5-17-AB24A-3046

E- HEALTH PROGRAM AND DATA PRIVACY PROTECTION IN INDONESIA

DR. SINTA DEWI ROSADI[1] AND PROF. EFA LAILA FAKHRIAH

ABSTRACT

Utilisation of ICT for health (e-health) has become a global issue. It is one of WHO's recommendations and is part of the Action Plan for ITU (the International Telecommunications Union) to connect health centres and hospitals to eefectively use information and communication technology. E-health is an ICT-based application related to the health care industry and aims to improve access to and the efficiency, effectiveness, and quality of medical process. Besides the organisation of medical services in hospitals, clinics, health centres, in which medical practitioners, doctors and therapists, laboratories and pharmacies are involved, insurers also involve the patient in medical processes as a consumer. Indonesia is in the early stages of implementing an e-health program, which is due to provide better health services to the community because of the increase in the number of internet users. However, this e-health program may also cause problems regarding how far health providers in Indonesia can protect the privacy of patients' personal data, which can be accessed, managed and disseminated by ICT. Health data is classified as very sensitive data that requires increased legal protection so as not to be misused for commercial purposes.

INTRODUCTION

The development of information technology and the wireless business environment offer considerable advantages in terms of efficiency and productivity (Saad, 2005), particularly in terms of innovations that are changing the landscape of disease prevention and control. The widespread availability of ICT technology, including mobile technology, in many developing countries such as Indonesia is an exceptional opportunity to expand the use of e-health ("ITU Report," n.d.). Indonesia is a developing country, although its economic growth is forecast to accelerate by an average of 5.1 % a year between 2016 and 2020 (The Economist Group, 2016). It nevertheless faces a number of problems and challenges in the field of public health. The development and use of e-health can help create opportunities for solving these problems and challenges in the health sector. Various types of applications can be used, such as the means of recording, reporting and managing outbreaks, electronic prescribing, patient medication management, mobile telemedicine systems, e-psychology, and mobile e-health. The statistics show that the number of internet users in Indonesia in 2016 was 104.2 million people, a figure projected to grow to 144.2 million in 2021 (Statista, 2016). The number of mobile internet users in Indonesia in 2016 was 56.25 million people, which has potential to support an e-health program that uses the internet as the main network for connections. However, the development of ICT also contains potential risks, due to the fact that modern technology provides access in seconds to limitless quantities of personal data. The possibility of creating personality profiles through the combination of different data files and e-health data is an issue that can lead to potential misuse or irresponsible use of the data (Saad, 2005), leading to injury being caused to the data subject. The legal issue here is how far the e-health provider will provide protection and confidentiality of personal medical data stored in their system (Sarabdeen, 2008). The development of the practice in other countries has shown that there have been many cases of violations of personal data that have been detrimental to the patient. For example, in Ohio,

[1] Dr. Sinta Dewi Rosadi, Lecturer, University of Padjadjaran. Efa Laila Fakhriah is a Professor of Law at Faculty of Law in Health Law.

Millford announced that the personal, health and financial information of 8800 patients had been compromised when the health system put all this information into a Web-based software program that was not password-protected. Likewise, Valley View Hospital in Glenwood, Colorado announced that it had suffered a data breach when hackers introduced a virus into the hospital's computer system and took screenshots of 5400 patients' personal records (Elison, 2014).

THEORY

The WHO defines e-health as "the cost-effective and secure use of information and communications technologies in support of health and health-related fields, including health-care services, health surveillance, health literature, and health education, knowledge and research" (WHO Resolution 58/28, 2005). Together with the ITU, (International Telecommunication Union) the WHO will assist developing countries in harnessing e-health and in delivering responsive health systems. To support such systems, the ITU conference has adopted Resolution 78 on Information and Communication Technology Applications and Standards for Improved Access or E-Health. One of the commitments is to establish the Geneva Plan of Action and to promote the collaborative efforts of government, planners, health professionals and other agencies, along with international organisations, to create reliable, timely, high quality and affordable health care and health information systems while simultaneously respecting and protecting citizens' rights to privacy.[2]

Since the legal terms of privacy were first stated by Warren and Brandheis, many legal experts have tried to define privacy rights. According to Greenleaf Graham (2014), privacy is a disputed concept both in law and philosophy and can take many directions. Alan Westin is the first scholar to define this very important concept. According to him, privacy is the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitudes and their behaviour to others. His opinion is often referred to as information privacy or data privacy (Munir, Yasin and Karim, 2014).

However, from an international law perspective, privacy is recognised as one of the fundamental human rights in the Declaration of Human Rights (UDHR) 1948, the International Covenant on Civil and Political Rights (ICCPR) 1966, and by regional instruments such as the European Convention of Human Rights and Fundamental Freedoms (ECHR) 1950, the American Convention on Human Rights 1969, the Cairo Declaration on Islamic Human Rights 1990, and the ASEAN Human Rights Declaration 2012 (Rosadi, 2015). In e-health programs, the key component of data privacy is how far the user can control the data that is collected, managed and distributed by the provider.

DISCUSSION

The Data Privacy Regime in a Global Context

The relationship between privacy with data privacy has not always been easy to reconcile, and data protection is often viewed as a technical term relating to specific information management practices. This is in contrast with privacy, which is considered as a fundamental human right (Munir and Yasin, 2002). Graham (2014, p. 5) states that privacy is a disputed concept in both law and philosophy which can take many directions. However, experts are now using the terminology of data privacy, which is perceived as a set of minimum data protection principles that have been accepted internationally, along with additional principles enshrined in national law (Graham, 2014, p.5). At least 102 countries with data privacy laws have adopted international data principles such as:

1. Fair and lawful use;

2. Use for limited, specifically stated purposes. Personal data will be used only for one or more specified and lawful purposes, and will not be further processed in any manner incompatible with that purpose or those purposes;
3. Use in a way that is adequate, relevant, and not excessive. Personal data will be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Accuracy. Personal data will be accurate and, where necessary, kept up to date;
5. Data to be kept no longer than is absolutely necessary. Personal data processed for any purpose or purposes will not be kept for longer than is necessary for that purpose or those purposes;
6. Data will be handled according to data protection rights. Personal data will be processed in accordance with the rights of data subjects;
7. Data will be kept safe and secure. Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage, to, personal data; and
8. Data will not be transferred outside a territory without adequate protection.

Protection of Users in E-health Programs

In the New Information era, when the principal commodity is information, databases of personal medical information have enormous commercial value and need appropriate legal protection, as Paul Hynes notes (quoted in Saad, 2005). Personal information databases, such as customer databases, have commercial value where it has been utilised to deliver customised marketing information to individuals based on profiling (Saad, 2005 p. 5). The OECD (Organization for Economic Co-operation and Development) released a report in 2010 which focused on the challenges to health care efficiency. It stressed the need for a legal framework allowing the sharing of health information between healthcare professionals within and across healthcare organisations, as well as across boundaries, without conflicting with the need for privacy protection of the patient (WHO, 2012).

In e-health programs where the medical profession in providing the services, there will be a potential of affecting privacy right of the patients, for example (Waldo, 2007):

1. The use of electronic health information can allow providers to collect and share patient information;
2. More people have access to patient information, including medical caregivers, researchers, and healthcare administrators;
3. Patient information is more easily accessible because it is increasingly stored in digital form and can be transmitted more easily than in paper form;
4. Patient information is held for a long time, and the longer it remains in existence the greater the opportunities for abuse; and
5. Patient information, such as DNA information, that has relevance to individuals relating to parents, siblings, or future offspring is a potential violation of medical privacy.

Patient Perspectives on Privacy

Many developed countries like the United States, the United Kingdom and Australia have specific laws on medical data privacy. They place importance on the concept of informed consent, and thus healthcare providers are required to provide privacy-relevant information to patients about how their personal health information will be used (Waldo, 2007, p. 224) and the principles adopted by the medical industry in the form of a code of conduct. For example:

Privacy consent and notifications

Privacy consent and notification requires written privacy consent for the processing of sensitive data and allows data processing only within the limits of a general authorisation issued by the data protection authority.

Data controller, processor and sub-processor

The role of the entities involved in the handling of collected data cannot be left to the discretion of the parties, and the data protection authorities are strict in defining these roles. In particular, hospitals are generally considered to be the sole data controllers, with sponsors acting as data processors and cloud platform providers acting as sub-processors. Sponsors will usually need to be qualified as data controllers to have a higher level of discretion in the processing of the data, but data protection authorities have challenged such qualifications in several instances.

Processing of biometric data

The use of remote patient monitoring systems may require notification to the data protection authority. This requirement will apply if technologies are used either to create user profiles (which might include a profile of the user's physical features) or to collect biometric data. Biometric data includes any data obtained about a person's physical or behavioural features (e.g., fingerprints, facial characteristics, hand geometry, and retina and iris scans). The data protection authority has issued stringent requirements regarding the modalities of biometric data collection, the security measures to be implemented for data storage, and the maximum term of storage.

The purpose of data processing

A common mistake made by medical device companies is to assume that once a patient's data has been collected, it may be used for any purpose and belongs to the company. This is not the case, and privacy consent – specific to the purpose for which the data will be processed – must be obtained from the patient. Except in limited circumstances, therefore, which will be assessed on a case-by-case basis, personal data collected as part of medical treatment cannot subsequently be used in the performance of a clinical trial without additional consent from the relevant patients. This requirement does not apply if the collected data is then aggregated and anonymised. However, in this case, the use of an identification code will not suffice if it is possible to connect a patient to the relevant code.

Transfer of data outside the European Union

Data transfers outside the European Union can be the most challenging part of assessing legal implications, since it is necessary to know the role and location of all parties involved, as well as which servers are used to manage the platforms, distinguishing between hospitals, sponsors and cloud platform providers. Based on the information collected, the usual solution is to implement *ad hoc* model clauses approved by the European Commission, but these must be tailored to the peculiarities of the case. For instance, a relevant issue is to ascertain whether the data processor that appoints the sub-processor is a European or non-European entity.

Potential liabilities

The potential privacy risks cannot be underestimated, given the fines for breach of privacy regulations prescribed by most EU countries and the criminal penalties that some countries – including Italy – impose for some breaches (e.g., if the breach has been performed to gain profit or causes damage). These penalties are expected to increase considerably as a consequence of the potential implementation of the new EU Privacy Regulations and should therefore be taken into account in the development of new technologies.

The Concept of Privacy in Indonesia

In discussing the concept of privacy in Indonesia, it is important to note the cultural context, since privacy as a concept originated in western culture (Graham, 2014, p. 12-13). In Indonesia, the cultural community is considered to be more important than in western society, where respect and status are obtained by individuals. In contrast, in communal societies, emphasis is placed on community, collaboration, mutual interest, harmony, tradition, mutual goodness, respectfulness, and the avoidance of embarrassment. Specifically, in Indonesia, the important collectivist values include familial relationships, mutual help, courtesy to guests, and respect

towards parents, teachers and lecturers (by avoiding debating with them). Individualist culture emphasises individual rights, responsibility, privacy, expressing personal opinion, freedom, innovation and self-expression. Since the reformation era in Indonesia, when democracy and the rule of law became the country's vision, privacy has become an important legal concept, especially after the constitution was amended and the international instrument of human rights was adopted. Data privacy has since emerged as an issue of concern in Indonesia. Privacy is perceived as a basic fundamental human right, as stated in Article 28(G):

> "Each person shall have the right to protection of their personal selves, families, respect, dignity and possessions under their control and shall have the right to security and protection from threat of fear of doing or of not doing something which constitutes a human right."

The constitution does not explicitly mention data privacy. It only strongly recommends protecting human rights research, as discussed by Palupy (2011). Based on this article, however, Indonesian legal experts always apply Article 28(G) as a legal basis for privacy protection in Indonesia. Like many ASEAN countries, Indonesia sees international law as an important source for its domestic law, so there tends to be a process of horizontal or comparative importation of international human rights standards through the domestic law of ASEAN countries (Graham, 2014, p.17).

Another significant factor in recognising the issue of privacy in Indonesia is the increasing number of internet users, which made a legal instrument for e-commerce protection necessary. In 2008, therefore, Indonesia enacted an Information and Electronic Transaction Law, using the term data privacy.

The E-Health Program in Indonesia and Their Impact on Data Privacy Regulation

Despite the commitments made to the WHO, the implementation of e-commerce is still at a minimum. Currently, the e-health program is only developing e-health in six pilot project hospitals, mostly in the capital city: the Cipto Mangunkusumo Hospital, the Friendship Hospital, the Maternal and Child Hospital, the Harapan Kita Heart Hospital, the Fatmawati Hospital and the Cancer Hospital Dharmais. Technically, the system is expected to be integrated in all hospitals in Indonesia. The Indonesian health system has been comprehensively addressed in Law Number 36, 2009. This act attempted to deal with overall healthcare in Indonesia. Its purpose was to provide better health services for the Indonesian people. Data privacy is also protected in this law in Article 57, Paragraph (1), which recognises the right of everyone with regards to the confidentiality of their personal health conditions as presented to healthcare providers. Article 57, Paragraph (2) deals with exemptions in terms of personal health confidentiality, which does not apply in the case of (1) authorisation by the law, (2) a court order, (3) the public interest, or (4) the interests of the person. Unfortunately, this law is not strong enough to protect data privacy. Due to the various community concerns over how far data privacy will be protected in Indonesia, the Indonesian government under the lead of the Ministry of Infocom tried to draft a Data Privacy Bill in 2015. This Bill is still under discussion. The Bill is intended to regulate the collection, processing and dissemination of personal data by the government, businesses or individuals. The proposed Bill also intends to give more protection for the e-health program, since medical data will be catogorised as sensitive data and will need more explicit and stricter protection than general data. Like other Asean countries such as Malaysia, Singapore and the Philippines, the draft Bill also adopts the international principles known as the international common standard by combining the OECD Guidelines, European Convention of Personal Data Protection and General Data Protection Regulations.

CONCLUSION

Indonesia is in the early stages of implementing an e-health program, which is due to provide better health services to the community because of the increase in the number of internet users. However, the e-health program may also cause problems regarding how far health providers in Indonesia can protect the privacy of their patients' personal data, which can be accessed, managed and disseminated by ICT. Health data is classified as very sensitive data that requires more legal protection so as not to be misused for commercial purposes. In addressing this issue, the Indonesian government has provided legal protection for medical data privacy under the Health Law, but it still cannot provide the maximum level of protection, because the regulation only comprises of one article. Indonesia thus needs a specific regulation in data privacy. In responding to the various concerns of the community, the Government of Indonesia is in the process of drafting a Data Privacy Bill that will adopt a comprehensive model that will apply to government agencies, businesses and individuals for the collection, processing and dissemination of personal data. The bill also will protect medical data privacy records as sensitive data that needs stricter protection than general data.

REFERENCES

Elison, A. (2014) 10 Recent Healthcare Data Breaches [Online]. Available from: http://www.beckershospitalreview.com/healthcare-information-technology/10-recent-healthcare-data-breaches.html [Accesed 12 August 2016].

Graham, G. (2014) *Asian Data Privacy Laws, Trade and Human Rights Perspectives*. Oxford, UK: Oxford University Press.

ITU Report. (n.d.) [Online]. Available from: http://www.itu.int/en/ITU-D/ICT- Application /eHEALTH/ [Accessed 15 September 2016].

Munir, A.B., Yasin, S.H.M. and Karim, M.E. (2014) *Data Protection Law in Asia*. Hong Kong: Thomson Reuteurs Hongkong Limited.

Munir, A.B., Yasin, S. and Hajar, M. (2002) *Privacy & Data Protection*. Malaysia: Sweet & Maxwell Asia.

Palupy, H.E. (2011) *Privacy and Data Protection: Indonesia Legal Framework*. MA in Law and Technology, Tilburg University.

Rosadi, S.D. (2015) *Legal Aspect of Data Privacy from International, Regional and National Law Perspectives*. Bandung: Refika Aditama.

Saad, A.R. (2005) *Personal Data and Privacy Protection*. Singapore: Lexis Nexis.

Sarabdeen, J. and Ishak, M. (2008) E-health Data Privacy : How Far It Is Protected. Communications of the IBIMA, 1, 110-117.

Statista. (2016) Number of Instagram users in the United States from 2015 to 2020 (in millions) [Online]. Available from: http://www.statista.com/statistics/293771/number-of-us-instagram-users/ [Accessed 10 July 2016].

The Economist Group. (2016) Indonesia Economic Report [Online]. Available from: http://country.eiu.com/Indonesia [Accessed 01 September 2016].

Waldo, J. (2007) *Enganging Privacy And Information Technology In A Digital Age*. United States of America: The National Academy of Science.

World Health Organisation (WHO) (2012) Legal Frameworks for E-Health. Geneva: WHO Press.

WHO E-Health Resolution 58/28. (2005).