection-law (last visited: 28/04/2023)

[8] At a glance: data protection and management of health data in Indonesia, Lexology, lexology.com/library/detail.aspx?g=1c823558-17b0-4e91-844a-82e746a80883#:~:text=Currently%2C%20Indonesia%20does%20not%20have,

data%20protection%20for%20electronic%20systems (last visited: 28/04/2023)
[9] Summary Of Privacy Laws In Canada Office Of The Privacy Commissioner Of Canada, Office Of The Privacy Commissioner Of Canada (2018), https://www.Priv.Gc.Ca/En/Privacy-Topics/Privacy-Laws-In-Canada/02_05_D_15/ (Last Visited: 15/01/2023).
[10] Privacy Act, 1985, Section 3, R.S.C, C. P-21 (Canada); Personal Information Protection and Electronic Documents Act (PIPEDA), 2000, Section 2, S.C, C. 5 (Canada)
[11] Office Of the Privacy Commissioner of Canada (2022) https://www.priv.gc.ca/en (last visited: 15/01/2023)
[12] Richard C. Alvarez, The Promise of E-Health- A Canadian Perspective, 1 E-Health Int. (2002)
[13] Rachel V. Rose and Lance H. Rose, Appreciating Healthcare Data Privacy Laws in Canada, the United Kingdom, and the United States, 49 EDP Audit, Control and Security Newsletter, 18 (2014)
[14] Adrian Thorogood, Canada: will privacy rules continue to favour open science? 137, Human Genet, 595 (2018); Nuffield Council on Bioethics, Artificial Intelligence (AI) In Healthcare and Research, https://www.nuffieldbioethics.org/publications/ai-in-healthcare-and-research (last visited Jan 15, 2023)
[15] New Privacy Laws Around the World and How They'll Affect Your Analytics, PIWIK 11 new privacy laws around the world and how they'll affect your analytics - Piwik PRO (last visited: 20/01/2023)
[16] Dipika Jain, Regulation of Digital Healthcare in India: Ethical and Legal Challenges, 11, healthcare (BASEL) (2023)
[17] The Digital Data Protection Act, 2023, No. 22, Acts of Parliament (India)
[18] Article 22, Regulation Number 20 of 2016 on Personal Data Protection in Electronic Systems (Indonesia)
[19] The Personal Data Protection Bill (2018), Government of India. Ministry Of Electronics and Information Technology,https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf, (last visited:01/03/2023).