JURNAL HUKUM KESEHATAN INDONESIA

Vol. 01, No. 02, Oktober 2021, h. 121-131
p-ISSN 2776-4753 e-ISSN 2776-477X
Available Online at https: https://jurnal-mhki.or.id/jhki

E-HEALTH PERSONAL DATA PROTECTION IN INDONESIA

Hendra[1], Ravel[2], Novel Firdhaus[3], Michael Ari Kurniawan[4], Gilbert Platina[5]
[12345]Faculty of Business Law, Bina Nusantara (BINUS) University
[1]*E-Mail*: Hendra012@binus.ac.id
[2]*E-Mail*: Ravel@binus.ac.id
[3]*E-Mail*: Novel.firdhaus@binus.ac.id
[4]*E-Mail*: Michael.kurniawan006@binus.ac.id
[5]*E-Mail*: Gilbert.nainggolan@binus.ac.id

Submitted : 01-08-2021	Be Accepted : 30-09-2021	Publication : 31-10-2021

ABSTRACT

Since Covid-19 day by day users additional attentive to their privacy and information protection. though this drawback is transverse to each digital service, it's particularly relevant once important and private info is managed, as in eHealth and well-being services. throughout the last years, many alternative innovative services during this space are projected. However, information management challenges area unit still in would like of an answer. In general, information area unit directly sent to services however no trustworthy instruments to recover this information or take away them from services area unit obtainable. In these paper author needs to debate privacy aspects of non-public information within the eHealth program and the way Indonesia regulate Privacy and protection of patient's personal information in Indonesia. the strategy used is normative juridical approach with descriptive analytical specifications. the method of knowledge assortment is finished through literature. eHealth is incredibly advanced and importance of this set of issues can't be solely managed by the self-regulation of personal people, not as a result of they pursue dark or ineligible interests, however as a result of the privately-owned enterprises cannot withstand the framework of values, principles and rights the charm to the role of the general public actors looks to be applicable within the regulation of this sector and for Republic of Indonesia the approach of existing law continues to be sectoral and extremely general.

Keywords: eHealth; Regulation; Personal data.

A. INTRODUCTION

One of the pillars of globalisation is that the use of communication that is main pillar of negotiation with exploitation advances in info technology. In its development, progress info technology has pushed countries to liberalize the arena communication thus on encourage competition and globalisation of communication and ultimately has aroused economic progress. Now, the planet is within the modern era wherever the existence of knowledge includes a necessary role important in human life (Smith, 2001). Through advances in data, communication, and technology (ICT) is one in all the most factors that promote development and growth world economy (Anan, 2004). Currently, data may be a trade goods that has price high economy as a result of not all parties ready to method from a data into associate acceptable data along with his desires

(Makarim, 2003). ICT play vital role in supporting life daily, as well as within the field of health.

In the future ICT is popping into a lot of complicated issue owing to pervasive sensing platforms, that supported by new technological paradigms like net of Things (IoT) and cyber physical systems (CPS), can modify a brand-new generation of eHealth and well-being services (X, 2016). These innovative services can improve their performance (including their personalization, cost, and process delay) with relation to presently existing solutions.(Bordel et al., 2017). To try that, an oversized catalogue of biological signals, environmental measures, and people's behaviour data (among different knowledge sources) should be captured and processed by well-being services. Besides, edge computing architectures should be enforced to succeed in that objective.Timmons, Evans, and Nair justify that nurse cannot be separated from the influence of world globalisation. globalisation not solely has associate influence on urbanization, however conjointly on the event of science and technology (Timmons et al., 2016). Information technology that's developing therefore apace is one in every of the world challenges in all scientific fields, as well as nursing. many applications, each within the sort of computer code and hardware or the mixing of each is employed in optimizing the delivery of health services. One that may be employed in community nursing is e-health. E-health applications is computer-based or integrated with smartphones. the chance for e-health applications in Indonesia is kind of massive, particularly mobile Health and telemedicine. (Peate, 2013) Types of eHealth several types of eHealth that can be developed in community nursing include:

1. Telephone conversations between patients and physicians concerning symptom sorting, provision of medical devices, watching important signs and pointers for victimisation drugs.
2. Calls or short messages regarding health promotion and also the remainder system.
3. Patients seeking health data use a mobile device. As an example, mobile phones or pc applications area unit sensible as a network for consultation or creating consultation agreements.
4. Consultation between patients and nurse's victimisation video conferencing.
5. Patients begin contact with practitioners.
6. Native web as a support cluster with chat rooms, blogs or social networks to share data with alternative users.

In this era information intensive software system, like social media, wellness, and mobile health (mHealth) apps, became present in standard of living and area unit often utilized in a spread of things. Years ago, social media networks were largely accessed from ancient computers, however the rising use of smartphones and apps to access those networks has opened a Pandora's Box concerning information assortment, together with geolocation, motion information, health-related information, and activity information (Ienca et al., 2018). The collection of further activity information regarding users was at the start terribly restricted, and solely a fraction of basic information was collected (IP address, software, and browser version). In distinction, current apps on smartphones have begun continuous watching of users by gather geolocation and motion information, and thus, they need the power to infer users' physical and psychological state states, as an example, to find signs of depression and predict their next probably location (Saeb et

al., 2015). Moreover, app corporations have collected an amazing quantity of knowledge on individuals' public and personal activities within the digital world, that area unit being reused not just for the sake of their primary platforms, however additionally in alternative profitable business sectors, like artificial intelligence, life sciences, automotive producing, and health information provision (Cao & Lin, 2017). Previously, users were ready to merely opt of those services, however this can be changing into progressively difficult these days given the monopoly market structure instilled by the businesses that drive digital transformation. Indeed, customers area unit progressively forced to use these services because of they either don't have the other equivalent alternatives in terms of services provided or they're influenced by their peers or oldsters (in case of children) to use the services. typically, these corporations nudge users with promoting methods, like substantial benefits and discounts offered solely on these platforms (Minh et al., 2013). This proves to be problematic since to use these currently necessary services, a minimum of to some extent, users need to consent to some obligatory information sharing and consequently expose their privacy (Kaplan, 2016).

In view of the aforesaid facts, it's important that the connection between users and firms is clear and controlled. This relationship is presently largely outlined within the terms and conditions (T&Cs), terms of service, and information privacy notices, that area unit sadly lacking in many aspects in term of sanctioning potential users to create an informed call once signing up for a service. for example, users aren't warned regarding doable harms that may result from their activities on the platforms (e.g., linkage of many anonymous information sources may lead to reidentification of otherwise anonymous datasets and lack of awareness of secondary use may undermine user privacy and confidentiality). to boot, the knowledge provided within the T&Cs of various platforms isn't reader-friendly and not compactly summarized to nudge users to read them totally. they're additionally not harmonic within the sense that every platform has its own implementation or they're merely not outstanding enough throughout the method of signing up for the service(Cate & Mayer-Schönberger, 2013). Another weakness of T&Cs is that they are doing not create it clear that social media and the linkage of many independent distinctive information bases will yield health data. Health information represent a special information class (Union, 2016), requiring special security and privacy policies for governance. Indeed, several international legislations outline health information as special information needing additional protection than "usual" non health connected information.

Right now, wherever digital services area unit altogether integrated into voters daily living, many totally different governmental establishments like the European Commission have planned rules to safeguard this personal vital information from malicious uses. particularly, future eHealth and well-being services ought to respect the proper of users with reference to their personal data: right to access, modify, and be forgotten. However, most times, well-being services cannot offer trustworthy instruments to execute these rights and, once provided, they are doing not guarantee an entire execution in line with revealed regulation. This drawback is extremely associated with current

service architectures. during this theme, personal information regarding users' health or situation area unit noninheritable and directly sent to remote servers wherever well-being services executed dead (Connor et al., 2017). Sometimes, this information are kept in native repositories, however they're forever sent to service providers' servers. This approach, in fact, is extremely helpful, as remote agents (such as doctors) access this information terribly simply once processed by services. however, it causes a belligerent situation: service suppliers replicate and store all users' personal and important information. Obviously, these service suppliers (legally) cannot use users' information with industrial or alternative similar objectives, and users will forever execute the rights delineated within the corresponding regulation (General information Protection Regulation (GDPR), in Europe, as an example.(Ramon Alcarria, Borja Bordel, Tomás Robles, Diego Martín, 2018).

In real things, users should trust service suppliers to get rid of (or modify) their information once requested, as no guarantee is provided. Besides, usually, this data is used with industrial functions while not the users' permission. in a very digital society wherever, additional and additional, individuals' area unit involved regarding their information privacy and wherever, additional and additional, digital services and flowing personal data area unit essential components within the daily living, this case should be self-addressed.

The fast technological advances that occur and are accelerated thanks to covid-19 actually have a myriad of advantages as a result of it makes it easier for all parties in telemedicine development and use and e-health and connected fields others has several opportunities to use facilitate solve issues and challenges within the field. differing kinds Applications that may be used include: recording and reportage, happening management, e-prescribing, management of TB patients, mobile telemedicine systems, e-psychology, mobile e-health, numerous styles of systems e-health with image process, further as systems open-EHR (Electronic health record) and cheaper prices however it looks that Indonesia doesn't appear prepared for the threats that exist, one in all that is E-health, legal problems which frequently escapes from: (1) with reference to a way to shield laws on privacy of patient's personal data; (2) however existing legal provisions will offer legal protection for patients. In fashionable economic developments like nowadays, data as well as personal knowledge may be a terribly valuable quality that has high measure so it's wide utilized by businesses so protection is required. Therefore In this article, the author answers two main questions:1) Privacy aspects of personal data in the e-health program; 2) How Indonesia regulate Privacy and protection of patient's personal data in Indonesia.

B. METODE

The research method used in this study is a normative juridical research method (Lili Rasjidi, 2005). It is said to be a normative juridical research because basically this research covers the entire national legislation on elections, as well as the criminal procedure law for elections which are specifically regulated. The results of the research data are processed by systematizing legal materials, making classifications of legal materials, then processing and interpreting them using legal interpretation methods that are common in legal science, and then analyzed in a normative juridical manner in the form of a normative juridical presentation.(C.F.G. Sunaryati Hartono, 1994; Soerjono Soekanto & Sri Mamudji, 1986; Soerjono Soekanto, 1986)

C. RESULTS OR DISCUSSION

1. Privacy Aspects of Personal Data In The E-Health Program

a) Definition of personal data

According to the OECD Guidelines and the Data Protection Convention of the Council of Europe, personal data are defined as all information about an identified or identifiable natural person ("information about an identified or identifiable natural person").ICT developments when analyzed in a limited manner, they cannot keep up with the times, which is why there are still many debates regarding each of them.

The classification of personal data varies from country to country. In countries with personal data protection laws, the data protection agency provides interpretations about the types of data protected by law (Mark F. Kightlinger, E. Jason Albert, 2002). Several national laws categorize personal data, for example: names, addresses, emails, phone numbers, ID numbers that can be combined with information in the public register in order to identify an individual. In E-health programs usually potected data is a protected personal data that is called a unique identifier such as full name, account number, service provider because it can identify a patient, data demographics such as address, telephone number, email address which is usually combined with age, gender. Furthermore, in addition to medical conditions, smoking or drinking habits, and data on hospital and doctor visits, including diagnostic results, are personal data that must be protected because they can identify individuals. Furthermore, in addition to medical conditions, smoking or drinking habits, and data on hospital and doctor visits, including diagnostic results, are personal data that must be protected because they can identify individuals. What is a data that must be protected is the patient's personal data that was sent using both ordinary and electronic media, for an example in The United States in HIPAA (The Health Insurance Portability and Accountability Act) talks between patients and doctors is a data that must be protected as only data in paper form.

b) Extended Notions of Health Data and Consent

It is possible to obtain permission to use pre-existing data in a variety of ways. In medicine, with "broad consent," research participants are sometimes asked to allow future reprocessing of data, and this process is overseen by a research ethics committee. It is necessary for researchers to obtain broad consent because those giving it have no idea whether their data will be used for specific projects in the future. Other models require contacting participants again to obtain specific consent for each future project. Data donation is a more radical idea in which people grant access to their data under limited conditions, if any (Shaw et al., 2016). All of these models are based on medical research and health care. As described in the T&Cs, consent is normally based on the initial agreement and has a commercial background in the case of social media, financial, and location data. This consent is often uninformed, despite the fact that data could be used in myriad ways, even if they are not ultimately health-related. Data that are currently generated are no exception to this. It is even worse in terms of the possible uses of old paper-based data that is digitalized or of future data that may seem

irrelevant now, but when combined with other datasets could yield highly relevant health information. Due to its broad nature, current consent for data sharing is largely blind. The consent system needs to look back and forward, as well as closely at the present. In essence, consent must be capable of time travel, just as data are capable of time travel.

In today's highly data-driven and data-intensive research, the traditional models of obtaining consent are no longer adequate, and this indicates the need for new forms of obtaining participant consent (Mostert et al., 2016). Moreover, in these environments, the traditional form of obtaining consent by informing each participant about his or her rights and protections is nearly impracticable because of the sheer scale and complexity of an endeavor of this kind (Ioannidis, 2013). Several scholars have suggested ways to address this problem, from information technology-based systems like dynamic consent, which provide a better way to inform and maintain a relationship between researchers and participants, to management-based solutions that ensure a community-based approach to data governance. and radical solutions like data donations (Kaye et al., 2015).

The configuration of personal data appears as an individual right to determine whether to share or exchange your personal data. In addition, individuals also have the right to determine the conditions for carrying out the transfer of personal data. Personal data in European countries regulate the input and output of personal data between countries and prohibit leaving personal data from European countries if third countries do not have equivalent laws. To avoid this, the OECD (Organization for Economic Development and Cooperation) has issued a guideline known as the guidelines for the protection of privacy and the cross-border movement of personal data (Ian, 2014).

c) Confidentiality And Data Sharing In New Healthcare Models

Direct health data is easier to manage, although it has its own challenges. A specific consent system may seem simple, but it can place significant restrictions on researchers and be very burdensome for patients. Broad consent raises its own problems, particularly with terminology; even with explicit consent to use a person's data in a particular project, researchers may also want broad consent to access and share a participant's full medical history Linking medical records to simple follow-up, d. H. Consent is given not only for health data generated in the project itself (currently), but also in previous years or decades (the past) and in the coming years (the future). The donation illustrates the ethical and legal challenges associated with consenting to further use beyond death of genetic health data and non-genetic data, some of which may affect family members.In fact, most current data protection frameworks like GDPR neglect data donation and the use of data after death is out of their reach. At least until the time of death, a dynamic consent system appears to be a promising means of controlling the access of different users to past and current medical data and of controlling the linkage of data with other studies. Another problem that makes direct data difficult to use relates to mHealth data (data that is collected when using mHealth solutions). Such applications are mainly monitored by national

authorities and require FDA approval in the USA, for example. The data collected by these apps must be legally protected more strongly than the US regulation and the GDPR currently provide, in particular the question of consent is unregulated and what could be regarded as possible consent (the acceptance of TandC) does not correspond to the high Standards imposed by traditional consent in research.

Indirect health data, such as movement data, social media, and an individual's movement data, are not currently regulated in the United States' health data model. In the European Union, the GDPR covers such data, but is not considered otherwise. Health data and therefore benefit from less protection than is the case with inferred data. As mentioned above, consent is usually given via the TandC of the corresponding applications. This should change in the future. Either TandC should be much more user-friendly and accessible o A completely different model and consent system should be introduced, which is more similar to the direct management of health data.

In eHealth systems, data processing plays a different and more extensive role. The quantitative increase in data sets and calculation options is changing the landscape. In fact, the data collection not only reflects the organizational purposes of the structure, but directly affects the therapy, also due to the appearance of Artificial Intelligence as a possible “third actor” in the doctor-patient relationship (Maeckelberghe et al., 2019). In an e-health system, an individual's data, along with that of others, can be used to gain new knowledge, but the model has a direct impact on the health of the individual, as in the case of personalized medicine, and gives some recommendations of the individual according to statistically oriented risk assessments. In addition, an artificial intelligence system can provide support with diagnostic or intervention techniques, the risk of errors is important and the management of the possible consequences includes questions of responsibility that are also being registered in other areas of new technologies, from robotics to artificial intelligence. Usually (Johnson, 2015). As a result of this declaration, the new regulation no longer requires the consent of the subject and the prior consent of the authorities as in the previous system.

In fact, according to the RGPD, the treatment of health data for medical purposes has an independent legal basis, an alternative to consent, i.e. of the person concerned (as in the case of medical applications) or for other special reasons, for example if the treatment is necessary for medical treatment. In the case of therapy, for example, consent to processing is no longer required because the activity requires processing. With the exception of some “involuntary treatments” (medical treatments performed without the person's consent), the doctor-patient relationship is definitely based on informed consent, so that consent to data processing is in some way linked to stronger consent Therapy is linked to the framework of the doctor-patient relationship.

Consent to the use of invisible health data can of course not be given at the moment, as we are not yet aware of the nature of this data and its possible significance for health. By introducing a similar level of supervision for all types of data concerning a person (the GDPR is a step in that direction), safeguards will be put in place as soon as it turns out that seemingly completely harmless data can be used by artificial intelligence

technologies. Once this happens, alerts to dynamic consent systems are a useful precaution. Since the future use of the data is currently not foreseeable, warning mechanisms play a particularly important role, especially with derived health data and invisible health data.

2. How Indonesia Regulate Privacy And Protection Of Patient's Personal Data In Indonesia

a) Definition and Scope of eHealth in Indonesia

Formal definitions of eHealth can be found, among others, as proposed by World Health Organization (WHO), namely "the use of information and communication technologies (ICT) for health" to, for example, treat patients, pursue research, educate students, track diseases and monitor public health." Meanwhile, in KepMenKes Number 192/MENKES/SK/VI/2012 it is stated that eHealth is the use of ICT in the health sector, especially to improve health services. Referring to the definition of eHealth proposed by WHO above, eHealth includes comprehensively: comprehensively all government affairs related to health services such as: patient care, research and education in the health sector, disease control and general public health monitoring. In this context, the development and e-Health implementation in a country involves several key institutions, namely: Government (ranks of the Ministry and Health Service, Health Council), health service institutions (hospitals, clinics, and pharmacies), educational institutions, and health financing institutions such as insurance.

b) Privacy on personal data in the Law of Health

Privacy on personal data also stipulated in Law No. 36 of 2009 on Health, which stated in Article 57 that: "Everyone is entitled to its personal health conditions confidentiality that has been presented to health care providers." Article 47 (2) of Law No. 29 of 2004 on Medical Practice also states that: "Medical records referred to in paragraph (1) shall be stored and kept confidential by the physician or dentist and the management of health care facilities" Within the Indonesian legal system, the protection provided by the government to the citizens is aimed to protect the privacy on personal data of their medical history from any disclosure made by health care providers. Individual's medical history is a part of human dignity and cannot be disclosed without the patient's consent. In other words, health care providers are prohibited from disclosing any information about the patient to other third party.

c) Privacy and Protection Of Patient's Personal Data In Indonesia

Regarding the protection of personal data, Indonesia has regulated in Law Number 11 of 2008 namely the Electronic Information and Transaction Law in Article 26 paragraph (1) of the ITE Law which stipulates that: Unless stipulated otherwise by the Laws and Regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned. Against the party who is harmed by the violation of the provision, can file a lawsuit for the loss caused under the provisions of paragraph (2) the article.

Then in Government Regulation No. 82 of 2002 concerning the Operation of Electronic Systems and Transactions, personal data is regulated in Article 15 which regulates the responsibilities of electronic system operators who are obliged to maintain the confidentiality, integrity and availability of the personal data they manage and are obliged to ensure that acquisition, use and utilization of personal data must be based on the consent of the owner of the personal data and the use of the personal data must be in accordance with the purpose of data collection. There is also a failure in the protection of personal data, so the owner of personal data can notify the organizer of the electronic system. Regarding the protection of medical records of patients' personal data, Law Number 29 of 2004 concerning medical practice has regulated at a glance the protection of patients' medical records. Article 47 paragraph (2) of this law says: "Medical records as referred to in paragraph (1) must be kept and kept confidential by doctors or dentists and leaders of health service facilities".

Doctors or dentists have an obligation to store, maintain, and protect all information they know about their patients. This is as regulated in Article 57 Letter (c) of the law on medical practice, which reads ….he kept everything he knew about the patient a secret, even after the patient died. "The problem of leaking patient data is regulated in Article 79 point (c) of the Medical Practice Act which reads: "Criminalized with a maximum imprisonment of 1 (one) year or a fine at most Rp. 50,000,000.00 (fifty million rupiah), every doctor or dentist who: …. intentionally does not fulfil the obligations as referred to in Article 51 letter a, letter b, letter c, letter d, or letter e".

d) The Next Step eHealth in Indonesia

In terms of policy, the Government through the Ministry of Health has provided serious support in the development of eHealth. This support is stated in the Decree of the Minister of Health of the Republic of Indonesia No. 374/MENKES/SK/V/2009 concerning the National Health System (SKN), which was then followed by the Decree of the Minister of Health of the Republic of Indonesia No.192/MENKES/SK/VI/2012 concerning the Roadmap for the Action Plan for Strengthening the Indonesian Health Information System.

Within the SKN, there is a Health Information and Management Subsystem which is an order which collects various health administration efforts supported by data management and information, development and application of science and technology, as well as the regulation of health law in an integrated manner and support each other, in order to ensure the achievement of the highest degree of health. To elements of health information explained that the main form is the development of the system National Health Information that combines regional health information systems and systems other related information. The planned source of data is from health facilities through regular and tiered recording and reporting as well as from the community obtained from surveys, surveillance, and censuses.

To achieve the vision of Healthy Indonesia 2025, a Grand Design for Information System Reform has been prepared Health which is divided into three roadmaps:

a. Roadmap 2011-2014 which focuses on Strengthening the SIK Foundation from the side Regulations/Policies, Resources, and SIK Integration Process;
b. 2015-2019 Roadmap: continue, maintain/maintain and improve integration and strengthening of SIK;
c. Roadmap 2020-2024: continue, maintain/maintain and improve integration and strengthening of SIK.

Several applications have also been developed by the Ministry of Health for health services namely the SIK application for health facilities (SIKDA, *Puskesmas*, hospitals) and the SIK application for the Health Service (SIKDA and DHS2). SIKDA was developed as a generic application that can be utilized by all health offices in various districts or cities.

D. CONCLUSION

It is clear that the complexity and importance of this set of problems cannot be only managed by the self-regulation of private individuals, not because they pursue dark or illegal interests, but because the privately-owned enterprises cannot take on the framework of values, principles and rights we are dealing with. The appeal to the role of the public actors seems to be appropriate in the regulation of this sector. There are currently no definitive solutions. Therefore, the scientific and lawyer communities are called to a particular commitment: to define a new of the digital space. They should gain a specific role in the complex geometry of soft law instruments and try to translate the temporary results of the scientific research in concrete patterns that can be used by the community of professionals and programmers. Specific patterns could mean documents, practical management models, governance models for companies or deliverables as a result of collective projects. In the case of health, medicine, medical research and the protection of health data, this hypothesis requires the collaboration of scientists coming from different fields, from computer science to law, from bioethics to medicine.

In Indonesia even though eHealth has been regulated in several laws, Government Regulations and Ministerial Regulations such as Law Number 11 of 2008 concerning Information and Electronic Transactions, Law Number 29 of 2004 concerning Medical Practices, Law Number 36 of 2009 concerning Health, Regulation of the Minister of Health Number 269/Menkes/Per/III/2008, Government Regulation No. 82 of 2002 concerning Implementation of Electronic Systems and Transactions, but the regulations are very general and have not implemented specific personal data protection principles so that they cannot provide adequate protection. Maximum and consequently there are still personal data or medical records belonging to patients that can be easily accessed by other parties without the consent of the owner of the data concerned.

E. REFERENCES

Anan, K. A. (2004). *UNCTAD E-commerce and Development*. UNCTAD Report.

Bordel, B., Alcarria, R., Robles, T., & Martín, D. (2017). Cyber–Physical Systems: Extending Pervasive Sensing From Control Theory To The Internet of Things. *Pervasive and Mobile Computing*, *40*, 156–184. https://doi.org/https://doi.org/10.1016/j.pmcj.2017.06.011

C.F.G. Sunaryati Hartono. (1994). *Penelitian Hukum di Indonesia pada Akhir Abad Ke-20*. Alumni.

Cao, H., & Lin, M. (2017). Mining Smartphone Data For App Usage Prediction and Recommendations□: A Survey. *Pervasive and Mobile Computing*. https://doi.org/10.1016/j.pmcj.2017.01.007

Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and Consent in a World of Big Data. *International Data Privacy Law*, *3*(2), 67–73. https://doi.org/10.1093/idpl/ipt005

Connor, Y. O., Rowan, W., Lynch, L., Heavin, C., Connor, Y. O., Rowan, W., Lynch, L., & Heavin, C. (2017). ScienceDirect ScienceDirect Privacy by Design□: Informed Consent and Internet of Things for Privacy by Design□: Informed Consent Smart Health and Internet of Things for Smart Health. *Procedia Computer Science*, *113*, 653–658. https://doi.org/10.1016/j.procs.2017.08.329

Ian, J. L. (2014). *Information Technology Law*. Oxford University Pers.

Ienca, M., Ferretti, A., Hurst, S., Puhan, M., Lovis, C., & Vayena, E. (2018). Considerations for ethics review of big data health research: A scoping review. *PLoS ONE*, *13*(10), 1–15. https://doi.org/10.1371/journal.pone.0204937

Ioannidis, J. P. A. (2013). Informed Consent , Big Data , and the Oxymoron of Research That Is Not. *The American Journal of Bioethics*, *13*(4), 40–42. https://doi.org/10.1080/15265161.2013.768864

Johnson, D. G. (2015). Technology with No Human Responsibility□? *J Bus Ethics*, *127*. https://doi.org/10.1007/s10551-014-2180-1

Kaplan, B. (2016). How Should Health Data Be Used?: Privacy, Secondary Use, and Big Data Sales. *Cambridge Quarterly of Healthcare Ethics*, *25*(2), 312–329. https://doi.org/10.1017/S0963180115000614

Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H., & Melham, K. (2015). Dynamic consent□: a patient interface for twenty-first century research networks. *European Journal of Human Genetics*, *23*, 141–146. https://doi.org/10.1038/ejhg.2014.71

Lili Rasjidi. (2005). *Metode Penelitian Hukum, dalam Filsafat Ilmu, Metode Penelitian, dan Karya Tulis Ilmiah Hukum*. Monograf.

Maeckelberghe, E., Brall, C., & Schro, P. (2019). Ethical Aspects of Digital Health From a Justice Point of View. *European Journal of Public Health*, *29*(3), 18–22. https://doi.org/10.1093/eurpub/ckz167

Makarim, E. (2003). *Kompilasi Hukum Telematika*. Raja Grafindo Persada.

Mark F. Kightlinger, E. Jason Albert, and D. P. C. (2002). *International Privacy, Chapter 10,*. Privacy International.

Minh, T., Do, T., & Gatica-perez, D. (2013). Where and what□: Using Smartphones To Predict Next Locations and Applications in Daily Life. *Pervasive and Mobile Computing*. https://doi.org/10.1016/j.pmcj.2013.03.006

Mostert, M., Bredenoord, A. L., Biesaart, M. C. I. H., & Delden, J. J. M. Van. (2016). *Big Data in medical research and EU data protection law□: challenges to the consent or anonymise approach This paper has been amended since online publication and a corrigendum also appears in this issue . July 2015*, 956–960. https://doi.org/10.1038/ejhg.2015.239

Peate, I. (2013). Technology, Health and The Home: EHealth and The Community Nurse. *British Journal of Community Nursing*, *18*(5), 222–227. https://doi.org/10.12968/bjcn.2013.18.5.222

Ramon Alcarria, Borja Bordel, Tomás Robles, Diego Martín, M.-Á. M.-C. (2018). A Blockchain-Based Authorization System for Trustworthy Resource Monitoring and Trading in Smart Communities. *Sensors*, *18*(3561), 1–30. https://doi.org/10.3390/s18103561

Saeb, S., Zhang, M., Karr, C. J., Schueller, S. M., Corden, M. E., Kording, K. P., & Mohr, D. C. (2015). Mobile Phone Sensor Correlates of Depressive Symptom Severity in Daily-Life Behavior: An Exploratory Study. *J Med Internet Res*, *17*(7), e175. https://doi.org/10.2196/jmir.4273

Shaw, D. M., Gross, J. V, Erren, T. C., & Shaw, D. M. (2016). *Data donation after death A proposal to prevent the waste of medical research data*. *17*(1), 14–17.

Smith, J. B. & S. (2001). *The Globalization of World Politics, An Introduction to International Relation*. Oxford University Press.

Soerjono Soekanto. (1986). *Pengantar Penelitian Hukum*. UI Press.

Soerjono Soekanto & Sri Mamudji. (1986). *Penelitian Hukum Normatif*. Rajawali Press.

Timmons, S., Evans, C., & Nair, S. (2016). The Development Of The Nursing Profession in a Globalised Context: A Qualitative Case Study in Kerala, India. *Social Science and Medicine*, *166*, 41–48. https://doi.org/10.1016/j.socscimed.2016.08.012

Union, O. J. of the E. (2016). *Regulation (EU) 2016/679 Of The European Parliament And Of The Council* (No. 679; Vol. 2014, Issue April).

X, C. (2016). *The Internet of Things*. Palgrave Macmillan.