Reliability and Security in the Implementation of Digital Health Service Application with the Application of "Reliability Certification or Electronic Certification" based on Indonesian Law

Charles Amirul Hanif[*], Muhamad Amirulloh[**], Helitha Novianty Muchtar[***]

DOI: https://doi.org/10.22304/pjih.v8n3.a6

Submitted: July 28, 2021 | Accepted: November 21, 2021

Abstract

Societies are always changing rapidly. Initially, societies recognize ordinary health services. Now, people acknowledge web application based digital health services. This rapid change raises potential problems such as the sale of illegal drugs, user data theft, and illegal health workers. Unfortunately, the government has not provided actions to respond the issues quickly. There is no law that underlies the implementation of web application. It increases the possibility of other potential problems. Therefore, it is necessary to question the reliability and security of the implementation of the application and the form of legal responsibility of the organizer. This study used a normative juridical method, which is carried out by examining secondary data as the main study material. The study reveals that the reliability and security in the implementation of applications both as an electronic system and as a health service facility can still be optimized. There are two forms of legal responsibility for the application operator, namely liability in the form of obligations and in the form of sanctions.

Keywords: electronic certificate, health service applications, reliability certificate.

A. Introduction

The Preamble to the 1945 Constitution mentions the purposes of the establishment of the Republic of Indonesia. One of them is to promote public welfare. To achieve the general welfare, economic development cannot be carried out separately from the development of Human Resources. The benchmark for human resource development is not based on per capita income but the Human Development Index (HDI) or the HR quality index. The HDI index is measured according to three main components that include education, health, and the economy.[1] The component to be prioritized is health. Health greatly affects humans

[*] Student of the Faculty of the Law, Universitas Padjadjaran, Jl. Dipatiukur No. 35, Bandung, charles16001@mail.unpad.ac.id.

[**] Lecturer of the Faculty of the Law, Universitas Padjadjaran, Jl. Dipatiukur No. 35, Bandung, muhamad.amirulloh@unpad.ac.id, S.H., M.H., Dr. (Universitas Padjadjaran).

[***] Lecturer of the Faculty of the Law, Universitas Padjadjaran, Jl. Dipatiukur No. 35, Bandung, helitha.novianty@unpad.ac.id, S.H., M.H.

[1] Soekidjo Notoatmodjo, "Kesehatan dan Pembangunan Sumber Daya Manusia", *Jurnal Kesehatan Masyarakat Nasional*, Vol. 2, No. 5, 2008, p. 196.

in daily activities. Health also affects humans' education and productivity to live economically.[2]

Rapid development of Information and Communication Technology (ICT), has affected many fields in people's lives, including the health sector. Military and research are the two fields that initiate the use of Internet leading to the advancement of ICT. In the development, other fields also exposed the ICT resulting the common terms of electronic commerce, electronic government, electronic banking, and electronic health.[3] E-health is a big potential for the government in managing a digital-based health service system, both related to reporting and recording as well as a digital health service system, the telemedicine. The telemedicine is derived from the word *tele* in Greek, meaning *far, at a distance*. Telemedicine can be defined as medical services for patients separated by distance.[4]

Before the appearance of telemedicine, every health service practice was carried out by conducting face-to-face examinations. Health workers faced patients directly. The telemedicine has made it possible to provide health services digitally. This service is carried out through an application. There are some companies providing health service applications in Indonesia. They are, among others,

1) Halodoc;
2) Alodokter;
3) Doctor.id;
4) Clickdoctor;
5) MedikaApp; and
6) Homecare24.[5]

Apart from the advancement of ICT, the health sector is also developing even more due to the Corona Virus Disease 19 (Covid-19). The disease, which has a high transmission rate, requires people to live in a new normal order of life. The new order makes people more limited in social activities. They are prohibited to visit crowded places, such as hospitals or other health facilities. The Covid-19 has made people using telemedicine, instead of face-to-face health care practices.

Covid-19 is the biggest factor that makes *telehealth* or telemedicine more popular. During the pandemic outbreak, the use of MHAs and MAs and telemedical solutions has greatly increased. The use of these digital technologies to set up virtual clinics, telemedical consultations, remote interpreting of data and virtual

---

[2] Anggie Septie Aningrum AN (et al.), "Analisis Penerapan Etika dan Hukum Kesehatan pada Pemberian Pelayanan Kesehatan di Rumah Sakit Nene Mallomo Kabupaten Sidenreng Rappang", *Jurnal Ilmiah Manusia dan Kesehatan*, Vol. 1, No. 3, 2018, p. 190.

[3] Muhamad Amirulloh, *Hukum Teknologi Informasi dan Komunikasi (TIK) sebagai Hukum Positif di Indonesia dalam Perkembangan Masyarakat Global*, Bandung: Unpad Press, 2016, pp. 3-4.

[4] Soegijardjo Soegijoko, *Perkembangan Terkini Telemedika dan E-Health Serta Prospek Aplikasinya di Indonesia*, Yogyakarta: Fakultas Teknologi Industri Universitas Islam Indonesia (TI FTI UII), 2010, p. 4.

[5] Devina Martha Listianingrum (et al.), "Perlindungan Hukum terhadap Konsumen dalam Pelayanan Kesehatan Berbasis Aplikasi Online", *Diponegoro Law Journal,* Vol. 8, No. 3, 2019, p. 1890.

education platforms is ideal for continuing medical care during the curfews and shortage of specialized workforce.[6] The rapid increase in the number of users of digital health service applications indicates that the e-health field is growing very rapidly. These developments provide opportunities for start-up companies because it opens new markets to create quality applications. On the other hand, it poses challenges to the community and government because it has the potential to cause problems. These problems may include the sale of medicines that are not registered to the Food and Drug Supervisory Agency (BPOM –*Badan Pengawas Obat dan Makanan*), leakage or theft of personal data and violation on user privacy, as well as the practice of unlicensed health workers.

The implementation of digital health service applications poses potential problems because the changes are so fast and significant. People initially have more conventional or face-to-face health services before they have turned into digital health services using applications. This condition occurred at the same time as the government was slowly responding to the issue of changes. It gives rise to a condition with no legislation that specifically underlies the implementation of the digital health service application. The implementation of digital health service applications that are not based on specific laws and regulations increase the possibility of the potential problems. These potential problems are rarely found in conventional health service delivery. If the health services are carried out digitally using digital health service applications, it will be more difficult to find problems in these health services. Therefore, it is necessary to question the reliability and security in the implementation of the digital health service application and the responsibilities of the provider of the digital health service application.

This study intends to examine (1) reliability and security in the implementation of digital health service applications; and (2) the responsibility of the operator of the electronic system for digital health service applications. These two problems are fundamental problems in creating reliability and security in the implementation of the application of the digital health service.

This study used normative juridical method. The study was carried out by reviewing and testing aspects of Electronic Trading Law, namely the reliability, security, and responsibility of the parties in implementing digital health service applications based on the relevant laws and regulations. They are the Law Number 11 of 2008 on Electronic Information and Transactions, the Law Number 36 of 2014 on Health Workers, and the Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions. This study is an analytical descriptive study. It describes the facts of the implementation of digital health service applications based on the Law of on Electronic Information and

[6] Sven Kernebeck (et al.), "Impact of Mobile Health and Medical Applications on Clinical Practice in Gastroenterologu", *World Journal of Gastroenterology*, Vol. 26, No. 29, 2020, p. 4183.

Transactions, the Law on Health Workers, and the Government Regulation on the Implementation of Electronic Systems and Transactions.

B. Legality of Digital Health Service Applications with the Application of Electronic Certification or Reliability Certification

1. Implementation of Digital Health Service Applications

The development of information technology affects human life greatly. The effect also covers the health sector. The health sector has to be adapted to the development of information technology. It provides benefits in increasing the accuracy and speed of medical diagnosis and medical consultation. This speed and accuracy are achieved through the provision of services using the telemedicine method in digital health service applications.

A digital health service application works like a *marketplace* in the trade sector. Providers of digital health service applications bring together service providers (such as doctors, dentists, pharmacists, etc.) to the service recipients (patients, medicine buyers, etc.). There are three parties involved in the implementation of the application of digital health services: (1) the application party, (2) health worker, and (3) the user.

Each of the parties has a legal relationship based on an agreement. The first is between the application party and the health worker based on a partnership agreement. Partnership is a business strategy carried out by two or more parties within a certain period to achieve mutual benefits with the principle of mutual need and mutual support.[7] The second is between the application party and the user based on a standard agreement as outlined in the terms and conditions that will be approved by the user after the registration. One of the parties prepares the requirements that have been standardized on a printed agreement format, in the form of a form to then give to the other party for approval (signed). This is what is standard agreement.[8] The third is between the health workers and the users based on a therapeutic agreement. Therapeutic agreement is an agreement made between a patient and a health worker and/or doctor/dentist, in which the health worker and/or doctor/dentist tries to make maximum efforts to heal the patient in accordance with the agreement made between the two and the patient is obliged to pay healing costs.[9]

Indonesia has started to use the services of digital health service application. The sector is widely developed by start-up companies. Some of the applications are halodoc, klikdokter, Alodokter, Medikaapp, and Dokterid.

a. Halodoc

---

7 Mohammad Jafar Hafsah, *Kemitraan Usaha*, Jakarta: Sinar Harapan, 2000, p. 43.

8 N. H. T. Siahaan, *Hukum Konsumen: Perlindungan Konsumen dan Tanggung Jawab Produk*, Jakarta: Panta Rei, 2005, p. 105.

9 Wila Chandrawila Supriadi, *Hukum Kedokteran*, Bandung: CV Mandar Maju, 2001, p. 29.

Halodoc is a secure healthcare platform that brings together patients, doctors, insurance, and pharmacy in one mobile phone application.[10] The Halodoc platforms consist of an application (Android or iOS version), a web application (an application that can be accessed in the web), and a website managed by PT. Media Doctor Investama that is updated from time to time.[11] Android user can download the application from Google's Playstore and the iOS user can download it from Apple's Appstore. User also can access Halodoc through the website https://www.halodoc.com/.

The Halodoc platforms has three interrelated parties. The first is the halodoc party. It is the party that provides and operates the platforms, either a web-based platform, a website, or an application-based platform contained in the Android or iOS operating system.[12] The second is a user who uses one of the halodoc platforms.[13] The third are service providers. The party provide services or sell goods to users such as, but not limited to, doctors, psychologists, veterinarians, pharmacies, laboratories, and/or delivery services.[14]

b. Klikdokter

Klikdokter.com is a communication, information, and health education portal site for the media community and the public. Klikdokter.com was founded in 2008 and carries out its vision and mission to provide communication, information, media education for the media and non-media communities.[15] Since 2016, Klikdokter.com is owned and operated by PT. Medika Komunika Teknologi, which is a joint subsidiary of PT Kreatif Media Karya (KMK) and the Kalbe Holding Company.[16]

Klikdokter has two main products: website and application. The website can be accessed at https://www.klikdokter.com/ and the application can be accessed in any mobile device with the Android or iOS operating system.[17] There are three parties involved in organizing Klikdokter. First, the PT Medika Komunika Teknologi is a limited liability company established under the laws of the Republic of Indonesia. it owns and manages a portal site or health application that provides health services for users under the name Klikdokter.[18] The second is the user of the site/application, including but not limited to registered or unregistered parties and site/application visitor.[19] The third is business partner. A business partner is a third

---

10 Halodoc, "Join Us – Career", https://www.halodoc.com/career, accessed on August 13, 2021.

11 Halodoc, "Syarat dan Ketentuan Pengguna Halodoc", https://www.halodoc.com/syarat-dan-ketentuan, accessed on August 13, 2021.

12 *Ibid*.

13 *Ibid*.

14 *Ibid*.

15 Klikdokter, "Tentang Kami", https://www.klikdokter.com/pages/tentang-kami, accessed on August 13, 2021.

16 *Ibid*.

17 Klikdokter, "Syarat dan Ketentuan", https://www.klikdokter.com/info/disclaimer, accessed on August 13, 2021.

18 *Ibid*.

19 *Ibid*.

party who has collaborated with Klikdokter and/or is appointed by KlikDokter to provide services on the site/application, including but not limited to health services, payment services, delivery services, and/or research agencies.[20]

KlikDokter provides services from their registered business partners. The partners register themselves or cooperate with Klikdokter. Therefore, Klikdokter is an intermediary or facilitator in bringing together business partners and users. The business partners can be in the form of pharmaceutical parties or health workers.

c. Alodokter

Alodokter is another health platforms in Indonesia.[21] The platform is available in two versions. The first is the website, https://www.alodokter.com; and the second is the application version named *alodokter* on the Android and iOS operating systems.[22] Alodokter admits that the platform is accessed every month by around 26 million active users and about 30 thousand doctors who are their members.[23] The two platforms owned by Alodokter are managed by the company, PT. Sumo Technology Solutions and other related organizations.[24]

There are three parties involved in Alodokter. The first is Alodokter, which is the party that operates the web or website version of the Alodokter platform and provides Alodokter applications on the Android and iOS operating systems.[25] The second is the service provider, namely the intermediary who provides health services including doctors and hospitals.[26] The third is users, customers or users of platforms provided and operated by alodokter.[27]

d. MedikaApp

Medika Platform is a digital healthcare platform designed to connect and develop the perfect service for patients and to help clinics and hospitals growing.[28] Similar to other digital health services, the Medika Platform is also divided into two versions, website version at https://medika-platform.com/ and an application, MedikaApp, on the Android and iOS operating systems.

MedikaApp and https://medika-platform.com/ are both managed by PT Medika Cipta Digital. Apart from PT Medika Cipta Digital, other parties involved in the implementation of applications and websites are users who uses and receives services and access to all content and service features contained in the

---

20 *Ibid*.

21 Alodokter, "Tentang Kami", https://www.alodokter.com/about, accessed on August 13, 2021.

22 *Ibid*.

23 *Ibid.*

24 Alodokter, "Syarat dan Ketentuan", https://www.alodokter.com/syarat-dan-ketentuan, accessed on August 13, 2021.

25 *Ibid*.

26 *Ibid*.

27 *Ibid*.

28 Medika *Platform*, "Cari dan Booking Dokter ataupun *Treatment* Hanya di Medika *Platform*", https://medika-platform.com/#about, accessed on August 13, 2021.

application.[29] Third parties are the service providers, namely doctors and/or dentists and/or hospitals and/or clinics who collaborate with MedikaApp or Medika Platform.[30] Unlike other applications, MedikaApp does not explain explicitly the types of services. It explains in general that the service offered is a service as a user facilitator to make online orders with doctors and/or dentists at hospitals and/or clinics.[31]

e. Doctorid

Doctorid is a health portal that provides integrated solutions for users with access via desktop or mobile.[32] The website address is at https://www.dokter.id. The mobile version can be accessed through the application Dokterid. PT Kumala Media Informatics manages both site and application platforms

The parties involved are the same as those involved with other healthcare applications. The parties are (1) the PT Kumala Media Informatika, which manages the application and the website; (2) users; and (3) the health workers such as doctors and/or dentists and/or hospitals and/or clinics.

2. Electronic System Reliability and Security of the Digital Health Service Applications through the Application of Electronic Certification or Reliability Certification

The globalization of information at the beginning of the 21st century has caused changes in the activities of human life and lead to new forms of actions and legal problems. The problems of the study were examined through a framework based on the Development Law Theory. The Development Law Theory is introduced by an Indonesian legal figure, Kusumaatmadja. He was a law professor and a legal figure during the New Order era making him close to the terminology of development. According to Kusumaatmadja, development is essentially change.[33] When development occurs, law cannot play a role in development but must have had a role in the development. The role of law in development is to ensure that changes occur in an orderly manner. Law plays a role through statutory assistance and court decisions, or a combination of both.[34] The essence of development is change. Therefore, law must play a role in it. Law cannot be understood as a static element that is always behind the change itself. Law must be in front of guarding the change.[35]

---

29 Medika Platform, "Term and Services", https://medika-platform.com/index.php/term, accessed on August 13, 2021.

30 *Ibid*.

31 *Ibid*.

32 Dokter Id, "FAQs (*Frequently Ask Question*)", https://www.dokter.id/faq, accessed on August 13, 2021.

33 Atip Latipulhayat, "Khazanah Mochtar Kusumaatmadja", *Padjadjaran Jurnal Ilmu Hukum*, Vol. 1, No. 3, 2014, p. 629.

34 Mochtar Kusumaatmadja, *Pembinaan Hukum dalam Rangka Pembangunan Nasional*, Bandung: Bina Cipta, 1975, p. 3.

35 Atip Latipulhayat, *op.cit.*

The theory can be divided into two highlighted aspects: the legal and the development aspects. The development aspect can be analogous to the changes that occur in society. In this study changes occur after people started to use digital health services change. The legal aspect can be analogized as legislation that is able to accommodate these changes. In this study, the laws and regulations are related to the implementation of the digital health service application. Therefore, legal aspects or laws and regulations relating to the implementation of digital health service applications should be able to play a role in controlling aspects of development to control changes within society. The legislation that can underlie community changes in the use of digital health service applications is the Law on Electronic Information and Transactions.

Reliability and security in the implementation of digital Health service applications is based on one article in the Law on Electronic Information and Transactions. Article 15 paragraph (1) of the law states that every electronic system operator must operate an electronic system reliably and safely and be responsible for the proper operation of the electronic system.[36] Reliable means trustworthy;[37] and safe means free from danger, free from interference, and protected or hidden.[38] Reliability in English terminology means the quality of being trustworthy or of performing consistently well or literally translated, namely quality that can be trusted or can perform consistently good performance. On the other hand, security means safety. It is the condition of being protected from or unlikely to cause danger, risk, or injury, which is literally translated into a protected condition or no possibility of causing harm, risk, or injury. Reliable, according to the Law on Electronic Information and Transactions, means that the electronic system has the capability according to the needs of its use. Safe means that the electronic system is protected physically and non-physically."[39] The meaning of being responsible is explained in the explanation of the Law on Electronic Information and Transactions. There are legal subjects who are legally responsible for the operation of the electronic system.[40]

Digital healthcare applications can be viewed from two major perspectives. The first can be seen from the field of information technology. The second can be seen from the field of health services. Reliability and security to be achieved in digital health service applications are reliability and security both in terms of information technology and in terms of health services. Reliability and security in terms of information technology are meant to be reliable and safe in the application of health services used, while reliability and security in health services are reliable and

---

36 Article 15 paragraph (1) of the Law Number 11 of 2008 on Electronic Information and Transactions.

37 Kamus Besar Bahasa Indonesia Elektronik, "Arti Kata Aman", https://kbbi.web.id/aman, accessed on August 13, 2021.

38 *Ibid.*

39 Article 15 paragraph (1) Elucidation of the Law Number 11 of 2008 on Electronic Information and Transactions.

40 *Ibid.*

safe in terms of the health services carried out, both in the teleconsultation process or in the capabilities of health workers who provide health services. Therefore, in its implementation to comply with the provisions of Article 15 paragraph (1) of the Law on Electronic Information and Transactions, the application must be reliable and safe as a facility of health service.

Reliability and security in terms of information technology means that the application of digital health services can run properly and is not subject to interference from other parties. The phrase electronic system is divided into two words: system and electronic. The word system comes from Latin (systēma) and Greek (sustēma), which means a unit consisting of components or elements that are connected together to facilitate the flow of information, matter or energy.[41] The word system refers to a set of elements that are regularly interrelated to form a totality.[42] Electronic means a tool made based on electronic principles; things or objects that use tools that are formed or work on the basis of electronics.[43] Therefore, the notion of an electronic system refers to a unit consisting of components or elements that are connected together to facilitate the flow of information and materials. They are formed and work on electronics. On the other hand, the definition of an electronic system, according to the Law on Electronic Information and Transactions is a series of electronic devices and procedures that function to prepare, collect, process, analyze, store, display, announce, transmit, and/or disseminate electronic information.[44]

Reliability and security in the application of digital health services as electronic systems can be achieved in two ways. The first way is to operate an electronic system in accordance with the minimum requirements according to Article 16 of the Law on Electronic Information and Transactions. It states that if it is not otherwise stipulated by a separate law, every electronic system operator is obliged to operate an electronic system that meets the following minimum requirements.

a. It can re-display electronic information and/or electronic documents in their entirety in accordance with the retention period stipulated by the laws and regulations.
b. It can protect the availability, integrity, authenticity, confidentiality, and accessibility of electronic information in the operation of the electronic system;
c. It can operate in accordance with procedures or instructions in the operation of the electronic system.

---

41 Kresna Ramanda, "Penerapan Sistem Manajemen Operasional Pelayanan Pemesanan Menu Makanan dengan Waiting Line Method", *Jurnal Pilar Nusa Mandiri*, Vol. XII, No. 2, 2016, p. 183.

42 Kamus Besar Bahasa Indonesia (KBBI), "Arti Kata Sistem", https://kbbi.web.id/sistem, accessed on 20 July 2021.

43 *Ibid*.

44 Article 1 Number 5 of the Law Number 11 of 2008 on Electronic Information and Transactions.

d. It is equipped with procedures or instructions announced in language, information, or symbols that can be understood by the party concerned with the operation of the electronic system.
e. It has a continuous mechanism to maintain the novelty, clarity, and accountability of procedures or instructions.[45]

Based on the article, several digital health service applications, such as Halodoc, Alodokter, Klik Doktor, Medika App, and Doctorid has met the minimum requirements because each website and application can run properly. They can display documents and/or electronic information, can protect the availability of electronic information, can operate according to instructions/procedures, and are equipped with instructions/procedures that are easy to understand and have a mechanism to keep the procedures/instructions up to date.

The second way to achieve the reliability and security of the digital health service application system is by applying the reliability certification as stated in Article 42 paragraph (2) of the Government Regulation on the Implementation of Electronic Systems and Transactions. According to the article, the implementation of electronic transactions can use a reliability certificate.[46]The reliability certification process can result in the form of a reliability certificate. Reliability certificates aim to protect consumers in electronic transactions, protect consumers by ensuring that business actors have met the criteria determined by the reliability certification body.[47] The criteria are as follows.

a. It contains the identity of the business actor.
b. It contains privacy protection policies and procedures.
c. It contains system security policies and procedures.
d. It contains a guarantee statement for the goods and/or services offered.[48]

Reliability certificates can be interpreted as documents that state that business actors who carry out electronic transactions have passed an audit or conformity test from a reliability certification agency.[49] Therefore, an electronic system that has carried out reliability certification means that it has passed an audit or conformity test so that it is entitled to a reliability certificate. The reliability certificate is an identity for electronic system operators that the electronic system they implement can be trusted to be safe and reliable. Every electronic system

---

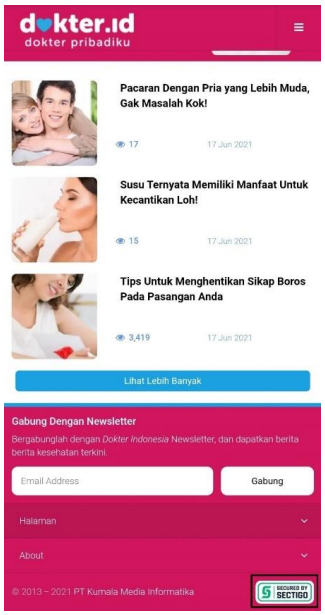
45 Article 16 paragraph (1) of the Law Number 11 of 2008 on Electronic Information and Transactions.
46 Article 42 paragraph (2)Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions.
47 Article 74 paragraphs (1) and (2) Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions.
48 Article 75 paragraphs (2) and (3)Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions.
49 Article 1 Number 27 Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions.

operator with a reliability certificate is safe and reliable because there are provisions in the Government Regulation on the Implementation of Electronic Systems and Transactions, Article 76 paragraph (1), which essentially states that reliability certificates issued by reliability certification bodies include the following categories.

a. Identity registration contains limited security that the identity of the business actor is correct (name of legal subject, status of legal subject, address, telephone number, email address, business license and/or TIN).
b. Electronic system security contains certainty about the process of delivering or exchanging data through business actors' websites with data exchange security technology such as SSL/secure socket layer protocols.
c. The privacy policy contains a guarantee that the consumer's personal data is protected as confidential as it should be.[50]

There is only one digital health service application that uses a reliability certificate, the Doctorid website. Evidence that reliability certification has been carried out is indicated by the existence of a certification logo in the form of a trust mark on the business actor's website. Therefore, the only application that has been certified is Doctorid, because there is a logo in the form of security credentials.

Figure 1. Doctorid *Website*



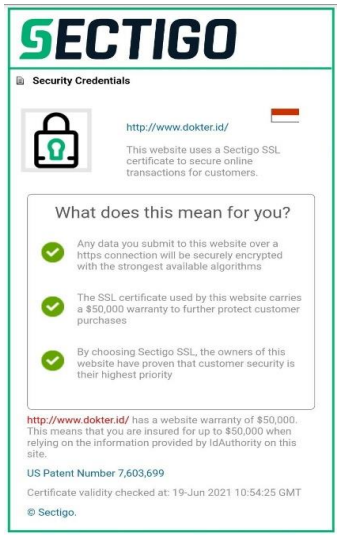
Source: Doctor.id.[51]

[50] Article 76 paragraph (1) Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions.

If the logo is opened, it will show that information related to the page is secured by the reliability certification agency to secure electronic transactions for users. Other applications such as Halodoc, Alokdokter, Klikdokter and Medika App do not have a logo in the form of security credentials on their respective websites or applications.

Doctorid uses a Reliability Certification Agency named Sectigo. SectigoStore.com is a division of Rapid Web Services, LLC, located just a block from the shoreline in sunny St. Petersburg, Florida. It is a Titanium Member of the St. Petersburg Chamber of Commerce (Top 10 Chambers of Commerce in the USA). Rapid Web Services, LLC is a Sectigo Platinum Partner and is among the most influential companies in the digital certificate industry. They have offices on four continents and clients around the world.[52] Sectigo is the Network Services division. The use of reliability certification bodies from abroad is also not solely due to the best quality but indeed until now there has been no reliability certification agency from Indonesia. according to Project Head of PT Telekomunikasi Indonesia Tbk (Telkom), Saiful Hidayat, as former coordinator of the Implementation of Electronic Systems and Transactions, currently no Indonesian certification agency that is publicly commercialized.[53]

Figure 2. Security Credentials



Source: secure.trust-provider.com.[54]

---

51 Dokter Id, Artikel, https://www.dokter.id/berita, accessed on June 19, 2021.

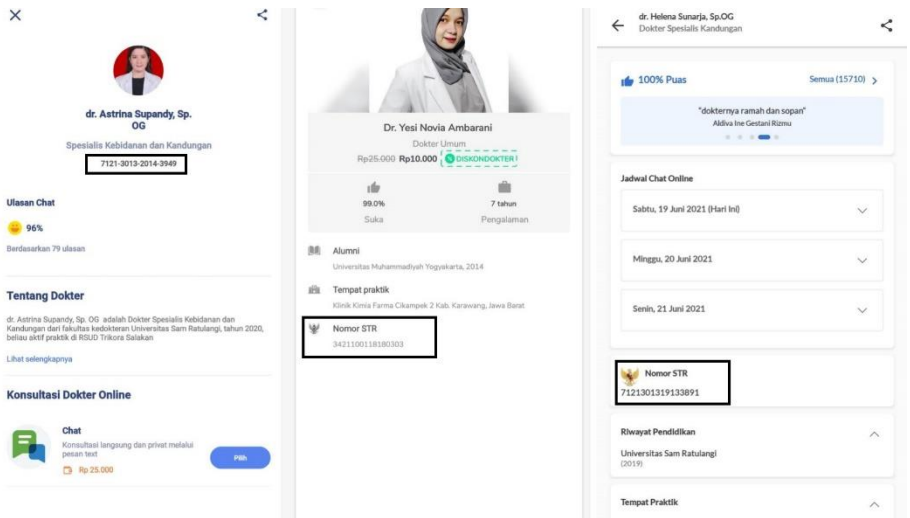
52 Sectigo, About, https://sectigostore.com/about, accessed on October 24, 2021.

53 Febrian D. A. Putri, "Lembaga Sertifikasi Keandalan Rancangan Permen akan Pacu LSK Lokal", https://teknologi.bisnis.com/read/20130401/105/5967/lembaga-sertifikasi-keandalan-rancangan-permen-akan-pacu-lsk-lokal, accessed on October 24, 2021.

54 Sectigo,https://secure.trust-provider.com/ttb_searcher/trustlogo?v_querytype=W&v_shortname=SECDV&v_search=https://www.dokter.id/berita&x=6&y=5, accessed on June 19, 2021.

Other laws and regulations that can be the basis for the reliability and security of digital health service applications as health care facilities are the Law on Health Workers and the Government Regulation on the Implementation of Electronic Systems and Transactions. It lies on Article 74 of the Law on Health Workers and Article 42 paragraph (1) of the Government Regulation on the Implementation of Electronic Systems and Transactions. The first article that can be used in the context of achieving the reliability and security of digital health service applications as health care facilities is Article 74 of the Law on Health Workers. It states that health care facility leaders are prohibited from allowing health workers who do not registered and permits to practice in health services facilities.[55] Halodoc, Alodokter, and Klik Dokter have complied with the Article 74 because the registration has been included in the profile of each doctor who works with these applications. Doctorid and Medika App do not include the registration on their respective doctor profiles.

Figure 3. Registration Number of Health Workers on Klikdokter, Halodoc and Alodokter



Source: KlikDokter Application, Halododc and Alodokter.

The second article used to achieve the reliability and security of digital health service applications as digital health service facilities is Article 42 paragraph (1) of the Government Regulation on the Implementation of Electronic Systems and Transactions. It states that electronic transaction organizers are required to use

[55] Article 74 of the Law Number 36 of 2014 on Health Workers.

electronic certificates issued by Indonesian Electronic Certification Operators.[56] Electronic Certificate is an electronic certificate containing an electronic signature and identity indicating the status of the legal subjects of the parties in an electronic transaction issued by the electronic certification operator.[57] Electronic certificates assume the role of an "electronic passport". It cannot be separated from the practice of electronic signatures. It carries strong legal force because it can ensure the identity of the signer.[58] Therefore, the implementation of electronic certification can also help achieve reliability and security in the implementation of digital health service applications because the contents of electronic certificates are data or complete identities of the parties conducting electronic transactions in the electronic system. The certificate should be used by health workers to prove that health workers who work together with digital health service applications have proven true to have the capacity of health services in the relevant digital health service application.

In practice, Halodoc, Alodokter, Klikdokter, Doctorid, and MedikaApp do not carry out the Article 42 paragraph (1) of the Government Regulation on the Implementation of Electronic Systems and Transactions. Based on observations of this study, in the terms of the cooperation offer issued by the application party to the health worker, there is no requirement that the health worker must have an electronic certificate to become a partner of the application. Therefore, Halodoc, Alodokter, Klikdokter, Doctorid, and MedikaApp do not carry out the provisions in Article 42 paragraph (1) the Government Regulation on the Implementation of Electronic Systems and Transactions on obligations regarding electronic certificates.

Based on the analysis, this study concludes that the application of digital health services as an electronic system and as a health service can further maximize and optimize their reliability and security. In practice there have been no cases related to reliability and security in digital health service applications to the level of law enforcement. However, most digital health service applications do not implement the provisions of laws and regulations related to basic safety and reliability, such as the provisions of Article 42 paragraphs (1) and (2) the Government Regulation on the Implementation of Electronic Systems and Transactions and Article 74 of the Law on Health Service. If the parties involved in the implementation of the digital health service application implement each of these provisions, their reliability and security in terms of systems and health services can be achieved. They will be able to further minimize interference from both internal and external health service applications.

---

56 Article 42 paragraph (1) Government Regulation Number 47 of 2016 on Health Service Facilities.

57 Article 1 Number 9 Government Regulation Number 47 of 2016 on Health Service Facilities.

58 Ahmad Budi Setiawan, "Studi Standarisasi Sertifikat Elektronik dan Keandalan dalam Penyelenggaraan Sistem Transaksi Elektronik"*, Buletin Pos dan Telekomunikasi*, Vol. 12, No. 2, 2014, p. 127.

3. Responsibilities of Operators of Electronic System Digital Health Service Applications

Digital health service applications work almost the same as peer-to-peer lending applications, where there are applications that bring together service requesters and service providers. The service requesting party is the user and the service provider is the health worker who cooperates with the digital health service application. The application party has an important role because it has the task of bringing together the two parties. The legal responsibilities borne by the digital health service application can be distinguished between legal responsibility as an electronic system operator and responsibility as an implementer of health services.

The legal responsibility as an electronic system operator appears due to a legal relationship between the application operator and the user. The legal relationship is a relationship between two or more legal subjects. In this legal relationship, the rights and the obligations of one party are in conflict with the rights and obligations of the other party.[59] The legal relationship is based on a standard agreement. A standard agreement (standard contract, standardized contract, pad contract, or an ordinary agreement) is an agreement made by the parties on something and the contents have been standardized.[60]

The provisions that have been standardized are set forth into terms and conditions made by the application operator. It also needs to be approved by the user as a sign of agreement from the user. In the standard agreement, there are provisions that violate the applicable laws and regulations, then the responsibility is born for the application organizer. In addition to being based on a standard agreement, the user and the application operator also bear legal responsibility based on an engagement according to the law, if the application operator takes prohibited actions or does not take actions ordered by law, especially the Law on Electronic Information and Transactions, the Government Regulation on the Implementation of Electronic Systems and Transactions, and the Health Manpower Act.

Responsibility refers to a state of being obliged to bear everything (if anything happens, you can be sued, blamed, sued, and so on).[61] According to Halim, Legal responsibility is a further consequence of the implementation of the role, whether the role is a right and an obligation or power. In general, legal responsibility is defined as an obligation to do something or behave in a certain way that does not deviate from existing regulations.[62] In the legal dictionary, there are two terms that refer to responsibility: liability (the state of being liable) and responsibility (the

---

59 R. Soeroso, *Pengantar Ilmu Hukum,* Jakarta: Sinar Grafika, 2011, p. 269.

60 Agus Satory, "Perjanjian Baku dan Perlindungan Konsumen dalam Transaksi Bisnis Sektor Jasa Keuangan: Penerapan dan Implementasinya di Indonesia", *Padjadjaran Jurnal Ilmu Hukum*, Vol. 2, No. 2, 2015, p. 274.

61 Kementerian Pendidikan dan Kebudayaan, "Kamus Besar Bahasa Indonesia Daring", https://kbbi.kemdikbud.go.id/entri/tanggung%20jawab, accessed on October 25, 2021.

62 Julista Mustamu, "Pertanggungjawaban Hukum Pemerintah (Kajian tentang Ruang Lingkup dan Hubungan dengan Diskresi)", *Jurnal Sasi*, Vol. 20, No. 2, 2014, p. 22.

state or fact of being responsible).[63] Liability is defined to designate all the characteristics of rights and obligations. It is also a condition of being subject to actual or potential obligations; the condition of being responsible for actual or possible things such as losses, threats of crime, costs or expenses. Responsibility means (things that are responsible for an obligation and include decisions, skills, abilities, and talents).[64] Responsibility is also defined as a moral attitude to carry out obligations. In the sense of liability, responsibility is a legal attitude to account for violations of obligations or violations of the rights of other parties.[65]

There are also two forms of legal responsibility borne by digital health service application providers: obligations and sanctions. The obligations arise without the need for a violation to occur; and sanctions arises when the provider commits a violation. Liability of sanctions is regulated by Article 42 paragraph (1) in conjunction with Article 100 paragraph (1) and (2) the Government Regulation on the Implementation of Electronic Systems and Transactions and Article 74 in conjunction with Article 82 paragraph (2) of the Law on Health Service. The obligations are regulated by Article 5 paragraphs (1) and (2), Article 15 paragraph (1), Article 18 paragraph (1) and Article 33 of the Government Regulation on the Implementation of Electronic Systems and Transactions.

The Article 42 paragraph (1) of the Government Regulation on the Implementation of Electronic Systems and Transactions states that organization of Electronic Transactions must use Electronic Certificates issued by Indonesian Electronic Certification Operators.[66] Therefore, if a provider does not carry out electronic certification, it can be asked for legal responsibility for its violation of the article. The form of responsibility is administrative responsibility, as stated by Article 100 paragraph (1) the Government Regulation on the Implementation of Electronic Systems and Transactions that violations of the provisions of Article 4, Article 5 paragraph (1) and paragraph (2), Article 6 paragraph (1), Article 9 paragraph (1) and paragraph (4), Article 14 paragraph (1) and paragraph (5), Article 15 paragraph (1), Article 17 paragraph (41), Article 18 paragraph (1), Article 21 paragraph (2) and paragraph (3), Article 22 paragraph (1), Article 23, Article 24 paragraph (1), paragraphs (2) and (3), Article 25, Article 26 paragraph (1), Article 28 paragraph (1), Article 29, Article 30 paragraph (1), Article 31, Article 32 paragraph (1) and paragraph (2), Article 33, Article 34 paragraph (1), Article 37 paragraph (1) and paragraph (2), Article 38 paragraph (3), Article 39 paragraph (2), Article 40 paragraph (1) and paragraph (2), Article 42 paragraph (1) and paragraph (3), Article 51 paragraph (1), Article 53 paragraph (3), Article 55 paragraph (2), Article 63

---

63 M. Sabaruddin Sinapoy, "Tanggung Jawab Hukum Presiden dalam Pemberian Izin Pemeriksaan Pejabat Negara", *Yuridika*, Vol. 27, No. 3, 2012, p. 224.

64 Ridwan HR, *Hukum Administrasi Negara*, Jakarta: Rajawali Pers, 2016, pp. 318-319.

65 Zainal Asikin (et al), *Pengantar Hukum Perusahaan*, Jakarta: Prenadamedia Group, 2016, p. 252.

66 Article 42 paragraph (1), Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions.

paragraph (3), Article 64 paragraph (1), Article 69 paragraph (1), Article 82 paragraph (7), Article 84 paragraph (1) and paragraph (2), Article 87 paragraph (2), and Article 98 paragraph (1), are subject to administrative sanctions.[67]
The above administrative sanctions are further explained in paragraph (2). It states that administrative sanctions as referred to in paragraph (1) can be in the form of
(1) written warning;
(2) administrative fines;
(3) temporary suspension;
(4) access termination; and/or
(5) removed from the list."[68]

Provider can help make the electronic system safe and reliable, by being more selective about the health workers who will be partners. One way to be more selective with health workers is to include provisions regarding the minimum requirements of health workers in accordance with the requirements as stipulated in the legislation. The minimum requirement can be found in Article 44 paragraph (1) of the Health Manpower Law. It states that health workers who carry out practice are required to have a Registration Certificate (STR).[69] Article 46 paragraph (2) of the Law on Health Workers states that every health worker who practices in the field of health services is required to have a permit in the form of a Practice License (SIP).[70]

Based on the two articles, a health worker must have STR and SIP to practice. In practice, some of these applications have included an STR on the profiles of every doctor or health worker who collaborate with these applications. However, there are still some applications that have not included an STR. If an application does not include it, there can be unlicensed health workers who become partners. This act has been prohibited in the Law on Health Workers. Article 74 of the Law states that the head of health care facilities is prohibited from allowing health workers who do not have STR and permits to practice in health care facilities.[71] The application party as a health service facility can be subject to sanctions and responsible for the violation, if it employs health workers who do not have a permit or STR. The form of legal responsibility borne is administrative responsibility. Article 82 paragraph (2) of the Law states that every health service facility that does not implement the provisions of Article 26 paragraph (2), Article 53 paragraph (1), Article 70 paragraph (4), and Article 74 are subject to administrative sanctions.[72] The administrative

---

67 Article 100 paragraph (1) Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions.
68 Article 100 paragraph (2) Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions.
69 Article 44 paragraph (1) of the Law Number 36 of 2014 on Health workers.
70 Article 46 paragraphs (1) and (2) of the Law Number 36 of 2014 on Health workers.
71 Article 74 of the Law Number 36 of 2014 on Health workers.
72 Article 82 paragraph (2) of the Law Number 36 of 2014 on Health workers.

sanctions in question are verbal warnings, written warnings, administrative fines and/or revocation of permits.[73]

There are some articles that reflect obligations to be carried out without the need for a violation. First, Article 5 paragraph (1) of the Government Regulation on the Implementation of Electronic Systems and Transactions states that electronic system operators are required to ensure that their electronic system does not contain electronic information and/or electronic documents that are prohibited in accordance with the provisions of the law.[74] Article 5 paragraph (2) of the Government Regulation on the Implementation of Electronic Systems and Transactions states that electronic system operators must ensure that their electronic system does not facilitate the dissemination of electronic information and/or electronic documents that are prohibited in accordance with the provisions of the law.[75] Based on the article, providers of digital health service applications must continue to ensure that the application does not contain or become a facility for disseminating something prohibited in other laws and regulations.

The next articles are Article 15 and Article 18 of the Government Regulation on the Implementation of Electronic Systems and Transactions. Article 15 paragraph (1) of the Government Regulation on the Implementation of Electronic Systems and Transactions states that every electronic system operator is obliged to delete irrelevant electronic information and/or electronic documents under his control at the request of the person concerned.[76] Article 18 paragraph (1) of the Government Regulation on the Implementation of Electronic Systems and Transactions states that every electronic system operator is obliged to provide a mechanism for deleting electronic information and/or electronic documents that are not relevant in accordance with the provisions of the legislation.[77] Based on these two articles, the operator of the digital health service application in operating the application has an obligation to delete irrelevant information or electronic documents. If the deletion is related to Article 18 paragraph (1), then the deletion is carried out automatically with a mechanism that must be owned by the application operator as the operator of the electronic system.

The next article is Article 33 of the Government Regulation on the Implementation of Electronic Systems and Transactions, which states that for the purposes of the criminal justice process, the electronic system operator is obliged to provide electronic information and/or electronic data contained in the electronic

---

73 Article 82 paragraph (3) of the Law Number 36 of 2014 on Health workers.

74 Article 5 paragraph (1) Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions.

75 Article 5 paragraph (2) Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions.

76 Article 15 paragraph (1) Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions.

77 Article 18 paragraph (1) Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions.

system or electronic information and/or electronic data generated by the electronic system upon a valid request from the investigator for certain criminal acts in accordance with the authorities regulated in the law.[78] Based on this article, providers of digital health service applications have an obligation to provide any information that is in or produced by their digital health service applications for the benefit of the judiciary with a legitimate request from investigators, although not for the benefit of the organizers of the digital health service application.

This study is of the position that there are two forms of legal responsibility for electronic system operators. First, obligations must be carried out as mandated in the provisions of the existing laws and regulations. This legal responsibility occurs when the legal subject has become the organizer of the electronic system. The second is legal responsibility that occurs following a violation of legislations. This legal responsibility can be borne by receiving sanctions. The sanctions can be criminal or civil sanctions. It also covers compensation and administrative sanctions. The legal responsibility only occurs when the electronic system operator violates a provision in the laws and regulations.

C. Conclusion

Based on the discussion, this study has generated several conclusions. First, based on Article 15 paragraph (1) of the Law on Electronic Information and Transactions, the reliability and security of the electronic system of digital health service applications can be achieved if the digital health service application uses a reliability certificate as referred to in Article 42 paragraph (2) of the Government Regulation on the Implementation of Electronic Systems and Transactions and electronic certificates as referred to in Article 42 paragraph (1) of the same regulation. It also should employ licensed health workers as referred to in Article 74 of the Law on Health Workers. In the implementation, most of the digital health service applications do not include provisions regarding the obligation to use electronic certificates, use certificates of reliability, and include the Registration of each health worker.

Second, the providers of digital health service applications have two forms of legal responsibility. The first is in the form of criminal liability, civil liability, and administrative responsibility. These responsibilities are borne if the provider of the digital health service application violates Article 15 paragraph (1) of the Law on Electronic Information and Transactions, Article 42 paragraph (1) and paragraph (2) of the Government Regulation on the Implementation of Electronic Systems and Transactions, Article 44 paragraph (1), Article 46 paragraph (2), and Article 74 of the Law on Health Workers. The second legal responsibility is responsibility in the form of obligations that must be carried out in operating the digital health service

[78] Article 33 Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions.

application. These obligations are as set out in Article 5 paragraphs (1) and (2), Article 15 paragraph (1), Article 18 paragraph (1), and Article 33 of the Government Regulation on the Implementation of Electronic Systems and Transactions.

Based on the conclusions, this study can also generate two suggestions to solve the problems. First, the Government needs to revise or update the laws and regulations related to the implementation of digital health service applications. They are the Law on Electronic Information and Transactions and Law on Health Workers, as well as their derivative laws and regulations. The update is in the provisions regarding the use of reliability certificates and electronic certificates to create reliability and security in the electronic system of digital health service applications. Provisions regarding the use of reliability certificates must be changed from the previous regulatory nature to being coercive, so that every electronic system operator has an obligation to use a reliability certificate.

Second, before the establishment of a legislation that specifically regulates the application of digital health services, the government can take preventive actions. Ministry of Communication and Information, in collaboration with the Ministry of Health, can take these preventive actions to disseminate information regarding the importance of electronic certification and reliability certification to improve reliability and security in the implementation of digital health service applications. In addition, the Ministry of Communication and Information and the Ministry of Health can regulate the use of electronic certification and reliability certification in the implementation of electronic systems.

References

Books

Mochtar Kusumaatmadja, *Pembinaan Hukum dalam Rangka Pembangunan Nasional*, Bina Cipta, Bandung, 1975.

Mohammad Jafar Hafsah, *Kemitraan Usaha*, Sinar Harapan, Jakarta, 2000.

Muhamad Amirulloh, *Hukum Teknologi Informasi dan Komunikasi (TIK) sebagai Hukum Positif di Indonesia dalam Perkembangan Masyarakat Global*, Unpad Press, Bandung, 2016.

N. H. T. Siahaan, *Hukum Konsumen: Perlindungan Konsumen dan Tanggung Jawab Produk*, Panta Rei, Jakarta, 2005.

R. Soeroso, *Pengantar Ilmu Hukum,* Sinar Grafika, Jakarta, 2011.

Ridwan HR, *Hukum Administrasi Negara*, Rajawali Pers, Jakarta, 2016.

Soegijardjo Soegijoko, *Perkembangan Terkini Telemedika dan E-Health serta Prospek Aplikasinya di Indonesia*, Fakultas Teknologi Industri Universitas Islam Indonesia (TI FTI UII), Yogyakarta, 2010.

Wila Chandrawila Supriadi, *Hukum Kedokteran*, CV Mandar Maju, Bandung, 2001.

Zainal Asikin (et.al), *Pengantar Hukum Perusahaan*, Prenadamedia Group, Jakarta, 2016.

Other Documents

Agus Satory, "Perjanjian Baku dan Perlindungan Konsumen dalam Transaksi Bisnis Sektor Jasa Keuangan: Penerapan dan Implementasinya di Indonesia", *Padjadjaran Jurnal Ilmu Hukum*, Vol. 2, No. 2, 2015.

Ahmad Budi Setiawan, "Studi Standarisasi Sertifikat Elektronik dan Keandalan dalam Penyelenggaraan Sistem Transaksi Elektronik"*, Buletin Pos dan Telekomunikasi*, Vol. 12, No. 2, 2014.

Alodokter, "Syarat Dan Ketentuan", https://www.alodokter.com/syarat-dan-ketentuan.

_____, "Tentang Kami", https://www.alodokter.com/about.

Anggie Septie Aningrum AN (et.al.), "Analisis Penerapan Etika dan Hukum Kesehatan pada Pemberian Pelayanan Kesehatan di Rumah Sakit Nene Mallomo Kabupaten Sidenreng Rappang", *Jurnal Ilmiah Manusia dan Kesehatan*, Vol. 1, No. 3, 2018.

Atip Latipulhayat, "Khazanah Mochtar Kusumaatmadja", *Padjadjaran Jurnal Ilmu Hukum*, Vol. 1, No. 3, 2018.

Devina Martha Listianingrum (et.al.), "Perlindungan Hukum terhadap Konsumen dalam Pelayanan Kesehatan Berbasis Aplikasi Online", *Diponegoro Law Journal,* Vol. 8, No. 3, 2019.

Dokter Id, "FAQs (*Frequently Ask Question*)", https://www.dokter.id/faq.

_____, Artikel, https://www.dokter.id/berita.

Febrian D. A. Putri, "Lembaga Sertifikasi Keandalan Rancangan Permen akan Pacu LSK Lokal", https://teknologi.bisnis.com/read/20130401/105/5967/lembaga-sertifikasi-keandalan-rancangan-permen-akan-pacu-lsk-lokal.

Halodoc, "Join Us – Career", https://www.halodoc.com/career.

_____, "Syarat dan Ketentuan Pengguna Halodoc", https://www.halodoc.com/syarat-dan-ketentuan.

Julista Mustamu, "Pertanggungjawaban Hukum Pemerintah (Kajian tentang Ruang Lingkup dan Hubungan dengan Diskresi)", *Jurnal Sasi*, Vol. 20, No. 2, 2014.

Kamus Besar Bahasa Indonesia (KBBI), "Arti Kata Sistem", https://kbbi.web.id/sistem.

_____, "Arti Kata Aman", https://kbbi.web.id/aman.

Kementerian Pendidikan dan Kebudayaan, "Kamus Besar Bahasa Indonesia Daring", https://kbbi.kemdikbud.go.id/entri/tanggung%20jawab.

Kernebeck, Sven (et.al.), "Impact of Mobile Health and Medical Applications on Clinical Practice in Gastroenterologu", *World Journal of Gastroenterology*, Vol. 26, No. 29, 2020.

Klikdokter, "Syarat dan Ketentuan", https://www.klikdokter.com/info/disclaimer.

_____, "Tentang Kami", https://www.klikdokter.com/pages/tentang-kami.

Kresna Ramanda, "Penerapan Sistem Manajemen Operasional Pelayanan Pemesanan Menu Makanan Dengan *Waiting Line Method*", *Jurnal Pilar Nusa Mandiri*, Vol. XII, No. 2, 2016.

M. Sabaruddin Sinapoy, "Tanggung Jawab Hukum Presiden dalam Pemberian Izin Pemeriksaan Pejabat Negara", *Yuridika*, Vol. 27, No. 3, 2012.

Medika Platform, "Cari dan *Booking* Dokter ataupun Treatment Hanya di Medika Platform", https://medika-platform.com/#about.

_____, "Term and Services", https://medika-platform.com/index.php/term.

Sectigo, https://sectigostore.com/about.

_____, https://secure.trust-provider.com/ttb_searcher/trustlogo?v_querytype=W&v_shortname=SECDV&v_search=https://www.dokter.id/berita&x=6&y=5.

Soekidjo Notoatmodjo, "Kesehatan dan Pembangunan Sumber Daya Manusia", *Jurnal Kesehatan Masyarakat Nasional*, Vol. 2, No. 5, 2008.

Legal Documents

The Law Number 11 of 2008 on Information and Electronic Transactions [*Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*].

The Law Number 36 of 2014 on Health Workers [*Undang-Undang Nomor 36 Tahun 2014 tentang Tenaga Kesehatan*].

The Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions [*Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*].