Security Value Issues on eHealth Implementation in Indonesia

P K Sari1*, P W Handayani2, A N Hidayanto3
1,2,3Faculty of Computer Science, Universitas Indonesia, Depok, Indonesia

Email : *puspita.kencana91@ui.ac.id

Abstract. eHealth is an information technology solution for improving healthcare to be more effective and efficient. eHealth innovations not only give expected benefits but also new problems, one of them is security value issues. This inquiry has purpose to identify problems of security-related value in eHealth implementation in Indonesia involving its stakeholders. We use constructivism as research paradigm with qualitative method. Data was collected through focus group discussion with five information security experts from State Cyber and Code Agency that work on security controls in healthcare sector. Data analysis using thematic coding with Atlas.ti as tool. This research explored some security value issues on eHealth implementation in Indonesia, including regulator value conflict, data integrity and reliability, and data privacy and confidentiality. Some of those problems are caused by specific regulation about information security for healthcare in Indonesia is not available yet that makes some value conflict among stakeholders involved in this sector. Some implications are also proposed, both practically and theoretically.

1. Introduction
Health is a basic human right that must be protected. However, providing health care services requires significant resources that should be well managed. Health information system, also known as eHealth, is one of the information technology solutions in the health sector to support more effective and efficient services. eHealth applications have some variances that can be used by health organization as management information system and by individual or patient to monitor his/her personal health condition independently. One of eHealth application is Health Information Technology (HIT), which includes Clinical Information System (CIS) and medical devices [1], which are used for the provision of health services in clinical environments such as hospitals, clinics, and other health centers. CIS used in hospitals is often referred as Hospital Information System (HIS). However, eHealth innovations not only provide benefits but also bring new problems, one of which is security value issues in protecting health data.

The main entities in the health care system are service providers, namely doctors and other medical professional, and service recipients, namely patients. Medical professional has code of ethics that should protect patient's data privacy; thus, data protection is part of professional value. Another health entity that can access health data is the payer such as health insurance institution or patient employer. If someone has health care coverage, then he is willing to exchange the privacy of his health data for financial gain [2]. eHealth makes those data is more open. Health data that initially only flowed between those entities, can also be accessed easily by other parties, such as eHealth service providers. In fact, not all those providers are part of health entities that carry the same value. This allows different values emerging from each party involved, even affecting the value of medical professional, that can cause some issues in the provision of health services through eHealth implementation.
In Indonesia, cyber-attack on the health industry occurred in mid-2017 where two large hospitals were attacked by the WannyCry Ransomware. As a result of this attack, health workers were unable to access related information so some surgical procedures could not be performed and endangered the patient. Other security incidents in the health sector are web defacement cases belonging to several health organizations, including health facilities. This case does not really have a significant impact on health organizations because the web pages that are defaced are mostly not on the main page. Usually pages that are attacked are web pages that are rarely accessed. However, this shows that there is a vulnerability in the system owned by health organizations so that good information security is needed so as not to provide greater risk.

Previous studies revealed some security value issues associated with the implementation of eHealth. Study from Laric et. Al [2] described issue related to the privacy and confidentiality of health data that occur due to the expansion of the network of health service providers that encourage information sharing with many stakeholders. Research by Sulmasy et. Al [3] described some problems in doctors-patients relationship who experience a shift in values and ethics due to eHealth usage. This issue is relevant with studies by Layman [4] and Ozair et. al[5] which explain some major challenges for health care providers in implementing Electronic Health Records (EHR), including the accuracy and reliability of data stored in the electronic system thereby causing loss of patient confidence and risk of patient safety. The term EHR is often used interchangeably with EMR, refers to an electronic form of medical record that stores patient medical data in detail, including history, physical examination, investigation and treatment [4]. On its development, EHR also added by information of billing for care, administrative, and regulatory costs [2] that can be used for the health care treatment, as well as for research, education, and public health review [6]. Thus, EHR becomes very attractive to people and organizations outside the health services field [1]. EHR usage also creates ethical dilemmas related to the ownership of personal health information (PHI) and the responsibilities of medical personnel and health service providers to maintain the confidentiality and privacy of PHI [7]. Meanwhile, a study by Karcher & Presser [8] discussed some issues in data security, privacy, boundary challenges and practices that occur across jurisdictional areas related to mHealth applications. The use of telehealth/telemedicine to share health information remotely also raises concerns related to trust and ethical practices such as competence, financial benefits, transparency, and informed consent, privacy and confidentiality, and continuity of care [9].

From previous studies, there are some security issues that should be considered in the development of eHealth that have been summarized in Table 1. However, we have not found any inquiry about ethical and security value issues related to eHealth implementation in Indonesia. In addition, only few studies had used empirical methods to describe security value problems. One of them is research by Laric et al [2]. Therefore, this study aims to identify any issues related to values and ethics in the development of eHealth in Indonesia, specifically in health data protection, using empirical methods.

| Issues                                      | eHealth application                                      | Literature |
|---------------------------------------------|----------------------------------------------------------|------------|
| Data privacy and confidentiality           | CIS, medical device, EHR, Telehealth/telemedicine, mHealth | [2, 7–9]   |
| Ownership of PHI                           | EHR (especially for PHI)                                 | [7]        |
| Doctor-patient relationship                 | HIT (especially CIS), telehealth/telemedicine             | [3, 9]     |
| Data integrity and reliability             | EHR                                                      | [4, 5]     |
| Technical and medical competencies         | Telehealth/telemedicine, mHealth                         | [8, 9]     |

2. Research Method
The method used in this study is a qualitative method with an empirical approach. Data collection is carried out through focus group discussions so that it can be immediately clarified by relevant parties as a form of data validity test. Data analysis process uses thematic coding with six stages namely (i)
preparing data for analysis; (ii) categorizing themes; (iii) coding data; (iv) using the coding results for the description; (v) grouping based on themes; and (vi) interpretation [10]. Themes are categorized based on security value issues from previous studies which have been summarized in Table 1. However, this study only focuses on protecting health data in the eHealth system in health facilities so that the themes used are data confidentiality and privacy (coded as RP), and integrity and eligibility data (coded as IK). This study also did not rule out the possibility of a new theme that emerged because it had never been discussed in previous studies but became an important issue according to the interviewees. Data collected in the form of transcripts from the results of focus group discussions are then entered into the ATLAS.ti 8 tool to be analyzed. The discussion involved five experts in the field of information security, especially in the health sector from the State Cyber and Code Agency (known as BSSN).

3. Results and Discussion

Security value issues in the use of eHealth can occur because of differences in values held by the stakeholders in the provision of healthcare services. From the results of data analysis using thematic coding, there are three value problems related to the implementation of eHealth in Indonesia. Summary of those issues can be seen in Table 2.

| Table 2. Summary of security value issues on eHealth implementation |
|--------------------------|-------------------------------------------------|------------|
| **Issues**               | **Sub-issues**                                  | **Code**   |
| Interest as regulator    | Regulator for security in healthcare sector is not obvious | KR-1       |
|                         | District hospital regulated by each district health agency | KR-2       |
|                         | Private hospitals comply with other country’s regulation | KR-3       |
|                         | Information security is not a priority for healthcare facilities | KR-4       |
| Data integrity and reliability | The authority over eHealth is unclear | IK-1       |
|                         | Data integrity on HIS is often ignored | IK-2       |
|                         | Difficulties in managing HIS | IK-3       |
| Data privacy and confidentiality | Data protection regulation is not established yet | KP-1       |
|                         | eHealth system is managed by vendor | KP-2       |
|                         | eHealth vendor is not certified in information security | KP-3       |
|                         | Data abuse risk | KP-4       |
|                         | Perception bias on data security and privacy | KP-5       |

3.1. Interest as regulator issue

In the health sector, there are several stakeholders acting as regulators, such as the Ministry of Health at the central level and the Regional Government (Health Agency) at the regional level. This is explained by the interviewee as follows.

“Regulation issued by the Ministry of Health is not directly referred to by all hospitals because there are regional authorities as regulators for hospitals in the regions. There is no clear sector regulatory and supervisory agency for the health sector.” (Code: KR-1)

"For hospitals in the national category, the main regulator is the Ministry of Health, while the district hospital is regulated by Health Agency of each district"(Code: KR-2)

This can lead to problems where the values carried by the two parties may be different or even conflicting. There are differences in regulations referred to also occur between government hospitals and private hospitals.

"Private hospitals are already relatively good. This may be due to the supervision of external parties such as independent auditors. In addition, the presence of foreign citizens as patients also causes
private hospitals to be more concerned about security issues due to the existence of global regulations such as GDPR” (Code: KR-3).

Different conditions occur in primary health center where awareness for the protection of health data is still very weak.

"Since there is no mandatory parent regulation, information security has not been a priority in the primary health center. Furthermore, mostly eHealth applications are developed by the Health Agency, so they only become operators for data input. There is no specific structure dealing with information security "(Code: KR-4).

3.2. Data integrity and reliability issue

The interviewees explained that there was a problem in the regulation of health care services, such as operational permits for medical devices.

“Most health services rely heavily on National health insurance agency (known as BPJS). Likewise, the Food and Medicine Agency and Ministry of Communication and Information that regulates operational licenses for medical devices.”(Code: IK-1)

Lack of data validity in the hospital information system due to the overly dominant role of BPJS in the healthcare service system.

"Health data owned by BPJS is more complete than data held by Ministry of Health. HIS developed by hospital supposed to be integrated with BPJS system where the data flows from HIS to BPJS system. To claim medical expenses, the data in BPJS system must be complete while not all data in HIS is mandatory". (Code: IK-2)

National health insurance system demands hospital and primary health center to provide complete information about the patient health care treatment who are guaranteed. Therefore, BPJS developed specific information system to collect the health data required.

"The hospital does not have the ability to update the HIS because it is managed by third party/vendor. When the BPJS system updates and is out of sync with the HIS used, the consequences will be to hamper services to patients. The solution taken by hospital is the HIS is bypassed and directly input into the BPJS system”. (Code: IK-3)

3.3. Data privacy and confidentiality issue

The next issue concerns about the confidentiality and privacy of health data. No specific regulations on personal data protection or health data in Indonesia becoming one of the causes.

"Patient data are vulnerable because there is no regulation for the protection of these data. Most of the health services do not have policies to implement patient data protection (including medical records). Although in the Health Act it has been stated that if personal data needs to be protected, the derivatives do not yet know what the mechanism is like”. (Code: KP-1)

Lack of financial allocations and human resource capabilities for the development and maintenance of information systems, making many health service facilities using third parties to manage their information systems.
"Most patient data (medical records) are in the HIS application, whereas the HIS is fully managed by a third party. This means that all data is submitted to third parties. There is no specific protection against the data." (Code: KP-2)

Health data management carried out by a third party without any guarantee that the provider has protected data confidentiality and privacy. Irresponsible providers can use the data for things that should not, such as giving the data to other parties who are not entitled for economic reasons. In another side, health facilities hand over the storage and management of health data to third parties because of limited resources, both financial and human.

"Nobody has ever done a security assessment to the provider. The provider also has not been certified information security. In the Information Security Management System regulation, all providers must be registered and certified by security agency. Some providers are already registered but do not know whether they are certified or not." (Code: KP-3)

Interviewee added that the absence of specific regulations for the protection of the safety of health data also increases this risk.

"From the results of the risk assessment conducted by BSSN, the highest risk is in privacy data, such as misuse of internal data or patient data." (Code: KP-4)

Although there is no specific protection mechanism for health data, but not many incidents of violation of the confidentiality and privacy of health data are reported. This could be due to biased values regarding privacy and confidentiality of data held by individuals (patients) or health care facilities. The interviewee explained this as one of the causes in the issue of the confidentiality of health data.

"The lack of security incident reporting could have been caused by a perception bias related to privacy in Indonesia. For example, data such as personal identity card photos are still easy to find on the Internet. In fact, there could have been incidents of violations of the privacy of health data, but they were not considered as incidents, so they were not reported”. (Code: KP-5).

3.4. Discussion and Implications
The results of data analysis with thematic coding using the Atlas.ti tool can be visualized with a network diagram as shown in Figure 1. Those three value problems discussed in this study are related to each other. First, the blue ones are issues related to interests as a regulator that has four sub-topics with the main issue being the absence of a single regulator for health care sector (code: KR-1). This issue is not found in previous studies. It causes different references in the application of eHealth, specifically related to data security, in various health facilities. District hospital refers more to the policies of the local Health State Agency (code: KR-2), while private hospital also complies to regulations from other countries that can be binding as a reference, such as GDPR from the European Union (KR-3). This issue is related with legal requirement of eHealth application, especially for EHR as discussed by Sittig & Singh [7]. Different conditions were also found in medical health center which did not prioritize data protection (code: KR-4). However, the selection of health care sector regulator, especially for eHealth implementation, must consider the interests of many parties and apply to all conditions.
Second, the issues related to data integrity and reliability with major issue is the unclear authority over the implementation of eHealth (code: IK-1). One of sub-topic is about information system usage from national health insurance (BPJS) that was not integrated and prioritized over the HIS (code: IK-2). Therefore, data on HIS became incomplete and unreliable for patient care. Previous studies \[4, 5\] also concerned about data accuracy and reliability in EHR. Another problem is the limited ability to manage eHealth systems by health facilities (code: IK-3) that make the system to be often ignored. The determination of the authority to implement eHealth is related to the absence of a single regulator in the health sector, so the solutions must also consider to the first problem.

The last, data confidentiality and privacy issue with the main topic is regulation related to health data protection that have not been established in Indonesia (code: KP-1). This causes the risk of misuse of health data (code: KP-4) and bias perceptions about data privacy and confidentiality (code: KP-5). The absence of such regulation also results in the absence of referrals for health facilities in handing over the management of the eHealth system to third parties (code: KP-2). Most of eHealth vendor does not certified in information security yet (code: KP-3), so that they cannot provide guarantees for the confidentiality and privacy of data. These problems are related to the other problems. Therefore, the solutions provided must also be interrelated and consider the interest of stakeholders. The more parties involved, the greater the potential for ethical and value conflicts \[2\]. These problems occur if there are stakeholders or entities in the health ecosystem that use health data not with their proper values.

This research offers some implications. Theoretically, this study revealed security value issues that have not been discussed in previous studies, which is about conflict of interest as regulator in health care sector. Several parties act as regulator in the healthcare sector result in value issues related to eHealth systems management in healthcare facilities. This study enriches empirical studies related to security values and ethics issues in the eHealth system which is still rare. Practically, this study give lesson learned for the government to determine the policies required for eHealth implementation in Indonesia. The main regulator establishment must consider the interests of various parties involved in the national health ecosystem including from information technology sector. It is expected to reduce the conflict of values in the implementation of eHealth in Indonesia.
4. Conclusion
There are some of the value issues in the implementation of eHealth in Indonesia. Many stakeholders are involved in the national health ecosystem poses complex issues in the protection of health data. The first problem is related to the importance of regulators. The second problem is related to the data integrity and feasibility issues caused by unclear authority from certain parties. The last value issue is related to data confidentiality and privacy. This is result in the absence of specific regulations related to health data. Limited resources and bias towards the value of privacy itself are also the cause of the problem. This study has several limitations. First, the participants in this study only involved one stakeholder in the health industry ecosystem. This study is the initial stage of research to be conducted regarding information security culture in the health sector. For further study, it will involve other stakeholders from hospitals, health care facilities, eHealth service providers, and related regulators. Second, the discussion is still dominated by one type of eHealth namely the Clinical Information System used in hospitals and primary health centers. The existence of security value issues from other types of eHealth has not been discussed in depth. Future studies may be able to discuss more deeply on other eHealth applications such as telehealth/telemedicine and mHealth. Both types of eHealth are currently developing so that they have potential value conflict that may not have been resolved before.

Acknowledgement
This article gets valuable input for improvement from Dr. Embun Kenyowati Ekosiwi S.S., M.Hum. and Dr. A. Harsawibawa M.Hum.

References
[1] Handayani, P. W., Hidayanto, A. N., & Budi, I. 2018. User acceptance factors of hospital information systems and related technologies: Systematic review. Informatics for Health and Social Care, 43(4), pp. 401-426.
[2] Laric, M. V., Pitta, D. A., & Katsanis, L. P. 2009. Consumer concerns for healthcare information privacy: a comparison of US and Canadian perspectives. Research in Healthcare Financial Management, 12(1), pp. 93.
[3] Sulmasy, L. S., López, A. M., Horwitch, C. A., & American College of Physicians Ethics, Professionalism and Human Rights Committee. 2017. Ethical implications of the electronic health record: in the service of the patient. Journal of general internal medicine, 32(8), pp. 935-939.
[4] Layman, E. J. 2008. Ethical issues and the electronic health record. The health care manager, 27(2), pp. 165-176.
[5] Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. 2015. Ethical issues in electronic health records: A general overview. Perspectives in clinical research, 6(2), pp. 73.
[6] Komesaroff, P. A., & Kerridge, I. 2018. The My Health Record debate: ethical and cultural issues. Internal medicine journal, 48(11), pp. 1291-1293.
[7] Sittig, D. F., & Singh, H. 2011. Legal, ethical, and financial dilemmas in electronic health record adoption and use. Pediatrics, 127(4), pp. e1042-e1047.
[8] Karcher, N. R., & Presser, N. R. 2018. Ethical and legal issues addressing the use of mobile health (mHealth) as an adjunct to psychotherapy. Ethics & Behavior, 28(1), pp. 1-22.
[9] Chaet, D., Clearfield, R., Sabin, J. E., & Skimming, K. 2017. Ethical practice in Telehealth and Telemedicine. Journal of general internal medicine, 32(10), pp. 1136-1140.
[10] Hassan, N. H., Maarop, N., Ismail, Z., & Abidin, W. Z. 2017, July. Information security culture in health informatics environment: A qualitative approach. In 2017 International Conference on Research and Innovation in Information Systems (ICRIIS) (pp. 1-6). IEEE.