

July 2022

PERTANGGUNGJAWABAN HUKUM PENGELOLA SISTEM ELEKTRONIK KESEHATAN DI INDONESIA SEBAGAI PENYELENGGARA ELEKTRONIK SEHUBUNGAN DENGAN PERLINDUNGAN DATA

Jessy Annastasia Aruan
Universitas Indonesia, jessy.aruan@gmail.com

Follow this and additional works at: <https://scholarhub.ui.ac.id/dharmasisya>



Part of the [Health Law and Policy Commons](#), [Internet Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Aruan, Jessy Annastasia (2022) "PERTANGGUNGJAWABAN HUKUM PENGELOLA SISTEM ELEKTRONIK KESEHATAN DI INDONESIA SEBAGAI PENYELENGGARA ELEKTRONIK SEHUBUNGAN DENGAN PERLINDUNGAN DATA," *"Dharmasisya" Jurnal Program Magister Hukum FHUI*: Vol. 1, Article 20. Available at: <https://scholarhub.ui.ac.id/dharmasisya/vol1/iss4/20>

This Article is brought to you for free and open access by the Faculty of Law at UI Scholars Hub. It has been accepted for inclusion in "Dharmasisya" Jurnal Program Magister Hukum FHUI by an authorized editor of UI Scholars Hub.

PERTANGGUNGJAWABAN HUKUM PENGELOLA SISTEM ELEKTRONIK KESEHATAN DI INDONESIA SEBAGAI PENYELENGGARA ELEKTRONIK SEHUBUNGAN DENGAN PERLINDUNGAN DATA

Cover Page Footnote

Sutanto. 2010. Pengembangan Sistem Informasi Manajemen Puskesmas (SIMPUS). <http://sutanto.staff.uns.ac.id/files/2010/03/prop-simpus.pdf>. Diunduh pada tanggal 1 Maret 2019. Pasal 1 poin (1) Peraturan Presiden No. 72 Tahun 2012 tentang Sistem Kesehatan Nasional. Sabarinah, "Penguatan Evidence-Based Public Health Melalui Sistem Informasi Kesehatan Berbasis Komunitas: Gagasan Kontribusi Kegiatan MB-KM", dalam Pidato pada Upacara Pengukuhan sebagai Guru Tetap dalam Bidang Ilmu Biostatistik Fakultas Kesehatan Masyarakat Universitas Indonesia, Depok 27 Maret 2021. Ibid. Shinta Dewi, "Aspek Perlindungan Data Pribadi Menurut Hukum Internasional, Regional dan Nasional", Bandung: Rafika 2015, hlm. 12. Rudi Natamiharja, "Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN, Lampung: Fakultas Hukum Universitas Lampung. Shinta Dewi, "Aspek Perlindungan Data Pribadi Menurut Hukum Internasional, Regional dan Nasional", Bandung: Rafika 2015, hlm. 10. Edmon Makarim, Kompilasi Hukum Telematika, Jakarta, Radja Grafindo Persada Tahun 2003, hlm 150. General Data Protection Regulation, Article 4(1) Handbook on European Data Protection Law 2018 Edition, hlm 83 Miller, Roger Leroy dan Jentz Gaylord, "Law for E-Commerce, hlm. 233. Pasal 28 G (1) UUD 1945 : "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi". ASEAN Human Rights Declaration, Pasal 21 : "Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attack upon that person's honour and reputation. Every person has the right to the protection of the law against such interference or attacks". Indonesia, Undang-Undang Keterbukaan Informasi Publik, UU No. 14 Tahun 2008, LN No. 61 Tahun 2008, TLN 4846, Ps. 22 dan Ps. 42 ayat (1). Edmon Makarim, "Pengantar Hukum Telematika (Suatu Kompilasi Kajian), hlm. 181 Pasal 56 ayat (1) dan (2) UU Kesehatan: "(1) Setiap orang berhak menuntut ganti rugi terhadap seseorang, tenaga kesehatan, dan/atau penyelenggara kesehatan yang menimbulkan kerugian akibat kesalahan atau kelalaian dalam pelayanan kesehatan yang diterimanya; (2) Tuntutan ganti rugi sebagaimana dimaksud pada ayat (1) tidak berlaku bagi tenaga kesehatan yang melakukan tindakan penyelamatan nyawa atau pencegahan kecacatan seseorang dalam keadaan darurat". Indonesia, Peraturan Presiden tentang Sistem Kesehatan Nasional, Perpres No. 72 Tahun 2012, BN No. 167 Tahun 2012, Pasal 3. Ibid, Lampiran Poin F.5.d. nomor 381-382. Indonesia, Peraturan Pemerintah tentang Sistem Informasi Kesehatan, PP Nomor 46 Tahun 2014, Lembaran Negara No. 126, Tahun 2014, Pasal 1. Ibid, Penjelasan Pasal 26 Ibid, Pasal 22 Indonesia, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik, PP No. 71 Tahun 2019, Lembaran Negara No. 185, Pasal 1 angka 1, 8, dan 30. Ibid, Pasal 2 ayat (3) dan (4) Ibid, Pasal 2 ayat (5) Edmon Makarim, Tanggung Jawab Hukum Penyelenggara Sistem Elektronik, (Jakarta: Raja Grafindo Persada, 2010), hlm. 134. Edmon Makarim, Tanggung Jawab Hukum Penyelenggara Sistem Elektronik, (Jakarta: Raja Grafindo Persada, 2010), hlm. 319.

PERTANGGUNGJAWABAN HUKUM PENGELOLA SISTEM ELEKTRONIK KESEHATAN DI INDONESIA SEBAGAI PENYELENGGARA ELEKTRONIK SEHUBUNGAN DENGAN PERLINDUNGAN DATA

Jessy Annastasia Aruan

Fakultas Hukum Universitas Indonesia
Korespondensi: jessy.aruan@gmail.com

Abstrak

Masyarakat yang sehat akan meningkatkan kualitas suatu bangsa. Oleh karena itu suatu sistem kesehatan nasional yang terpadu dan terintegrasi untuk mengoptimalkan kesehatan masyarakat adalah hal yang diperlukan untuk menjaga agar masyarakat tetap produktif dan sehat. Sistem informasi kesehatan salah satu fungsinya adalah mengumpulkan data dari kesehatan dan sektor terkait lainnya, menganalisis data dan memastikan kualitas, relevansi dan ketepatan waktu secara keseluruhan, dan mengubah data menjadi informasi untuk pengambilan keputusan terkait kesehatan. Data kesehatan tidak saja mengandung kondisi kesehatan masyarakat namun juga akan mengandung data pribadi seseorang. Kebocoran data yang terjadi sebagian besar adalah karena adanya sistem keamanan elektronik yang kurang memadai sehingga oknum-oknum tertentu dapat mengintervensi sistem tersebut kemudian mencuri data serta menjual data pribadi tersebut untuk keuntungan pribadinya. Penulisan ini akan membahas dan menguraikan mengenai bagaimana tanggung jawab dari pengelola sistem elektronik kesehatan itu sendiri.

Kata Kunci: Sistem Informasi Kesehatan, Data Pribadi, Penyelenggara Sistem Elektronik Kesehatan

Abstract:

A healthy society will improve the quality of a nation. Therefore, an integrated and integrated national health system to optimize public health is necessary to keep the community productive and healthy. One of the functions of a health information system is to collect data from health and other related sectors, analyse the data and ensure its overall quality, relevance and timeliness, and transform the data into information for health-related decision making. Health data will not only contain public health conditions but will also contain a person's personal data. Data leaks that occur are mostly due to an inadequate electronic security system so that certain party can intervene in the system and then steal data and sell the personal data to personal gain. This article will describe how the responsibilities of the administrator of the health electronic system itself.

Keywords: Health Law and Policy | Internet Law | Science and Technology Law

I. PENDAHULUAN

Kesehatan masyarakat adalah hal yang utama dalam pembangunan suatu negara. Pembangunan suatu negara tidak hanya selalu terkait dengan pembangunan ekonomi tetapi perlu ditelaah juga terkait pembangunan kesehatan dari masyarakatnya itu sendiri. Ekonomi suatu negara dapat optimal apabila kesehatan masyarakatnya juga tergolong optimal. Dapat dikatakan suatu masyarakat yang sehat adalah aset bagi negaranya. Hal ini karena apabila orang atau masyarakat yang terkena penyakit akan menjadi ancaman bagi perkembangan ekonomi ataupun pembangunan negara tersebut. Sudah ada contoh kejadian yang terjadi akhir-akhir ini yaitu penyebaran Covid-19 yang mewabah di seluruh dunia telah memberikan implikasi atau dampak yang signifikan terhadap jalannya suatu negara terutama ekonomi. Mengambil contoh negara-negara di Asia, maka bisa dilihat GDP dari beberapa negara mengalami penurunan dan di sisi lain tingkat inflasi negara mengalami kenaikan.

Masyarakat yang sehat akan meningkatkan kualitas suatu bangsa. Misi strategi yang baru untuk menjadikan pembangunan nasional berwawasan kesehatan harus merupakan komitmen bagi seluruh pihak, sehingga dapat menggeser paradigma pembangunan kesehatan yang lama. Salah satu strategi untuk mencapai paradigma sehat adalah diupayakan adanya peningkatan pelayanan kesehatan bagi penduduk berpendapatan rendah, percepatan proses desentralisasi dan perubahan konsep pembiayaan, dengan tetap memperhatikan pada peningkatan kemampuan daerahnya sesuai dengan kewenangan yang diserahkan.¹

Keberhasilan pembangunan kesehatan dapat tercapai apabila negara memiliki kebijakan pembangunan kesehatan yang lebih dinamis dan proaktif serta mengikutsertakan tidak hanya Pemerintah namun juga pihak swasta dan komunitas masyarakat. Oleh karena itu suatu sistem kesehatan nasional yang terpadu dan terintegrasi untuk mengoptimalkan kesehatan masyarakat

¹ Sutanto. 2010. *Pengembangan Sistem Informasi Manajemen Puskesmas (SIMPUS)*. <http://sutanto.staff.uns.ac.id/files/2010/03/prop-simpus.pdf>. Diunduh pada tanggal 1 Maret 2019.

adalah hal yang diperlukan untuk menjaga agar masyarakat tetap produktif dan sehat.

Berdasarkan Peraturan Presiden Nomor 72 Tahun 2012 tentang Sistem Kesehatan Nasional maka yang disebut sebagai Sistem Kesehatan Nasional atau SKN adalah “pengelolaan kesehatan yang diselenggarakan oleh semua komponen bangsa Indonesia secara terpadu dan saling mendukung guna menjamin tercapainya derajat kesehatan masyarakat yang setinggi-tingginya”². Salah satu komponen yang penting dari Sistem Kesehatan Nasional adalah sistem informasi kesehatan, dimana komponen sistem informasi ini akan menopang proses pengambilan keputusan pada komponen lainnya.³

Fungsi utama dari sistem informasi kesehatan adalah: (i) pembuatan data, (ii) kompilasi, (iii) analisis dan sintesis, dan (iv) komunikasi dan penggunaan. Sistem informasi kesehatan mengumpulkan data dari kesehatan dan sektor terkait lainnya, menganalisis data dan memastikan kualitas, relevansi dan ketepatan waktu secara keseluruhan, dan mengubah data menjadi informasi untuk pengambilan keputusan terkait kesehatan. Data kesehatan bisa dihasilkan atau digunakan oleh banyak pihak, misalnya saja kementerian kesehatan, kantor statistik nasional, sektor tanggap darurat, sektor swasta, organisasi masyarakat sipil, donor, dan lembaga bantuan pembangunan. Oleh karena pengembangan sistem informasi kesehatan bukanlah ranah dari satu institusi atau bidang saja maka, diperlukan suatu rencana yang sifatnya komprehensif dan kolaboratif dalam mereformasi sistem informasi kesehatan.⁴

Menyadari bahwa data merupakan suatu hal yang penting, Pemerintah dalam hal ini Presiden Republik Indonesia juga telah mengeluarkan Peraturan Presiden No. 39 Tahun 2019 tentang Satu Data Indonesia, yang bertujuan untuk memastikan perolehan data yang akurat, mutakhir, terpadu, dan dapat dipertanggungjawabkan, mudah diakses, dan dibagikan. Di dalam Peraturan Presiden ini juga mengatur bahwa interoperabilitas menjadi suatu prinsip, yaitu data yang dihasilkan dari setiap Lembaga pemerintah (pusat atau daerah) harus memenuhi kaidah interoperabilitas data. Pasal 9 ayat (2) Peraturan Presiden ini juga mengatur bahwa data harus disimpan dalam format terbuka yang dapat dibaca sistem elektronik.

Perlu disadari bahwa data kesehatan tidak saja hanya mengandung kondisi kesehatan masyarakat namun juga akan mengandung data pribadi seseorang. Banyaknya kasus pencurian data pribadi memperlihatkan adanya tantangan- tantangan terkait perlindungan data pribadi di berbagai sektor, termasuk juga sektor kesehatan.

Berdasarkan latar belakang yang diuraikan di atas, maka yang menjadi pokok permasalahan dari penelitian ini adalah: i) Bagaimana perlindungan terhadap data pribadi dalam hukum positif Indonesia? dan ii) bagaimanakah tanggung jawab hukum pengelola sistem elektronik kesehatan sebagai penyelenggara sistem elektronik sehubungan dengan perlindungan data?

II. PEMBAHASAN

A. Perlindungan Data Pribadi Sebagai Hak Atas Privasi

Hak atas privasi adalah hak yang melekat pada setiap orang. Perlindungan terhadap privasi sebagai bagian dari penghormatan atas hak privasi (*the right of privacy*) diartikan sebagai hak untuk menikmati kehidupan dan hak untuk dihargai perasaan dan pikirannya.⁵ Dimana untuk memberikan perlindungan atas hak privasi tersebut tentu harus dimulai dengan adanya

² Pasal 1 poin (1) Peraturan Presiden No. 72 Tahun 2012 tentang Sistem Kesehatan Nasional.

³ Sabarinah, “Penguatan Evidence-Based Public Health Melalui Sistem Informasi Kesehatan Berbasis Komunitas: Gagasan Kontribusi Kegiatan MB-KMP”, dalam Pidato pada Upacara Pengukuhan sebagai Guru Tetap dalam Bidang Ilmu Biostatistik Fakultas Kesehatan Masyarakat Universitas Indonesia, Depok 27 Maret 2021

⁴ *Ibid.*

⁵ Shinta Dewi, “Aspek Perlindungan Data Pribadi Menurut Hukum Internasional, Regional dan Nasional”, Bandung: Rafika 2015, hlm. 12.

pemberian kepastian akan hukum.⁶ Hak atas privasi merupakan suatu hak asasi manusia yang sifatnya fundamental dan menjadi dasar timbulnya berbagai hak asasi – hak asasi manusia yang lain.

Konsep privasi pertama dikembangkan oleh Warren dan Brandeis dalam tulisannya di Jurnal Ilmiah dengan judul “*The Right to Privacy*” atau hak untuk tidak diganggu. Dalam jurnal tersebut dituliskan bahwa terdapat kesadaran masyarakat tentang hak untuk menikmati hidup, hal ini timbul karena adanya perkembangan dan kemajuan teknologi. Hak untuk menikmati hidup tersebut memiliki arti yaitu merupakan suatu hak bagi seseorang untuk tidak diganggu dalam kehidupan pribadi atau kehidupan sehari-harinya, baik oleh orang lain atau negara. Hukum menjadi berperan dalam pengakuan dan perlindungan hak privasi tersebut.⁷

Pengertian privasi bisa diinterpretasikan luas dan mempunyai batasan yang bermacam-macam tergantung dari sisi mana penilaiannya. Berdasarkan Kamus Besar Bahasa Indonesia, privasi memiliki arti bebas, kebebasan atau keleluasaan. Sedangkan pengertian privasi berdasarkan Black’s Law Dictionary adalah sebagai berikut:

“The right to be alone; the right of a person to be free from unwarranted public. Term right of privacy is generic term encompassing various rights recognized to be inherent in concept of ordered liberty and such rights prevents governmental interference in intimate personal relationship or activities, freedom of individual to make fundamental choices involving himself, his family and his relationship with others”.

Perlindungan privasi dan data pribadi merupakan hal yang saling terkait. Privasi selalu dikaitkan dengan hak asasi manusia dan data pribadi adalah terkait tentang akses atau proses data individu. Negara pertama yang pertama kali mengundang perlindungan data adalah negara bagian Hesse di Jerman yaitu pada tahun 1970, yang selanjutnya diikuti oleh negara Swedia pada tahun 1973 dan kemudian negara Amerika Serikat di tahun 1974 dan selanjutnya di negara Inggris pada tahun 1984.⁸ Data pribadi terdiri atas fakta, komunikasi atau pendapat atau data yang berkaitan dengan individu yang merupakan informasi yang sangat pribadi sehingga orang yang bersangkutan ingin menyimpan atau membatasi orang lain untuk mengoleksi, menggunakan atau menyebarkan kepada pihak lain. Menurut General Data Protection Regulation data pribadi itu didefinisikan sebagai berikut:⁹

“Personal data means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

Berdasarkan Article 4 (1) tersebut GDPR mendefinisikan data pribadi sebagai informasi yang berkaitan dengan seseorang (*natural person*) yang “sudah teridentifikasi”, atau yang “dapat diidentifikasi”. “sudah teridentifikasi” memiliki pengertian bahwa informasi tentang data pribadi sudah jelas nyata identitasnya, baik secara tidak langsung atau langsung, sehingga suatu data atau informasi akan merujuk kepada individu tersebut. Sedangkan yang dimaksud dengan “dapat diidentifikasi” adalah bahwa informasi tersebut dapat dibentuk dari informasi tambahan lainnya sehingga suatu data atau informasi akan merujuk pada individu, seperti nama, nomor identifikasi (Nomor Induk), alamat dan faktor lain seperti faktor fisik, psikis, *genetic*,

⁶ Rudi Natamiharja, “Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN, Lampung: Fakultas Hukum Universitas Lampung.

⁷ Shinta Dewi, “Aspek Perlindungan Data Pribadi Menurut Hukum Internasional, Regional dan Nasional”, Bandung: Rafika 2015, hlm. 10.

⁸ Edmon Makarim, Kompilasi Hukum Telematika, Jakarta, Radja Grafindo Persada Tahun 2003, hlm 150.

⁹ General Data Protection Regulation, Article 4(1)

mental, ekonomi, serta sosial budaya individu tersebut¹⁰

Perlu menjadi catatan bahwa setiap negara memiliki definisi yang berbeda yaitu antara penggunaan istilah informasi pribadi dan istilah data pribadi, namun secara substansi tetap sama. Di Indonesia kita menggunakan data pribadi sedangkan di Amerika Serikat dan Kanada menggunakan istilah informasi rahasia. Perlindungan hak privasi erat berkaitan dengan perlindungan data pribadi seseorang, hal ini berangkat dari kondisi perkembangan teknologi dalam dunia internet yang telah mengalami kemajuan pesat yang pada akhirnya membuat orang-orang dapat mengakses data pribadi orang lain tanpa sepengetahuan dan/atau seijin pihak pemilik data atau informasi¹¹

Sehubungan dengan hak privasi ini, Indonesia juga telah mengakui dalam undang-undang dasar negaranya yaitu dalam Pasal 28 G (1) yang menyatakan bahwa setiap orang berhak atas perlindungan atas diri pribadi serta berhak atas rasa aman.¹² Indonesia sebagai anggota dari *Association of South East Asian Nations* (ASEAN) juga telah menandatangani deklarasi hak asasi manusia yaitu *ASEAN Human Rights Declaration*, yang khususnya pada pasal 21 mengkonfirmasi adanya hak privasi sejalan dengan ketentuan atau deklarasi dalam *Universal Declaration of Human Rights*. Adapun pasal 21 tersebut pada intinya menyatakan bahwa setiap orang memiliki hak untuk bebas dari intervensi orang lain terhadap privasinya, termasuk data pribadinya, dimana seseorang tersebut memiliki hak untuk mendapatkan perlindungan hukum untuk setiap intervensi dan pelanggaran haknya.¹³

Pada Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, khususnya (UU HAM) pada pasal 14 menguraikan adanya perlindungan terkait informasi dan berkomunikasi, yaitu dengan menyatakan:

1. “setiap orang berhak untuk berkomunikasi dan memperoleh informasi yang diperlukan untuk mengembangkan pribadi dan lingkungan sosialnya”;
2. “setiap orang berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis sarana yang tersedia”.

Selain hak terkait informasi dan komunikasi tersebut maka dalam Pasal 21 UU HAM juga diatur bahwa dalam hal seseorang menjadi objek penelitian maka harus mendapatkan terlebih dahulu persetujuan dari orang bersangkutan. Berikut kutipannya:

“Setiap orang berhak atas keutuhan pribadi, baik rohani maupun jasmani dan karenanya tidak boleh menjadi obyek penelitian tanpa persetujuan darinya”

Dari Pasal 21 di atas dapat diinterpretasikan bahwa UU HAM mencoba menerapkan bahwa adalah hak asasi manusia untuk mendapatkan pemberitahuan dandengan persetujuan terlebih dahulu dalam hal privasinya akan di-intervensi oleh pihaklain.

Perangkat hukum lainnya yang dapat dijadikan rujukan terkait perlindunganprivasi ini adalah melalui Undang-Undang Nomor 23 Tahun 2006 tentang “Administrasi Kependudukan” (UU Adminduk) dan Undang-Undang No. 14 tahun 2008 tentang “Keterbukaan Informasi Publik” (UU KIP). Pada UU KIP yaitu pada Pasal 6 ayat (3) sudah jelas diatur bahwa “*informasi publik yang tidak dapat diberikan oleh suatu Badan Publik salah satunya adalah informasi yang berkaitan dengan hak-hak pribadi*”. Pasal 17 mengatur Informasi rahasia pribadi ini dikecualikan dalam hak untuk mendapatkan akses terhadap informasi publik. Sedangkan rahasia pribadi apa saja yang

¹⁰ Handbook on European Data Protection Law 2018 Edition, hlm 83

¹¹ Miller, Roger Leroy dan Jentz Gaylord, “Law for E-Commerce, hlm. 233.

¹² Pasal 28 G (1) UUD 1945 : “*Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi*”.

¹³ ASEAN Human Rights Declaration, Pasal 21 : “*Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attack upon that person’s honour and reputation. Every person has the right to the protection of the law against such interference or attacks*”.

dikecualikan adalah:¹⁴

- a. riwayat dan kondisi anggota keluarga;
- b. riwayat kondisi perawatan, pengobatan kesehatan fisik dan psikis seseorang;
- c. kondisi keuangan, aset, pendapatan dan rekening bank seseorang;
- d. hasil-hasil evaluasi sehubungan dengan kapabilitas, intelektualitas dan rekomendasi kemampuan seseorang, dan/atau
- e. catatan yang menyangkut pribadi seseorang yang berkaitan dengan kegiatan satuan Pendidikan formal atau satuan pendidikan nonformal.

Pada UU Adminduk, data pribadi sudah didefinisikan yaitu sebagai data perserorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya (Pasal 1 angka 22). Sedangkan dalam Pasal 2 UU Adminduk dinyatakan secara tegas bahwa setiap penduduk mempunyai hak untuk mendapatkan perlindungan atas data pribadinya. Lalu yang termasuk kategori sebagai data pribadi penduduk berdasarkan Pasal 84 UU Adminduk ini adalah sebagai berikut:

- a. Nomor Kartu Keluarga;
- b. Nomor Induk Kependudukan;
- c. Tanggal/bulan/tahun lahir;
- d. Keterangan tentang kecacatan fisik dan/atau mental
- e. Nomor Induk Kependudukan Ibu Kandung
- f. Nomor Induk Kependudukan ayah; dan
- g. Beberapa isi catatan peristiwa penting

Melihat pada Penjelasan Pasal 84 dan Pasal 1 butir 17 maka dapat diinterpretasikan pengertian dari “catatan peristiwa penting” adalah beberapa catatan mengenai data yang bersifat pribadi dan berkaitan dengan peristiwa penting yang perlu dilindungi yaitu mencakup peristiwa yang dialami seseorang antara lain perkawinan, perceraian, kelahiran, kematian, pengesahan anak, pengangkatan anak, pengakuan anak, perubahan nama seseorang, termasuk perubahan status kewarganegaraan seseorang.

Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi mengatur beberapa hal yang berkenaan dengan kerahasiaan informasi, yaitu kewajiban penyelenggara jasa telekomunikasi untuk merahasiakan informasi yang dikirim atau diterima oleh pengguna jasa telekomunikasi melalui jaringan telekomunikasi dan/atau jasa telekomunikasi yang diselenggarakan oleh penyelenggara jasa telekomunikasi. Setiap penyelenggara yang melanggar kewajiban tersebut akan diancam pidana penjara maksimal dua tahun dan atau denda maksimal Rp. 200.000.000,- (dua ratus juta Rupiah). Penyelenggara jasa telekomunikasi juga wajib menyimpan setiap informasi atau data yang dibutuhkan sehubungan dengan suatu proses peradilan atas tindak pidana tertentu dan yang sudah memiliki surat permintaan tertulis dari Kepala Kepolisian Republik Indonesia dan/atau Jaksa dan/atau penyidik, yaitu berupa tindakan yang diancam dengan pidana penjara selama lima tahun ke atas, seumur hidup atau mati.¹⁵

Undang-Undang Nomor 19 Tahun 2016 tentang “Informasi dan Transaksi Elektronik” (UU ITE) telah cukup menguraikan secara lengkap terkait ketentuan- ketentuan perlindungan data pribadi, data badan hukum dan data Pemerintah. UU ITE mengatur larangan adanya orang dengan cara apapun untuk membuka informasi milik orang lain dengan tujuan ataupun bahkan jika data yang sifatnya rahasia sampai dapat terbuka kepada publik. Pada intinya UU ITE mengatur setiap akses melalui sistem elektronik, dengan cara menerobos sistem pengamanan dan

¹⁴ Indonesia, *Undang-Undang Keterbukaan Informasi Publik*, UU No. 14 Tahun 2008, LN No. 61 Tahun 2008, TLN 4846, Ps. 22 dan Ps. 42 ayat (1).

¹⁵ Edmon Makarim, “Pengantar Hukum Telematika (Suatu Kompilasi Kajian), hlm. 181

dilakukan secara melawan hukum terhadap data seseorang yang bertujuan memperoleh informasi orang tersebut tanpa persetujuannya adalah dilarang. Perlindungan data tidak hanya mencakup pengaturan akses pembukaan data yang melawan hukum tetapi juga apabila data dibuka dan dimodifikasi dengan cara apapun sehingga seperti atau seolah-olah menjadi data otentik. Perlindungan data dalam UU ITE juga mengatur tentang larangan setiap tindakan yang dapat mengakibatkan sistem elektronik menjadi terganggu dan pada akhirnya mengakibatkan akses data oleh pemilik data menjadi terganggu. Dapat disimpulkan yaitu perlindungan data dalam UU ITE tidak hanya mencakup pada terbebasnya data untuk terbuka tanpa persetujuan pemilik data, namun juga dalam bentuk kewajiban pengamanan sistem elektronik dimana data tersebut diproses, disimpan dan digunakan agar dapat berjalan sesuai tujuan awal perolehannya.

Peraturan Menteri No. 20 Tahun 2016 tentang Perlindungan Data Pribadi (Permenkominfo No. 20) mengatur bahwa data pribadi yang diperoleh dan dikumpulkan secara langsung harus diverifikasi kepada pemilik data pribadi dan sumber data dalam perolehan dan pengumpulan data pribadi harus memiliki dasar hukum yang sah untuk menjamin otentikasi. Data Pribadi yang disimpan dalam penyelenggaraan sistem elektronik harus yang sudah di verifikasi dan harus dalam bentuk enkripsi meskipun tidak dijelaskan tingkatan dan model enkripsinya. Namun sayangnya Permenkominfo No. 20 ini belum menguraikan lebih lanjut terkait mekanisme verifikasi, otentikasi, enkripsi data dan jangka waktu minimal penyimpanan data

Perlindungan data pribadi juga sudah diatur dalam perangkat hukum di ranah kesehatan yaitu melalui Undang-Undang Nomor 23 Tahun 1992 dan telah diubah dengan Undang-Undang Nomor 36 Tahun 2009 tentang “Kesehatan” dan kemudian mengalami perubahan lagi sesuai Undang-Undang Nomor 11 Tahun 2020 (UU Kesehatan). Dalam UU Kesehatan disebutkan suatu istilah data kesehatan dan informasi kesehatan. Disebutkan dalam Pasal 8 juncto Pasal 56 ayat (1) UU Kesehatan:

“setiap orang berhak memperoleh tentang data kesehatan dirinya termasuk tindakan dan pengobatan yang telah atau maupun yang akan diterimanya dari tenaga kesehatan”.

“(1) setiap orang berhak menerima atau menolak sebagian atau seluruh tindakan pertolongan yang akan diberikan kepadanya setelah menerima dan memahami informasi mengenai tindakan tersebut secara lengkap”.

Dari kutipan di atas dapat diambil kesimpulan bahwa data kesehatan adalah terkait dengan data kesehatan dari diri seorang tersebut, yang merupakan hak dari orang tersebut sebelum mendapatkan pertolongan atau tindakan medis tertentu. Setiap data kesehatan yang diungkapkan kepada penyelenggara pelayanan kesehatan menjadi suatu yang bersifat rahasia, kecuali memang terdapat perintah dari pengadilan, berdasarkan suatu undang-undang, demi kepentingan umum, atau kepentingan orang itu sendiri atau memang sudah diizinkan oleh pemilik data kesehatan (Pasal 57 ayat

(1) dan (2) UU Kesehatan). Terkait pelanggaran atas kerahasiaan ini maka apabila secara umum diinterpretasikan dalam Pasal 58 UU Kesehatan, si pemilik data kesehatan dapat saja mengajukan gugatan ganti rugi apabila memang orang tersebut mengalami kerugian akibat kesalahan dan/atau kelainan dalam pelaksanaan hak kerahasiaan data kesehatan.¹⁶

B. Sistem Informasi Kesehatan Indonesia dan Penyelenggaraannya

Sistem Informasi Kesehatan merupakan salah satu bagian dari Sistem Kesehatan Nasional. Sistem Kesehatan Nasional sendiri terdiri dari: upaya kesehatan, penelitian dan

¹⁶ Pasal 56 ayat (1) dan (2) UU Kesehatan: *“(1) Setiap orang berhak menuntut ganti rugi terhadap seseorang, tenaga kesehatan, dan/atau penyelenggara kesehatan yang menimbulkan kerugian akibat kesalahan atau kelalaian dalam pelayanan kesehatan yang diterimanya; (2) Tuntutan ganti rugi sebagaimana dimaksud pada ayat (1) tidak berlaku bagi tenaga kesehatan yang melakukan tindakan penyelamatan nyawa atau pencegahan kecacatan seseorang dalam keadaan darurat”.*

pengembangan kesehatan, pembiayaan kesehatan, SDM, kesediaan farmasi alat kesehatan dan makanan, manajemen informasi dan regulasi kesehatan dan pemberdayaan masyarakat.¹⁷ Subsistem manajemen informasi dan regulasi kesehatan diselenggarakan agar dapat menghasilkan fungsi-fungsi antara lain informasi dan hukum kesehatan yang mema, suatu kebijakan dan administrasi, yang diharapkan dapat mendukung adanya penyelenggaraan upaya kesehatan secara maksimal.

Tujuan penyelenggaraan sistem informasi kesehatan sendiri adalah untuk menyediakan data dan informasi terkini, akurat, valid, cepat, transparan serta berhasilguna dan berdaya guna. Data dan informasi ini digunakan sebagai bahan pengambilan keputusan kesehatan dengan mempertimbangkan faktor desentralisasi, kecukupan data termasuk data terpilih yang responsif gender, dan aspek kerahasiaan yang berlaku di bidang kesehatan.¹⁸

Untuk sistem informasi kesehatan yang dapat mendukung pembangunan sistem kesehatan maka dibutuhkan sistem informasi kesehatan yang terintegrasi. Suatu sistem informasi kesehatan dikatakan terintegrasi apabila sistem tersebut memiliki mekanisme saling terhubung diantara satu subsistem informasi dengan subsistem informasi lainnya. Dimana dalam satu ekosistem data ini, setiap data yang ada dapat rutin mengalir dari satu sistem ke sistem yang lain, dalam hal ini integrasi data akan termasuk integrasi sistem secara teknis dan kontennya.

Dari sisi praktis maka fisik dari pelaksanaan integrasi sistem informasi kesehatan adalah melalui pembuatan aplikasi sistem informasi yang terhubung dengan aplikasi-aplikasi lain (misalnya aplikasi sistem informasi diantara rumah sakit, puskesmas- puskesmas, serta fasilitas kesehatan lainnya). Selain itu Sistem Informasi Kesehatan harus mampu interoperabilitas dan interkoneksi tidak hanya dengan subsistem informasi kesehatan tetapi dengan sistem informasi lainnya. Integrasi dari sistem informasi kesehatan harus mencakup setidaknya integrasi sistem informasi diantara fasilitas-fasilitas pelayanan kesehatan.

C. Keamanan dan Kerahasiaan Data dalam Sistem Informasi Kesehatan

Pengertian data kesehatan berdasarkan Peraturan Pemerintah Nomor 46 Tahun 2014 adalah “angka dan fakta kejadian berupa keterangan dan tanda-tanda yang secara relatif belum bermakna bagi pembangunan kesehatan”. Sedangkan untuk informasi kesehatan didefinisikan sebagai “Data Kesehatan yang telah diolah atau diproses menjadi bentuk yang mengandung nilai dan makna yang berguna untuk meningkatkan pengetahuan dalam mendukung pembangunan kesehatan”.¹⁹ Dalam pengelolaan suatu sistem informasi kesehatan, maka baik data atau informasi kesehatan harus terinci sekaligus terklasifikasi.

Adapun klasifikasi data kesehatan ada 2 macam yaitu data rutin dan data non rutin. Adapun perbedaan antara keduanya adalah data rutin akan dikumpulkan secara teratur oleh penyelenggara fasilitas pelayanan kesehatan, instansi Pemerintah Daerah dan Pemerintah Pusat melalui pencatatan dan pelaporan atau cara-cara lain. Sedangkan data non rutin dikumpulkan dalam waktu tertentu dan dilakukan sesuai kebutuhan dan prioritas dari program pembangunan kesehatan yang dijalankan oleh Pemerintah dari waktu ke waktu. Data Non Rutin ini terbagi menjadi dua yaitu: i) data khusus (yang meliputi data faktor risiko, lingkungan, dan lainnya yang mendukung program pembangunan kesehatan); dan ii) data luar biasa (data yang dikumpulkan dalam kejadian luar biasa, misalnya apabila dalam kondisi terjadi bencana, atau wabah, atau kondisi kedaruratan kesehatan di masyarakat).

¹⁷ Indonesia, *Peraturan Presiden tentang Sistem Kesehatan Nasional*, Perpres No. 72 Tahun 2012, BNNNo. 167 Tahun 2012, Pasal 3.

¹⁸ *Ibid*, Lampiran Poin F.5.d. nomor 381-382.

¹⁹ Indonesia, *Peraturan Pemerintah tentang Sistem Informasi Kesehatan*, PP Nomor 46 Tahun 2014, Lembaran Negara No. 126, Tahun 2014, Pasal 1.

Menurut pada ketentuan Peraturan Pemerintah Nomor 46 Tahun 2014 tentang “Sistem Informasi Kesehatan” maka sumber data dan informasi kesehatan dalam penyelenggaraan sistem informasi kesehatan adalah :

- i. Fasilitas kesehatan (baik milik Pemerintah maupun swasta), salah satunya diperoleh dari rekam medik (baik elektronik maupun non elektronik);
- ii. Masyarakat, baik perseorangan maupun kelompok, yang bisa diperoleh dari kegiatan penelitian, survei atau sensus, pelaporan, dan/atau kegiatan-kegiatan lain yang ditentukan oleh peraturan perundangan;
- iii. Instansi Pemerintah dan Pemerintah daerah terkait.

Pemerintah melalui Peraturan Pemerintah No. 46 Tahun 2014 tentang “Sistem Informasi Kesehatan” mengakui pentingnya menjaga kerahasiaan data dan informasi kesehatan, dimana disebutkan bahwa untuk menjaga keamanan dan kerahasiaan informasi kesehatan:

- a. Pemerintah Pusat, dalam hal ini Menteri Kesehatan, akan menetapkan kriteria atau persyaratan dan batasan hak akses bagi para pengguna informasi kesehatan;
- b. Adanya kewajiban dari pengelola informasi kesehatan yaitu melakukan pemeliharaan, penyimpanan, dan penyediaan cadangan data dan informasi kesehatan secara baik dan teratur, serta membuat suatu mekanisme pencegahan kerusakan data dan informasi kesehatan.

Dikatakan dalam peraturan yang sama, perihal kerahasiaan informasi kesehatan dan standar pengamanan sesuai dengan ketentuan peraturan perundangan, dimana dalam penjelasan pasal 25 Peraturan Pemerintah No. 46 Tahun 2014 tentang Sistem Informasi Kesehatan menjelaskan bahwa keamanan dan kerahasiaan Informasi Kesehatan akan merujuk kepada *National Cyber Security* (NCS) Indonesia.

D. Penyelenggara Sistem Informasi Kesehatan Indonesia

Merujuk pada ketentuan yang diatur dalam Pasal 26 Peraturan Pemerintah Nomor 46 Tahun 2014 tentang “Sistem Informasi Kesehatan” maka disebutkan bahwa pengelolaan sistem informasi kesehatan akan dilakukan oleh:

- a. Pemerintah sehubungan dengan pengelolaan Sistem Informasi Kesehatan ditingkat nasional dalam ruang lingkup Sistem Kesehatan Nasional;
- b. Pemerintah Daerah provinsi, sehubungan dengan pengelolaan satu Sistem Informasi Kesehatan di tingkat provinsi;
- c. Pemerintah Daerah kabupaten/kota, sehubungan dengan pengelolaan satu Sistem Informasi Kesehatan di tingkat kabupaten/kota; dan
- d. Fasilitas Pelayanan Kesehatan, sehubungan dengan pengelolaan Sistem Informasi Kesehatan di tingkat fasilitas pelayanan kesehatan.

Pengelola Sistem Informasi Kesehatan di atas memiliki tanggung jawab untuk mengembangkan dan mengelola sistem informasi kesehatan sesuai dengan fungsi dan tugasnya dari masing-masing Lembaga atau institusi, termasuk ketersediaan akses terhadap Informasi Kesehatan dalam upaya meningkatkan derajat kesehatan masyarakat. Tanggung jawab pengelolaan sistem informasi kesehatan juga mencakup kewajiban untuk memastikan keamanan dan keandalan sistem yang digunakan termasuk perlindungan terhadap kerahasiaan data yang dimiliki serta pengaturan pembatasan akses terhadap data-data yang bersifat pribadi dan rahasia.²⁰

Sehubungan dengan data dan informasi kesehatan, maka tanggung jawab Pengelola antara lain:

- a. Mengumpulkan, mengolah/memproses, menyimpan, dan menyajikan informasi kesehatan;
- b. Bertanggung jawab atas pengembangan dan pengelolaan sistem elektronik kesehatan dalam

²⁰ *Ibid*, Penjelasan Pasal 26

pelaksanaan pemrosesan data kesehatan;

- c. Menjaga keamanan dan kerahasiaan data dan informasi kesehatan.

Sesuai dengan Pasal 22 Peraturan Pemerintah Nomor 46 Tahun 2014 tentang “Sistem Informasi Kesehatan” untuk kegiatan penyimpanan data, pengelola sistem informasi kesehatan diberikan hak untuk menunjuk pihak ketiga dalam negeri untuk mendapatkan jasa dan fasilitas sehubungan dengan penyimpanan data tersebut, dengan syarat:²¹

- a. pemilik Data dan Informasi Kesehatan yang disimpan tersebut tidak dapat melepaskan tanggung jawab atas kerahasiaan informasi;
- b. pemilik Data dan Informasi Kesehatan wajib menyampaikan laporan penyimpanan Data dan Informasi Kesehatan tersebut kepada Menteri;
- c. harus dilakukan sesuai dengan ketentuan peraturan perundang-undangan terkait aksesibilitas arsip.

Istilah pemilik data dan informasi kesehatan ini merujuk pada pengelola sistem informasi kesehatan. Dalam hal demikian, maka tanggung jawab terkait kerahasiaannya tetap menjadi tanggung jawab dari si pengelola.

Melihat pada ketentuan-ketentuan dalam Peraturan Pemerintah Nomor 46 Tahun 2014 tentang “Sistem Informasi Kesehatan”, setiap pengelola Informasi Kesehatan bertanggung jawab atas setiap kegiatan pengumpulan, pengolahan, penyimpanan, akses keterbukaan/diseminasi, sampai dengan keamanan dan kerahasiaan data dan informasi. Dengan demikian dapat diambil kesimpulan yaitu setiap pengelola sistem informasi kesehatan adalah pihak yang melakukan tindakan pemrosesan data secara keseluruhan. Diselaraskan dengan ketentuan *controller* dan *processor* pada ketentuan GDPR, maka dalam konteks pengembangan sistem informasi kesehatan ini pengelola sistem informasi kesehatan adalah pihak *controller* sedangkan pihak ketiga yang bekerjasama dengan pengelola adalah sebagai *processor*.

E. Tanggung Jawab Pengelola Sistem Elektronik Kesehatan dalam kaitannya dengan Penyelenggaraan Sistem Elektronik

Pengolahan data dan informasi kesehatan dalam penyelenggaraan Sistem Informasi Kesehatan di Indonesia akan diselenggarakan melalui penggunaan sistem elektronik kesehatan, dimana pengolahan yang dimaksud meliputi pemrosesan, analisis, dan penyajian. Oleh karena itu Penulis merasa perlu untuk menguraikan terlebih dahulu terkait tanggung jawab penyelenggara sistem elektronik untuk melihat apakah pengelola sistem informasi kesehatan dapat dikategorikan sebagai penyelenggara sistem elektronik dan memiliki tanggung jawab hukum yang sama dengan penyelenggara sistem elektronik yang ditetapkan dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PPPSE).

Melihat pada definisi “Sistem Elektronik” dalam PP PSE maka yang dimaksud dengan “Sistem Elektronik” adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik. Dimana informasi elektronik adalah satu atau sekumpulan data berbentuk elektronik yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.²²

Penyelenggaraan sistem informasi kesehatan mencakup kegiatan-kegiatan pengumpulan, pengolahan, analisis, menyimpan dan menyebarkan data dan informasi kesehatan, dimana pengolahannya tersebut akan menggunakan sistem elektronik. Dalam hal demikian

²¹ *Ibid*, Pasal 22

²² Indonesia, *Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik*, PP No.71 Tahun 2019, Lembaran Negara No. 185, Pasal 1 angka 1, 8, dan 30.

maka penyelenggaraan sistem informasi kesehatan melalui sistem elektronik atau disebut juga sistem elektronik kesehatan akan masuk dalam ranah penyelenggaraan sistem elektronik berdasarkan PP PSE.

Istilah “penyelenggara sistem elektronik” didefinisikan dalam ketentuan Pasal 1 angka 6a Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang “Informasi dan Transaksi Elektronik” yang berbunyi:

“Penyelenggara Sistem Elektronik adalah setiap orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain”

Penyelenggaraan sistem elektronik dapat dilaksanakan oleh:

- a. penyelenggara sistem elektronik lingkup publik; dan
- b. penyelenggara sistem elektronik lingkup privat.

Penyelenggara sistem elektronik lingkup publik adalah instansi penyelenggara negara atau institusi yang ditunjuk oleh instansi penyelenggara negara (instansi yang melaksanakan penyelenggaraan sistem elektronik atas nama instansi yang menunjuk).²³ Adapun pengertian instansi penyelenggara negara adalah sebagai institusi di tingkat pusat dan daerah (legislatif, eksekutif, dan yudikatif) serta instansi lain yang diamanatkan melalui peraturan perundang-undangan, namun tidak termasuk otoritas pengatur dan pengawas sektor keuangan.

Di sisi lain, penyelenggara sistem elektronik lingkup privat adalah orang, badan usaha, dan masyarakat, yang meliputi:²⁴

- a. Penyelenggara Sistem Elektronik yang diatur atau diawasi oleh Kementerian atau Lembaga berdasarkan ketentuan peraturan perundang-undangan; dan
- b. Penyelenggara sistem elektronik yang memiliki portal, situs, atau aplikasi dalam jaringan melalui internet.

Dari uraian di atas, maka dapat disimpulkan pengelola sistem elektronik kesehatan dapat dikategorikan sebagai penyelenggara sistem elektronik, dengan alasan sebagai berikut:

- a. Baik instansi Pemerintah di tingkat Pusat maupun Daerah yang menjalankan sistem elektronik kesehatan dapat dikategorikan sebagai penyelenggara sistem elektronik lingkup publik.
- b. Fasilitas Pelayanan Kesehatan, baik publik maupun swasta dapat dikategorikan sebagai penyelenggara sistem elektronik lingkup privat karena memenuhi salah satu atau lebih kualifikasi di bawah ini:
 - Penyelenggaraan pelayanan kesehatan diatur dan diawasi oleh Kementerian (dalam hal ini Kementerian Kesehatan) berdasarkan peraturan (rumah sakit dan puskesmas);
 - Memiliki portal/situs/aplikasi dalam jaringan internet dalam mengoperasikan dan/atau menawarkan jasa (rumah sakit, laboratorium, puskesmas);
 - Memiliki portal/situs/aplikasi dalam jaringan internet yang memproses data pribadi untuk operasional pelayanan masyarakat yang terkait dengan kegiatan transaksi elektronik (misal pendaftaran rumah sakit dan laboratorium)

Sesuai dengan ketentuan yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang “Informasi dan Transaksi Elektronik”, maka suatu sistem harus diselenggarakan secara handal, aman dan bertanggung jawab serta harus dapat dijamin berjalan sebagaimana mestinya. Sehubungan dengan unsur keamanan data maka penyelenggara diwajibkan untuk selalu menjaga sistem pengamanan dari sistem elektroniknya. Dengan kata lain, perlu diketahui sejauh

²³ *Ibid*, Pasal 2 ayat (3) dan (4)

²⁴ *Ibid*, Pasal 2 ayat (5)

mana sistem pengamannya (*security system*) berjalan, dengan pertimbangan bahwa keutuhan informasi dan/atausistem itu sendiri dari sisi teknis sangatlah rentan untuk dapat diubah-ubah ataupun diterobos oleh pihak lain ataupun sistem-nya sendiri tidak bekerja sebagaimana mestinya,²⁵

Melihat pada uraian di atas maka dapat disimpulkan penyelenggaraan sistem elektronik kesehatan termasuk dalam ranah penyelenggaraan sistem elektronik berdasarkan PP PSE, dan pengelola sistem elektronik kesehatan dikategorikan sebagai penyelenggara sistem elektronik. Dengan demikian Penulis menarik kesimpulan standar yang diterapkan dalam penyelenggaraan sistem elektronik PP PSE dan peraturan pelaksana dan peraturan terkait lainnya juga harus diterapkan padapenyelenggaraan sistem elektronik kesehatan di Indonesia.

Pada bagian di bawah ini Penulis akan menguraikan mengenai standar pelaksanaan yang perlu dipenuhi oleh pengelola sistem elektronik kesehatan wajib untuk melakukan pendaftaran, pendaftaran ini diajukan kepada Kementerian Komunikasi dan Informatika sesuai dengan ketentuan perundangan, Selain itu dalam menjalankan penyelenggaraan sistem elektronik kesehatan, maka pengelola sistem elektronik kesehatan harus memberikan jaminan sebagai berikut:

- i. memiliki dan menjamin ketersediaan perjanjian tingkat Layanan (SLA);
- ii. memiliki perjanjian keamanan informasi dengan jasa layanan teknologi informasi yang digunakan; dan
- iii. memiliki pedoman keamanan informasi dan sarana komunikasi internal.

Komitmen yang harus dipenuhi oleh pengelola sistem elektronik kesehatan sebagai penyelenggara sistem elektronik berdasarkan ketentuan PP PSE, antara lain:

- i. Menerapkan manajemen resiko terhadap kerusakan atau kerugian yang ditimbulkan;
- ii. Memiliki prosedur kerja pengoperasian (serta tata kelola), dan mekanisme audit yang dijalankan secara berkala terhadap sistem elektronik yang bersangkutan;
- iii. Melaksanakan perlindungan data pribadi dalam melakukan pemrosesan data pribadi, dengan prinsip sebagai berikut: (a) terbatas dan spesifik; (b) sesuai dengan tujuannya; (c) menjamin hak pemilik data pribadi; (d) akurat; (e) melindungi keamanan data pribadi; (f) memberitahukan tujuan dan aktivitas pemrosesan serta kegagalan perlindungan data pribadi; (g) penghapusan/retensi; (h) akuntabel.
- iv. Menghapus informasi atau dokumen elektronik yang tidak relevan, serta menyediakan mekanisme penghapusan informasi dan/atau dokumen elektronik yang sudah tidak relevan. Dalam konteks data dan informasi kesehatan elektronik, maka perlu menjadi catatan periode penyimpanan adalah paling singkat 25 tahun.
- v. Memiliki rencana keberlangsungan kegiatan untuk menanggulangi gangguan atau bencana sesuai dengan resiko dari dampak yang ditimbulkan.
- vi. Tidak melakukan pemrosesan data di luar wilayah Indonesia dan hanya melakukan pemrosesan di wilayah Indonesia. Dalam hal dilakukan di luar wilayah Indonesia, maka sejumlah persyaratan harus dipenuhi.

Selain itu, sesuai dengan Pasal 9 Peraturan Kementerian Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang “Penyelenggara Sistem Elektronik Lingkup Privat”, ada beberapa komitmen tata kelola dan moderasi informasi dan/atau dokumen elektronik yaitu:

- i. pertanggungjawaban atas penyelenggaraan sistem elektronik dan pengelolaan informasi elektronik dan/atau dokumen elektronik di dalam sistem elektronik secara andal, aman, dan bertanggung jawab;
- ii. penyediaan pedoman penggunaan layanan dalam bahasa Indonesia sesuai dengan

²⁵ Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*, (Jakarta: Raja Grafindo Persada, 2010), hlm. 134.

- ketentuan perundang-undangan;
- iii. memastikan sistem elektroniknya tidak akan memuat informasi dan/atau dokumen elektronik yang dilarang; serta tidak memfasilitasi adanya penyebarluasan informasi dan/atau dokumen elektronik yang dilarang tersebut. Sebagai penyelenggara sistem elektronik, maka pengelola sistem elektronik kesehatan wajib menjamin keamanan keamanan informasi dan sarana komunikasi internal yang diselenggarakan. Realisasi atas komitmen tersebut, maka pengelola sistem elektronik kesehatan wajib:
 - iv. Memiliki pedoman dan prosedur serta menjalankannya, termasuk memiliki sarana untuk pengamanan sistem elektronik untuk menghindari gangguan, kegagalan, dan kerugian;
 - v. Menyediakan sistem pengamanan yang mencakup prosedur dan pedoman sistem pencegahan serta penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian;
 - vi. segera melaporkan dalam kesempatan pertama kepada aparat penegak hukum dan Kementerian atau Lembaga terkait. Apabila terjadi gangguan sistem yang memiliki dampak serius sebagai akibat adanya perbuatan dari pihak lain terhadap Sistem Elektronik;
 - vii. selalu menjaga kerahasiaan, keutuhan, ketersediaan, dan kemampuan untuk penelusuran suatu informasi elektronik dan/ atau dokumen elektronik;
 - viii. melakukan edukasi tidak hanya kepada Pengguna Sistem Elektronik, termasuk juga melatih karyawan atau petugas yang ditunjuk dan yang memiliki tanggung jawab terhadap pengamanan sistem elektronik;
 - ix. menyediakan desain-desain tertentu sesuai dengan karakteristik sistem elektronik yang digunakannya;
 - x. menyampaikan informasi kepada pengguna sistem elektronik paling sedikit mengenai: identitas Penyelenggara Sistem Elektronik; objek yang ditransaksikan; kelaikan atau keamanan Sistem Elektronik; tata cara penggunaan perangkat; syarat kontrak; prosedur mencapai kesepakatan; jaminan privasi dan/atau perlindungan Data Pribadi; dan nomor telepon pusat pengaduan.
 - xi. mengamankan dan melindungi sarana dan prasarana sistem elektronik atau informasi yang disalurkan melalui sistem elektronik;
 - xii. melakukan uji kelaikan sistem elektronik; dan
 - xiii. mendapatkan sertifikasi elektronik atas sistem elektroniknya.

Sebagaimana diamanatkan dalam PP PSE dan yang telah diuraikan di atas bahwa penyelenggara sistem elektronik wajib memiliki sistem pengamanan, maka pengelola sistem elektronik kesehatan juga perlu menerapkan manajemen pengamanan informasi berdasarkan asas risiko atau dikenal dengan istilah Sistem Manajemen Pengamanan Informasi (SMPI), dengan merujuk pada ketentuan ketentuan di dalam Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang “Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik”.

Untuk melihat pada tanggung jawab hukum pengelola sistem elektronik dalam kaitannya dengan perlindungan data, maka perlu menjadi perhatian adalah siapa yang menjadi subjek dan objek dari tanggung jawab hukum ini. Dari sisi subjek hukum maka dari uraian-uraian yang disampaikan dalam bab-bab sebelumnya maka subjeknya adalah para pengelola sistem informasi kesehatan yaitu fasilitas kesehatan (baik swasta maupun pemerintah) dan Pemerintah (baik tingkat Pusat maupun daerah) yang memang melakukan pengelolaan data kesehatan dan informasi kesehatan, terutama yang memiliki peran sebagai *controller* atau pengendali (dalam konteks memang data yang diproses adalah data pribadi). Sedangkan yang menjadi obyek adalah perlindungan data kesehatan dan informasi kesehatan terutama data pribadi. Data pribadi disini menurut penulis tidak hanya data yang dapat meng-identifikasi pribadi seseorang tapi juga termasuk data-data yang sifatnya sensitif yaitu mengenaikondisi

kesehatan atau perawatan yang diberikan kepada pemilik data tersebut. Sebagaimana diuraikan sebelumnya maka data kesehatan melihat pada sumber datanya akan mengandung suatu data pribadi baik dari pasien ataupun masyarakat.

Setelah melihat pada subjek dan objek dari tanggung jawab hukum ini, maka berikutnya Penulis akan menguraikan bagaimanakah bentuk tanggung jawab hukum itu dalam pengertian implikasi atau sanksi terhadap penyelenggara sistem elektronik kesehatan yang melakukan pelanggaran perlindungan keamanan dan kerahasiaan data dengan melihat pada ketentuan dalam peraturan perundang-undangan yang berlaku.

Berdasarkan peraturan perundangan di sektor kesehatan yaitu UU Kesehatan, Undang-Undang No. 36 Tahun 2012 tentang “Rahasia Kedokteran”, Undang-Undang No. 29 Tahun 2004 tentang “Praktik Kedokteran”, Undang-Undang No. 44 Tahun 2009 tentang “Rumah Sakit”, Peraturan Pemerintah Nomor 46 Tahun 2014 tentang “Sistem Informasi Kesehatan” dan Peraturan Menteri Kesehatan No. 269/MENKES/PER/III/2008 tentang “Rekam Medis”, Peraturan Menteri Kesehatan No. 1171/MENKES/PER/VI/2011 Tahun 2011 tentang Sistem Informasi Rumah Sakit dan Peraturan Menteri Kesehatan No. 31 Tahun 2019 tentang Sistem Informasi Puskesmas, maka Penulis melihat bahwa:

- a. Jenis data-data yang diatur dalam peraturan tersebut adalah terkait rekam medis, rahasia kedokteran, data kesehatan dan informasi kesehatan, Dimana rahasia kedokteran itu adalah identitas pasien, kesehatan pasien meliputi hasil pemeriksaan fisik, penunjang, diagnosis, pengobatan dan/atau tindakan kedokteran.
- b. Secara eksplisit, maka peraturan-peraturan tersebut mengatur subyek yang memiliki kewajiban atas perlindungan data adalah dokter dan fasilitas pelayanan kesehatan, termasuk pengelola sistem informasi kesehatan dalam hal ini Pemerintah Pusat dan Pemerintah Daerah.
- c. Secara umum terkait pelanggaran perlindungan keamanan dan kerahasiaan data, maka sanksi yang diberikan berdasarkan peraturan-peraturan di sektor kesehatan ini hanya terdapat sanksi administratif baik berupa teguran, pembekuan ijin, dan pencabutan ijin, dan tidak ada pengaturan pengenaan sanksi pidana atas pelanggaran perlindungan keamanan dan kerahasiaan data.
- d. Selain sanksi di atas maka ada hak gugat yaitu berdasarkan UU Kesehatan maka setiap orang berhak untuk mengajukan tuntutan ganti rugi akibat kesalahan atau kelalaian dalam pelayanan kesehatan, dimana kesalahan ini termasuk tindakan pembocoran rahasia kedokteran.
- e. Hal lain bisa menjadi catatan adalah adanya ketentuan yang diatur dalam Pasal 29 Peraturan Pemerintah Nomor 46 Tahun 2014 tentang “Sistem Informasi Kesehatan” yaitu dalam hal terjadi manipulasi data/informasi termasuk membocorkan data/informasi dapat dikenakan sanksi sesuai peraturan perundang-undangan. Berkaitan dengan hal ini masih menjadi pertanyaan apakah sanksi tersebut dapat dihubungkan dengan ketentuan peraturan dari sektor non kesehatan yaitu seperti melalui UU ITE.

Sedangkan melihat pada peraturan-peraturan di sektor lain selain kesehatan sehubungan dengan kewajiban perlindungan keamanan dan kerahasiaan data oleh penyelenggara sistem elektronik kesehatan, yaitu dari UU ITE, PP PSE, Peraturan Menteri No. 20 Tahun 2016 tentang “Perlindungan Data Pribadi”, Peraturan Kementerian Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang “Penyelenggara Sistem Elektronik Lingkup Privat”, dan Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang “Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik”, maka Penulis melihat bahwa:

- a. data yang menjadi obyek pengaturan dalam peraturan-peraturan yang disebut di atas adalah terkait data pribadi. Pengertian data pribadi adalah setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi (secara langsung atau tidak langsung) dari

masing-masing individu, yang disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiaannya.

- b. subyek yang memiliki kewajiban hukum berdasarkan peraturan-peraturan tersebut adalah penyelenggara sistem elektronik, baik dalam lingkup privat maupun publik. Yang menjadi catatan dari Penulis adalah saat penulisan ini dibuat maka peraturan menteri terkait penyelenggaraan sistem elektronik lingkup publik masih dalam proses penyusunan oleh Kementerian Komunikasi dan Informasi.
- c. bentuk sanksi yang diatur dalam peraturan adalah berupa sanksi administratif, baik berupa teguran, pembekuan atau pencabutan ijin dan/atau sertifikasi kegiatan operasional dari penyelenggara sistem elektronik. Penulis tidak menemukan adanya sanksi pidana terhadap pelanggaran kewajiban hukum terkait perlindungan keamanan dan kerahasiaan data.
- d. Dapat dijadikan catatan juga bahwa dalam berdasarkan pada UU ITE maka seseorang diberikan hak untuk mengajukan gugatan perdata kepada penyelenggara sistem elektronik yang menimbulkan kerugian bagi orang yang bersangkutan.

Sampai dengan saat ini belum ada peraturan khusus setingkat undang-undang yang mengatur mengenai perlindungan data pribadi, dan hanya baru terdapat Rancangan Undang-Undang Perlindungan Data Pribadi, dimana ketentuan tanggungjawab hukum dalam bentuk yang sanksi, maka Penulis menemukan bahwa:

- a. Yang menjadi obyek dari peraturan ini adalah data pribadi, dengan subyek hukumnya adalah pengendali data pribadi (*controller*). Pengertian pengendali adalah pihak yang menentukan tujuan dan melakukan kendali pemrosesan data pribadi.
- b. Sanksi administratif diberikan dalam bentuk teguran, penghentian sementara pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, ganti kerugian, dan denda untuk pelanggaran kewajiban-kewajiban sehubungan perlindungan kerahasiaan dan keamanan data pribadi.
- c. Diatur mengenai sanksi pidana yaitu untuk tindakan pemrosesan data pribadi yang dilakukan secara melawan hukum.

Merujuk pada teori tentang tanggung jawab hukum dan melihat penerapannya sehubungan dengan penyelenggaraan sistem elektronik kesehatan dalam konteks sistem kesehatan nasional, maka dalam sub-bab ini Penulis akan menguraikan mengenai tanggung jawab hukum dari pengelola sistem elektronik kesehatan.

Sebagai pengelola sistem elektronik kesehatan dimana kegiatannya adalah mengelola data dan/atau informasi kesehatan sehingga pada akhirnya informasi kesehatan tersebut dapat dipergunakan sebagai alat/tools untuk mengambil keputusan, maka tanggung jawab tersebut ditujukan kepada si pengguna informasi kesehatan, baik masyarakat dalam menentukan keputusan terkait kesehatannya atau Pemerintah dalam konteks pembuatan kebijakan serta peraturan perundangan.

Untuk menjaga mutu penyelenggaraan jasanya, maka penyelenggara sistem elektronik memiliki tanggung jawab untuk memastikan penyediaan jasanya dapat sesuai dengan standar yang berlaku lazim dalam komunitasnya (dalam ini sehubungan dengan penyelenggaraan sistem elektronik), termasuk juga untuk menyesuaikan penyediaan jasa dan output dari jasanya tersebut sesuai dan tidak melanggar pedoman atau peraturan pemerintah yang merupakan patokan dalam melakukan upaya yang terbaik dan untuk menjaga mutu penyelenggaraan jasanya. Sedangkan tanggung jawab si penyelenggara sistem elektronik sehubungan dengan kerugian yang timbul karena ada kesalahan dari si penyelenggara adalah sebenarnya mutlak, namun dapat berubah menjadi terbatas (pembatasan tanggung jawab), jika suatu mekanisme tertentu yang menjadi ukuran dalam "*best practice*".²⁶

²⁶ Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*, (Jakarta: Raja Grafindo Persada, 2010), hlm. 319.

Oleh karena itu, adalah tanggung jawab dari pengelola sistem elektronik kesehatan untuk mematuhi tidak saja ketentuan hukum dari sektor kesehatan namun juga wajib mematuhi standar yang berlaku di sektor teknologi informasi dan komunikasi, termasuk memperhatikan pedoman-pedoman yang berlaku secara internasional yang berkaitan dengan penyelenggaraan sistem informasi kesehatan itu sendiri. Misalnya adalah ketentuan terkait perlindungan data pribadi dan pedoman pemrosesan data pribadi yang berlaku secara internasional.

III. KESIMPULAN

Berdasarkan hasil pembahasan maka dapat diambil kesimpulan bahwa:

1. Data pribadi sebagai hak privasi yang melekat kepada seseorang, menjadi penting untuk diberikan perlindungan karena data pribadi tersebut saat ini sudah menjadi komoditas dalam hal seseorang ingin memperoleh suatu akses, barang atau jasa tertentu dari pihak lain. Dimana untuk memberikan perlindungan atas hak privasi tersebut tentu harus dimulai dengan adanya pemberian kepastian akan hukum. Indonesia sendiri telah memiliki perangkat hukum terkait perlindungan data pribadi, namun masih tersebar di beberapa peraturan tanpa adanya suatu peraturan payung yang membawahi ketentuan perlindungan data pribadi dari berbagai macam sektor. Adapun rancangan undang-undang perlindungan data pribadi di Indonesia masih dalam proses pembahasan di DPR.
2. Sesuai dengan teori tanggung jawab hukum, maka pengelola sistem elektronik kesehatan tidak hanya menanggung kerugian pengguna atas setiap kerugian atau kegagalan sistem elektroniknya (*ex-post liability*), namun juga tanggung jawab sebelum terjadinya kerugian atau peristiwa kegagalan (*ex-ante liability*) dengan cara mematuhi standar yang berlaku baik di sektor kesehatan maupun di sektor teknologi informasi dan komunikasi, termasuk memperhatikan pedoman-pedoman yang berlaku secara internasional yang berkaitan dengan penyelenggaraan sistem informasi kesehatan itu sendiri.

Daftar Pustaka

Buku

- Dewi, Shinta, *Aspek Perlindungan Data Pribadi Menurut Hukum Internasional, Regional dan Nasional*. Rafika. Bandung. 2015.
- Makarim, Edmon. *Kompilasi Hukum Telematika*. Radja Grafindo Persada. Jakarta. 2003.
- Makarim, Edmon. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. Raja Grafindo Persada. Jakarta.
- Natamiharja, Rudi. *Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN*. Fakultas Hukum Universitas Lampung. Lampung.
- Sabarinah, *Penguatan Evidence-Based Public Health Melalui Sistem Informasi Kesehatan Berbasis Komunitas: Gagasan Kontribusi Kegiatan MB-KM*, dalam Pidato pada Upacara Pengukuhan sebagai Guru Tetap dalam Bidang Ilmu Biostatistik Fakultas Kesehatan Masyarakat Universitas Indonesia, Depok 27 Maret 2021.
- Soekanto, Soerjono. *Pengantar Penelitian Hukum*. UI-Press. Jakarta. 2010.

Peraturan Perundang-undangan

- Indonesia, Undang-Undang Dasar 1945 Amandemen II.
- _____, Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi. Undang-Undang No. 29 Tahun 2004 tentang Praktik Kedokteran.
- _____, Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Undang-Undang No. 14 tahun 2008 tentang Keterbukaan Informasi Publik.

- _____, Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik,
Undang-Undang No. 36 Tahun 2009 tentang Kesehatan.
- _____, Undang-Undang No. 44 Tahun 2009 tentang Rumah Sakit. Undang-Undang No.
36 Tahun 2012 tentang Rahasia Kedokteran.
- _____, Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang
No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- _____, Peraturan Presiden No. 72 Tahun 2012 tentang Sistem Kesehatan Nasional.
Peraturan Pemerintah No. 46 Tahun 2014 tentang Sistem Informasi Kesehatan.
- _____, Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan
Transaksi Elektronik
- _____, Peraturan Menteri Kesehatan No. 269/MENKES/PER/III/2008 tentang “Rekam
Medis”. Peraturan Menteri Kesehatan No. 1171/MENKES/PER/VI/2011
Tahun 2011 tentang Sistem Informasi Rumah Sakit.
- _____, Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang
Perlindungan Data Pribadi Dalam Sistem Elektronik.
- _____, Peraturan Menteri Kesehatan No. 31 Tahun 2019 tentang Sistem Informasi
Puskesmas. Peraturan Kementerian Komunikasi dan Informatika Nomor 5 Tahun
2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat.
- _____, Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem
Pengamanan dalam Penyelenggaraan Sistem Elektronik.

Internet

- Sutanto, “*Pengembangan Sistem Informasi Manajemen Puskesmas (SIMPUS)*”.
<http://sutanto.staff.uns.ac.id/files/2010/03/prop-simpus.pdf>. diakses pada
tanggal 1 Maret 2019.

Lain-Lain

- ASEAN Human Rights Declaration
General Data Regulation Protection/GDPR (European Union Regulation 2016/679)
Handbook on European Data Protection Law 2018 Edition
Rancangan Undang-Undang Data Pribadi