Data Protection in Contemporary ASEAN:
Analyzing the Healthcare Data Breach in Indonesia.

May 2022

ASEAN YOUTH ORGANIZATION
RESEARCH CENTER 2023

Data Protection in Contemporary ASEAN: Analyzing the Healthcare Data Breach in Indonesia.

Competence, Equity, and Opportunity

rd@aseanyouth.net | Arcade Business 6-03, Penjaringan, North Jakarta, Indonesia

Acknowledgements

Data Protection in Contemporary ASEAN: Analyzing the Healthcare Data Breach in Indonesia

This research was created as a part of AYO Recent's Project Cycle 1 (October 2021 to May 2022). The researchers have created this report under the guidance and supervision of AYO Recent, Research Center.

Research Team

Surya George (Researcher).
Grace (Thiri) (Researcher).

All the researchers contributed to this manuscript equally.

Abhishek Vats, Co-Founder, AYO Recent (Principal Investigator).
Chendy Puspita, Youth Research Consultant.

Design and Graphics

Ratu Naurah Hilalah, AYO MarCom Department.

Table of Contents

Abstract

The cases of cyberattacks have been more prevalent since the rapid shift of daily activities into digital-based, especially amid the Covid-19 pandemic when the utilization of digital technologies is carried out in various countries to store the citizens' health information data as an attempt to prevent further spread of the virus. However, some challenges appeared, such as the threat of data security since personal health information is considered more valuable in the market. The leakage and theft of personal health information from the citizens, including the Covid-19 test status, medical records, vaccination certificates, and other personal information, have threatened the security of the citizens. ASEAN countries are especially vulnerable to cybersecurity which is proven by several personal data breach cases. Indonesia is one of the countries which has experienced the case of a personal healthcare data breach in the last two years of the pandemic, which has brought disadvantages for the citizens. The findings of recent research specifically share that the cause of data breaches in Indonesia is due to the lack of basic security measures of the data privacy protocols and weak cybersecurity infrastructure which make Indonesia healthcare information prone to be leaked by hackers. However, the discussion regarding the regulation and framework which could be the method for preventing such cases are yet to be discussed. Even though Indonesia has issued a commitment to personal data protection together with other ASEAN countries, the seriousness of the government to implement the proper regulation specifically for data protection remains questioned. Using secondary data from Indonesian healthcare data breaches, including two cases of BPJS and test-and-trace Covid-19 applications, this paper is trying to analyze the root causes of the accident and include the contribution of the existing laws and regulations in preventing such accidents from happening in the future.

Keywords: Health care, Data protection, Data leak, Indonesia, Cyber security.

Background of the Study

Health is the most crucial parameter of a country's development. Healthy citizens are an asset to the country's progress. Therefore providing the citizens with an affordable and quality health care service has been a growing concern of all nations worldwide. In recent years, the government has developed dramatically in the healthcare sector to make the services equally affordable and bridge the health gap.

Indonesia is on its road to achieving universal health coverage. To strengthen the health of its citizens, the government introduced its Universal Health Coverage which is locally known as JKN (Jaminan Kesehatan Nasional), in 2014, which the Social Security Administrator runs for the Health (BPJS) agency. Citizens must enrol in the program; it is one of the world's most extensive universal health programs that cover 200 million people by providing them medical services ranging from dental check-ups to complicated procedures, making it accessible to all its citizens.

Digitalization in healthcare services is considered one of the key parameters to achieve health equality by the World Health Organization; since 2005, it has been adopted to promote more equitable, affordable, and universal access to healthcare (HKTDC Research). Ever since then, ASEAN Members State (AMS) have also developed specific strategies to develop the healthcare sector and, as a result, initiated ASEAN Digital Master Plan 2025 to enhance digital health because it was believed that digitalization could help ASEAN alleviate the existing challenges in the health sector, can expand patients access to healthcare, and provide affordable and quality access to healthcare services. Indonesia being the fourth most populous country globally with a unique geographical composition and over the distribution of population in the rural areas, presents immense challenges to bring equitable and quality healthcare services to all its citizens. Therefore, tapping newer digital innovations of the inspiration of the ASEAN Digital Master Plan can ensure excellent traceability and affordability to healthcare services.

Thus a country with the highest internet penetration rate and increased urbanization pushes the need to satisfy the growing demand for digitization.

The digital healthcare platform provides a great range of services, but the three main segments according to KEN research are Telemedicine/Tele-health - where patients can consult doctor through an online teleconsultation, Halodoc is a notable telemedicine service platform in Indonesia which has immense healthcare service option such as e-pharmacies, help patient connect with required diagnostic centers etc; E-pharmacies – where patients can receive their medicines prescribed, delivered at their doorsteps without need to wait for long queues before pharmacies in the hospital, Health Management Services – where patients can manage their health records and share their health records with their consulting doctors without waiting long time to get documents at hand, insurance companies have partnered with various digital health initiative to kick start the digital drive such as in Indonesia the insurance company Prudential partnered with Halodoc to provide telemedicine services to its premium holders, providing e-services to do the process of medical insurance claims etc, digital payment options to pay digitally without cash transactions and the list goes endlessly. These immense services can help the healthcare industry take a new leap towards equality and equitable health services. To facilitate the digital drive in ASEAN, the government has considered various partnership options with the private sector to develop the healthcare sector of an economy, which can help the government facilitate the needs of rural sides of ASEAN, thus reaching out to more unreachable places.

Introduction

Digital Health Ecosystems, a report by McKinsey & Company, states that the consumer-centric digital health market in Asia is projected to grow from US$37.4 billion in 2020 to US$100 billion in 2030, in which ASEAN countries like Indonesia, Vietnam, Philippines and Malaysia are considered good potential markets in Asia.

According to AsiaLink Business, digital healthcare revenues in Indonesia are expected to reach $973 million by 2023 at a compound annual growth rate of 60%. For Indonesia, the health sector is using technology and the benefits of growing internet connectivity to address complex challenges associated with delivering health services to 260 million people across an archipelago of 17,000 islands. However, a shortage of health professionals and physical infrastructure constraints exacerbate this challenge's scale.

The pandemic even increased further dependence on digital health systems. Governments in all ASEAN nationals come forward with several digital platforms to track and trace the infected patients, update citizens about government health updates, and keep track of citizens' health status. In Indonesia, the Ministry of Communication and Information Technology launched a mobile application, Peduli Lindungi, that warns users when they enter into contact with a patient. The government also partnered with Halodoc and Go-jek (a ride-hailing app firm) to provide COVID-19 diagnostics support in rural areas.

Another unknown, not much talked about, dimension of digital health care is its vulnerability to cyber-attacks and data privacy. Since the health care sector mainly deals with a tremendous amount of sensitive information, its confidentiality makes it more likely to undermine a bad attack. Hackers are misusing this vulnerability to manipulate and steal victims' sensitive data.

The Motivation of the Study

- **How national security is paramount to maintaining and preserving human resources.**
- **Having privacy and security is the essential requirement and right for citizens to attain safety and justice.**
- **To achieve a systematic strategy and institutions to develop Indonesia's healthcare system and reduce the vulnerability of health data placed digitally.**
- **Covid-19 has proved how vital and inevitable an individual's health is and how a robust framework can transform Indonesia into a new secure and strongly protected nutshell.**

"Health information is a treasure trove for criminals," says Tom Kellermann, Chief Cybersecurity Officer at Carbon Black. The rapid paradigm shift to the digital economy from manual report keeping and hundreds of papers has no worries to present us. Still, the vulnerability of data exposure in healthcare is a serious concern to the health and care sector because the data itself handles the most super-sensitive information of an individual. The problem is not just cybersecurity but also the threat that it conveys to the health and safety of the patients. The Healthcare industry is the most vulnerable target group for cyberattacks as a health record consists of a patient's physical and mental health information. This abundant sensitive and confidential information makes itself more risk-prone to attacks and raises the need for increased data protection at all levels.

Rapid digitalization has increased the level of healthcare data breaches worldwide, and a breach has become so inevitable for an institution to escape from it.

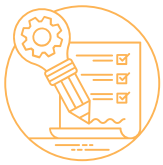
The external and internal threats include threats posed by hackers through malware and ransomware attacks, SQL injections, data theft by employees etc. Health statistics are the most important and valuable data in the black market than a financial card detail, yet, the nature of the data's sensitivity makes it more prone to breaches. The immense network of devices often makes hackers take advantage of manipulating and initiating an attack. These opportunistic attacks towards digital health data are a situation of life and death. The more likely the problem grows, developing this problem can lead to financial losses to the institutions, making it lose the credibility the users provide them. Health is the integral element of a nation; lack of data security in health matters can open up the country to more susceptible security threats resulting in the invasion of national security. Apart from that, invading privacy and manipulating the person's identity can give rise to psychological, economic and social trauma and loss of trust towards the systems established and executed by the national/private authorities.

Objective of the Study

Analyze the healthcare data breaches happening in Indonesia and draw inferences from them.

Highlight the most recent and relevant data breaches in healthcare from Indonesia and cite an example of a role model for Indonesia.

Highlight the consequences of the data breaches towards the citizens and the vulnerability of ASEAN towards cyber-attacks.



Analyze existing laws regarding data protection and its application and technicalities.

Summarize the findings of data breaches and provide recommendations for the enhancement of both national security and healthcare safety.

Research Question

1. Is the Indonesian health care sector strong enough to withstand a cyber apocalypse?
2. Do we have to comprise the country's national security by lacking behind in the cybersecurity arena?
3. What can the changing paradigm shift to the digital healthcare sector mean to Indonesia?

Expected Outcome

This research paper will equip us with the knowledge of how a data breach in the healthcare sector means the development of cyber security and the economy and how exposure to confidential reports can hamper the nation's safety. Last but not the least, it provides the readers with the most suitable recommendations and presents them with the awareness needed to overcome the social issue.

Methodology

Qualitative Method

Journals | Newspaper Articles | Blogs | Websites

The method used in the research is the qualitative method by referring to the information collected from various sources such as journals, newspaper articles, blogs, websites etc. Then, we observed the problems of the healthcare data breach, studied relevant case studies, and gathered the information for the process of the textual analysis where we analyzed the existing laws and regulations that are meant to protect the integrity and privacy of the citizens of Indonesia. With the research method, we will cite another ASEAN country that will stand up as a role model for the development of digital healthcare in Indonesia.

Our study aims to provide the readers with awareness about the data breaches in the healthcare sector of Indonesia. As part of the sample size selection, we primarily focus on Indonesia, which has the highest internet penetration rate in ASEAN and is also emerging as a digital economy. The research paper highlights the previous incidents of data breaches in healthcare, the causes of a breach, their impact on society, and recommends possible remedies to overcome the social cause.

Literature Review

Overview of Indonesian Digital Healthcare System

In Indonesia, by the onset of the pandemic, the healthcare system has taken up a digital transformation to improve the health system in general where earlier it was heavily dependent on traditional pen-paper manual works. But the process has caught up with various challenges for acing the advantage of digitalization, to name a few:

- Fragmented Data
- Third party interference
- Digital data being manually documented
- Inadequate Regulation in the form of lack of data protection and privacy laws

These process of maintaining incomplete, inaccurate data recording hampered the quality of health service offered by the government. In response to further harnessing digital health, the government came up with a digital policy, "The Digital Health Transformation Strategy Blueprint 2024" which talks about the integration and development of health data systems and healthcare application systems. The failure to allocate a team dedicated for overviewing the data protection aspect of digital health was a major missing puzzle point in the policy framework adopted by the government.

Case Study

2017: The Darkest Period of Data Breaches

"2017: Year of Data Breach," says Bloomberg News Agency
The year 2017 witnessed a massive ransomware attack that withheld all major companies, schools, universities, hospitals etc around the globe. The worst-hit countries were the UK, USA, Spain, France and Russia. In Indonesia, two major cancer hospitals were attacked which put a hold on all major activities of the hospital for a day. The hackers tricked the victim to open the attachments of emails that appear to be invoices, job offers etc and demanded money in the form of bitcoin to restore the files. The ransomware blocked the user's access to data which can only be revised after the payment is done, it took the advantage of the vulnerability of Microsoft's Windows Software. The attack was called cruel by the chairperson of one of the hospitals but lucky Indonesia doesn't appear to be the worst hit by the attack. This incident was called a wake call by the President of Microsoft to further harness the cyber security infrastructure.

Sources: BBC News, govinsider.asia

Case Study

PeduliLindungi & eHAC Data Breach in 2021

PeduliLindungi and eHAC are both mandatory COVID-19 tracing apps required to travel within Indonesia not just for citizens but also for foreigners as well. The app collects personal information, health status, contact details and COVID-19 test results. In 2021, around 1.3 million personal data of Indonesian citizens were reported to be leaked from the government-owned COVID-19 tracking app causing even President Joko Widdo data to be made available online. The security failure in the app featured the outsiders gaining personal and COVID-19 information of citizens. Researchers from vpnMentor discovered that the app failed to implement privacy protocols to prevent data from getting leaked from the open servers. Later, an investigation on eHAC by Indonesia's Computer Emergency Response Team, the Ministry of Communication and Information Technology(Kominfo) reveals that the breach was on an older version of eHAC and the new version of eHAC is under the peduliLindungi and denied the breach on peduliLindungi. In a press conference, the health ministry announced an investigation and urged citizens to delete the older version and download the government's newer version, peduliLindungi with integrated eHAC. The breach created an outcry among the citizens and the netizens took the internet to express their concern. "A majority of data breaches in Indonesia affect government-held data," says Alia Yofira Karunian, a researcher at the Institute for Policy Research and Advocacy or ELSAM, in an analysis of the eHAC databases.

Sources: Jakarta Globe, govinfosecurity

BPJS Data Breach

BPJS- BPJS Kesehatan (Badan Penyelenggara Jaminan Sosial Kesehatan) is a social security agency of Indonesia aimed at providing universal health care to its citizens, it's required not only for Indonesian citizens but also foreigners living in Indonesia. As a public institution, BPJS Kesehatan manages a huge and detailed data repository in support of its mandate to administer universal health coverage for the Indonesian public. It is regulated under legislation No.14, 2004 regarding the national social security system. The first incident happened in May 2021 when the personal data of 279 million Indonesians were stolen and sold on hacking platforms called raid forums. The exposed data includes names, BPJS identity numbers, addresses, phone numbers and payment status of the victims. After the incident, the Communication and Information Technology Ministry said that it has suspected personal records of at least 100,000 individuals have been leaked from BPJS Kesehatan and asked the country's national insurance company to notify the individuals about the breach also summoned BPJS Kesehatan's directors to explain the data breach and agreed to investigate it deeper alongside the National Cyber and Encryption Agency (BSSN). Immediately after the breach was noticed the Communication and Informatics Ministry (Kominfo) announced they had blocked the website.

Analysis

Consequences of A Healthcare Data Breach

PHIs include the most crucial sensitive information about a patient's health status; therefore, maintaining it with utmost security and safety has become a significant concern to most healthcare providers that have initiated digitalization in healthcare services. As we all know, in the modern world, "Data is the new oil" therefore, hackers find those sensitive data profitable enough to share on the dark web to steal the patient's identity and manipulate their moves for their motive.

Regardless of the causes of a data breach, the aftereffects of a healthcare breach can be classified into three main categories, which include psychological, social and economic impacts from our observations on various literature reviews:

- Psychological Impact: Mental health professionals have stated that the increasing number of data breaches have taken a toll on the mental health of individuals as their sensitive data has been hacked by bad actors and sold online. Individuals are said to be suffering from various mental health conditions such as depression, anxiety, stress disorders and many more. As the intensity of cyberattacks has been increasing at a profound rate and the attacks are more complex enough to skip over, the security measures have made severe psychological trauma to the individual's level of thinking, feelings and emotions. The cases of data theft to manipulate an individual's identity can result in feeling worried, frustrated, and sad for individuals. The increased number of attacks and breaches have resulted in causing more trust issues for individuals. In extreme cases, these incidents can create chaos in the lives of the individuals, causing severe physical repercussions such as loss of ability to concrete & reason & act accordingly, which would also result in suicides. Even though it's hard to measure the psychological impact, the hidden consequences can tire apart from the life of the victims and cause more damage than physical destruction.

- Social Impacts: Digital health can pose a significant threat - it has become and has made people question the core values of dignity, non-discrimination, and equality because of its constant exposure to cyber-attacks that threatens national security. The inability of a breach to regain the lost information of an individual ultimately would erode a victim's trust in the integrity and reliability of the healthcare system. It would pull them back in further providing necessary information. The loss of faith is not just because of the result of a breach alone but also can trigger them if the information is handed out to third-party vendors without permission and the owner's knowledge. Moreover, overexposure to continuous data breaches in the healthcare sector can be lethal for a nation as misusing sensitive health information can threaten the nation's security. The increased exposure can disclose a country to cyber terrorism and thus further disturb the social and economic balance.

- Economic & Financial Impacts: The data breaches cause substantial financial loss to the organizations/institutions that handle the information. They are mainly unable to recover fully because of the nature of the attack, and healthcare data are imperishable. The financial loss does not just concentrate on the organizational level. It is costly to build more secure servers, and the affected individuals as the information are more likely to make their insurance claims stolen and misused. Results of the Marsh-Microsoft Global Cyber Risk Perception Survey 2017, more than 70 per cent of respondents from the healthcare industry expect that a cyber breach could cost them more than $1 million per case. Apart from financial losses, the impact breaches leave on the nation's residents would be everlasting.

Analysis

Analysis of Laws and Regulations in Data Protection

In the modern society where technology is intertwined with rights the need to inculcate digital rights under privacy is a need of the hour. Data has started to replace the human element in all the resources that we use these days. Therefore data protection, which protects in-dividuals against the misuse of their personal data by data processors, is considered an important element of the Right to Privacy. The surveillance potential of computers initiated the need to include data protection under the right.

Universal Declaration of Human Rights

Data Protection is entitled in Article 12 of United Nations Human Rights Instruments, which is the fundamental Right under the Right to Privacy that safeguards the person's dignity and enables the individual to assert their rights in the face of power imbalances in handling electronic data. As privacy concerns are growing, the General Assembly adopted resolution 68/167 in December 2013, which protects the Right to privacy in the digital age.

The privacy element in data protection is obligatory. The above-said declaration has proved to be an effective mechanism in solving the issues regarding privacy matters and ensures that an individual is dignified in their own space as technology is evolving rapidly globally, regulations on digital privacy matter a lot. Still, the concept of storing and managing non-perishable and highly sensitive dates doesn't even happen to be covered under the digital charters created. This lack of security regulations prevents escalations in healthcare data breaches.

ASEAN Framework on Personal Data Protection

In 2016, ASEAN ministers developed a framework that guides the implementation of data protection measures at both regional and national levels, called the ASEAN Framework on Data Protection. The framework serves to strengthen the personal data in ASEAN and facilitate cooperation among its member states. It fosters regional integration and collaboration and propels to transform ASEAN towards a safe, secure, and digitally-enabled economy. Economies implementing the ASEAN framework have to adopt changes that suit the domestic environment of the country, and this framework doesn't create any legally binding obligations. The ASEAN framework on PDP is considered the most effective and legitimate framework as it is more inclined to the direction of the Universal declaration of human rights - where it thinks the right to privacy as a fundamental right and seeks consent from the individual regarding the usage, collection and disclosure of personal data by providing them with a timeframe upon which the personal data will be used. It is considered more streamlined in the angle of EU GDPR and does indeed provide security patronage. On the other hand, the framework doesn't provide much detailed legal framework that has to be initiated during a data breach. Also, it doesn't cater to sector-specific regulations and the necessary security measures that have to be taken to prevent further escalation of a breach/cyber attack.

Analysis

Law of the Republic of Indonesia on Data Protection

Globalization of information and digital overload placed Indonesia in making a regulation concerning Electronic Information and transactions at the national level for the development of Information Technology to carry out in an optimal, distributive, and widespread manner throughout all levels of society to advance the intellectual life of people. The usage of Information Technology must continuously be developed to foster, maintain, and strengthen the national union and unity under laws and regulations in the national interest. The rapid shift to digital technologies has resulted in hampering society's unity and socio-cultural values; therefore, it is imperative to come up with regulations that cater to the security of citizens in the digital world to prevent misuse.

Indonesia doesn't have a data protection law, however, have specific regulations concerning the use of electronic data (known as "EIT Regulations"):

- Law No. 11 of 2008 on Information and Electronic Transaction as amended with Law No. 19 of 2016 on the Amendment of Law No. 11 of 2008 on Information and Electronic Transaction;
- Government Regulation No.82 of 2012 on Electronic System and Transaction Operation and its implementing legislation, Minister of Communication and Informatics Regulation No.20 of 2016 on Personal Data Protection in an Electronic System;
- Government Regulation No. 71 of 2019 on the Implementation of Electronic System and Transaction.

The above mentioned EIT Regulations apply to those who use electronic information and transactions both in and outside of Indonesia with Indonesian jurisdiction and are detrimental to the interest of Indonesia.

Health Sectoral EIT regulation - protections against the medical records of the patient, is regulated under Law No. 26 of 2009 on Health and Minister of Health Regulation No. 269/Menkes/Per/III.2008 on Medical Records (every person is entitled to the confidentiality of their health conditions that have been disclosed to the healthcare provider). (Personal Data Protection in ASEAN, Zico law, 2020)

The Indonesian regulation on data protection proves to be in accordance with respecting the individual's privacy and is streamlined with the ASEAN framework on PDP. However, the regulation lacks to cater for the domestic needs of protecting electronic data. It seems to be vague to mention that the process of protecting personal data does not speak much on how to tackle a data breach and the measures needed to prevent a breach. The regulation speaks out about the lack of necessary cyber security infrastructure to make cyberspace safe. Even though the health sector remains the most vulnerable to breaches and attacks, it lacks specialized regulation like the banking sector. It only talks about maintaining the confidentiality and does not mention the usage and disclosure of personal data.

According to the Center for Indonesian Policy Studies, cybersecurity laws and regulations in Indonesia remain ineffective in preventing cyberattacks against various sectors, and a comprehensive and overarching regulation is urgently required in Indonesia.

Findings and Implications

The following are the findings based on the literature referred to and the general observations of the situation of the data breach

- The recent increase in the number of data breaches worldwide shows how vulnerable the healthcare sector, in general, is toward a cyber attack. In the rapidly growing digital world, it is impossible to be immune to a data breach as no institution/organization has ever touched a cyberattack; the case is the same in the archipelagic country, Indonesia. Therefore the need to further harness security infrastructure and implement strong regulation is the need of the hour.

- From the international conventions and treaties based on cyber attacks, there is a lack of specific updates in the regulation with the changing times of today's technology. Most of the national laws for data protection worldwide are based on particular articles passed on certain international treaties and conventions. When those articles fail to provide updates to the changing times, it would negatively affect domestic law enforcement. A similar effect is also seen in Indonesia.

- Compared to EU countries, ASEAN countries don't have a strong regulations like EU GDPR, so the vulnerability of ASEAN, especially Indonesia, towards cyber-attacks increases as owning a strong regulation plays a crucial role in cybersecurity. The lack of a proper strong regulation to enforce data protection often downplays the efforts put into tackling the issue in Indonesia. This country is growing rapidly in the 4th industrial revolution. Thus, reducing data breaches is impossible to eliminate without having a strong cyber institution in the healthcare sector.

Findings and Implications

Spanish model of e-health - Role Model to Indonesia's healthcare System

Spain is ranked as the most efficient country globally as per the Bloomberg Health Efficiency Index 2018. The Healthcare sector in Spain is based on the principle that all citizens have the right to health, regardless of their economic and employment situation. The state is responsible for equal implementation. As part of modernizing innovations in healthcare, the government 2006 started its eHealth initiative. The strong regulatory schemes and better quality affordable healthcare services in Spain make it one of Indonesia's best suitable role models. The core regulatory framework to protect digital healthcare data in Spain is the Law on Patient Autonomy and EU GDPR.

Under the regulation GDPR, health data is included in the "special categories of personal data", in which processing of personal data is strictly prohibited. In contrast, it is only allowed under certain circumstances under the individual's consent. Under section 58 of the GDPR, national data protection authorities are given wide investigative and corrective powers to enforce the data protection laws.

Under the Spanish regulation, the Spanish Data Protection Act (SDPA) Law 41/2002 on patient autonomy and the rights and obligations regarding clinical information and documentation (the Law on Patient Autonomy) regulates patients' medical records. It includes relevant provisions in relation to the permitted use, conservation of the documentation, rights of access and custody of said records. The Law on Patient Autonomy establishes a general principle that personal identification data (ID Card, Social Security number) and health data contained in medical records must be separated to safeguard patients' anonymity. This obligation shall only be exempted when patients give their consent or when needed in scientific research, judicial inquiries or relevant public health risk. Under GDPR, violation of the above can bring fines or prison sentences.

The Spanish Data Protection Agency is the national authority to supervise and ensure the data privacy principles and regulations under GDPR. The regulatory framework is strong enough to protect to reduce the intensity of healthcare data during a breach. The special mention of healthcare data under a special law with great emphasis on maintaining the anonymity of the records makes the Spanish model stand unique as the most innovative e-health system in the world.

- ***Under the laws and regulations for healthcare in Indonesia, we could find that only the non-electronic aspect of healthcare is covered. In contrast, no specific law covers digital healthcare, which makes Indonesia more vulnerable to cyber-attacks and breaches in healthcare.***
- ***From the Indonesian law perspective, we could find there is a lack of proper execution of laws and regulations that are meant to protect the confidentiality of the citizens' data where often the data holders get themselves away from undergoing formal investigation, strict punishment/penalties and further mitigation measures resulting in more people being denied their right to justice for a secure and save digital healthcare service.***

Conclusion & Recommendations

Conclusion

The cases of cyberattacks have been more prevalent since the rapid shift of daily activities into digital-based, especially amid the Covid-19 pandemic when the utilization of digital technologies is carried out in various countries to store the citizens' health information data as an attempt to prevent further spread of the virus. However, some challenges appeared, such as data security threats since personal health information is considered more valuable in the black market.

Indonesia seems to be lacking in its cyber security. Still, within two years, the country has witnessed six significant cyber-attacks with two attacks around the healthcare sector which even exposed data of high profile diplomats such as President Joko Widodo; the major security lapse exposed the data of millions of its citizens. The two major data breaches that the country faced in the digital healthcare system was the breach of BPJS & eHAC, both of which play a crucial role in the healthcare service sector of the country. The breach was believed to occur due to a lack of security infrastructure and security awareness.

Indonesia is a growing digital economy with a desire to develop in industry 4.0 and emerge as a manufacturing hub. Still, the ever-increasing concern comes in because the country lacks sector-specific data protection regulations to prevent extreme cases of data exposure. With the vulnerability of healthcare data being imperishable from financial data, the country serves itself as a breeding ground for breaches and attacks that develop growing concern among its citizens. The imperfection and lack of stiffness in law and regulations to curb data breaches result in further consequences such as psychological, social and financial impacts that would seriously dreadful implications to national security and make itself prevalent to cyberterrorism.

Recommendations

- At the international level, international organizations like the UN can bring real-time changes to the already existing regulations meant for data protection further to enhance the need for specific changes to national policies.
- A country like Indonesia with a growing young population can take inspiration from the European Union countries as ASEAN holds an important relationship status with EU countries. Spain, which leads in e-health, can be taken as a potential role model for developing digital health in Indonesia.
- The number of data breaches has increased in Indonesia over the past years. The government is currently undergoing a new preparation of a comprehensive first data protection framework coined as "PDPL Draft", which is yet to be passed by the house of parliament; the law is built following the European Union's GDPR. The new regulation might give a ray of hope to the challenges Indonesia has faced over the past years as the law regulates sensitive personal data that can hamper an individual's privacy. It covers data ownership rights prohibitions on data use and the collection, storage, processing, and transfer of personal data of Indonesian users.
- Adoptions of new digital healthcare systems have to be more favoured and introduced, preventing escalating more breaches in the future. Thus, there has to be increased awareness of providing better security infrastructures for the future development of digital healthcare systems.
- Increasing public-private partnership investment in healthcare security can help safeguard the nation's critical healthcare infrastructure as digital healthcare services often lack the necessary budget to finance their expenditure. Therefore there comes a pressing need to enhance the importance of increased investment in digital healthcare services.

References

Apte, P. (2020). Why is the social impact of cyber security important to business? Verizon. Retrieved 2021, from https://www.verizon.com/business/resources/articles/s/the-social-impact-of-cyber-security-attacks/

ASEAN Telecommunications and Information Technology, "ASEAN Framework on PDP_final"

Basu , M., & Rohaidi, N. (n.d.). Massive cyber attacks hit Asian hospitals, schools and universities. Gov Insider. Retrieved from https://govinsider.asia/innovation/ransomware-attack-asia-wannacry/

Brandon, J. J. (2018). Why ASEAN Needs to Invest More in Cybersecurity. Retrieved 2020, from https://asiafoundation.org/2018/05/09/why-asean-needs-to-invest-more-in-cybersecurity/.

Cahaydi N and Kristyan SA, "Implementation of Digital Protected Health Information in the Healthcare Sector Organization"

CHANDRA, G. R. A. C. E. N. A. D. I. A. (2021). Gov't Launches Investigation After Data of 1.3m Reportedly Leaked From Its Covid-19 Tracking App. Retrieved from https://jakartaglobe.id/tech/govt-launches-investigation-after-data-of-13m-reportedly-leaked-from-its-covid19-tracking-app.

Data protection and security. AEPD. (2020). Retrieved from https://www.aepd.es/en/prensa-y-comunicacion/blog/data-protection-and-security

Georgetown Law Library. (n.d.). Treaties and International Agreements on Privacy & Data Protection. Retrieved from https://guides.ll.georgetown.edu/c.php?g=363530&p=4795565#ECHR%20Case%20Law.

Ghosh, S. (2021). 2 Data Leaks Reported in Indonesia's COVID-19 Tracking Apps. Gov Info Security. Retrieved from https://www.govinfosecurity.com/2-data-leaks-reported-in-indonesias-covid-19-tracking-apps-a-17478

Greig, J. (2021). Passport info and healthcare data leaked from Indonesia's Covid-19 test-and-trace app for travelers. ZDNet. Retrieved 2021, from https://www.zdnet.com/article/passport-info-and-healthcare-data-leaked-from-indonesias-covid-19-test-and-trace-app-for-travellers/.

GSMA, "GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows"

Hadi, S., Candra, S., & Himawan, D. A. (n.d.). ICLG. Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/indonesia.

Harsono, N. (2019). Businesses as risk: Experts sound alarm on cyberthreat . The Jakarta Post. Retrieved 2020, from https://www.thejakartapost.com/news/2019/02/22/businesses-as-risk-experts-sound-alarm-on-cyberthreat.html.

Inforial. (2021). Rising to the cybersecurity challenge in Indonesia's healthcare system T. The Jakarta Post. Retrieved from https://www.thejakartapost.com/adv/2021/06/28/rising-to-the-cybersecurity-challenge-in-indonesias-healthcare-system.html.

Lago, C. (2018). APAC tops the list of cybersecurity incidents. Retrieved 2020, from https://www.cio.com/article/222416/apac-tops-the-list-of-cybersecurity-incidents.html.

Lee, J. (2018). Asean remains 'prime target' for cyberattacks. NIKKEI ASIA. Retrieved 2020, from https://asia.nikkei.com/Business/Business-trends/ASEAN-remains-prime-target-for-cyberattacks.

Platsis , G. (2021). Health Care Data: It's Your Personal 'National Security' Information. Retrieved 2021, from https://securityintelligence.com/articles/health-care-data-personal-national-security/.

Raman J and others, "Holding Healthcare to Ransom-INDUSTRY PERSPECTIVES ON CYBER RISKS"

Ransomware cyber-attack: Who has been hardest hit? (2017). BBC. Retrieved 2020, from https://www.bbc.com/news/world-39919249.

Salma. (2021). Indonesia Has Yet to Pass Personal Data Protection Bill. Universitas Gadjah Mada.

Seh , A. H., Zarour , M., Alenezi , M., Sarkar, A. K., Agrawal , A., Kumar , R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. https://doi.org/https://doi.org/10.3390/healthcare8020133

Sit, D. (2021). The ASEAN Digital Health Landscape: An Overview. Retrieved 2021, from https://research.hktdc.com/en/article/ODU1NDkyNDU0.

Spencer, L. (2021). How Asean is driving global cyber security efforts. Channel Asia. Retrieved 2021, from https://www.channelasia.tech/article/691880/how-asean-driving-global-cybersecurity-efforts/.

Steger, A. (2019). What Happens to Stolen Healthcare Data? Retrieved 2020, from https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

Tan, S., & Azman, N. S. (2019). The Eu Gdpr's impact on Asean data protection law. Financierworldwide. Retrieved 2020, from https://www.financierworldwide.com/the-eu-gdprs-impact-on-asean-data-protection-law#.YjdsU49BxPa.

THE PRESIDENT OF THE REPUBLIC OF INDONESIA, "RUU-ITE_english"

Thomas Paterson (2019) Indonesian cyberspace expansion: a double-edged sword, Journal of Cyber Policy, 4:2, 216-234, DOI: 10.1080/23738871.2019.1627476

Umali, T. (2019). Philippines and Singapore to co-lead the ASEAN Data Protection and Privacy Forum. OpenGov.

What Is Privacy? Privacyinternational. (2017). Retrieved from https://privacyinternational.org/explainer/56/what-privacy

Yu, E. (2021). Asean champions regional efforts in cybersecurity, urges international participation. ZD Net. Retrieved 2020, from https://www.zdnet.com/article/asean-champions-regional-efforts-in-cybersecurity-urges-international-participation/.

CONTACT US

www.ayorecent.com

ASEAN Youth Organization

ASEAN Youth Organization

@ayoasean

AYO Recent Research Center

@ayoasean

AYO RECENT,
ASEAN Youth Organization Research Center
Email: rd@aseanyouth.net
Address: AYO Kreasi Internasional
Arcade Business Center 6-03, North Jakarta, Indonesia.