WIDYA YURIDIKA: JURNAL HUKUM
P-ISSN: 2615-7586, E-ISSN: 2620-5556
Volume 8, (1), 2025

http://publishing-widyagama.ac.id/ejournal-v2/index.php/yuridika/

Rekam Medis Elektronik Berbasis *Cloud Computing*: Pertanggungjawaban Hukum Akibat Kebocoran Data Pasien

Oliviani Yanto[1], Kezia Annabel Rinda Putri[2] , Dyah Hapsari Prananingrum[3]

[1] Fakultas Hukum, Universitas Kristen Satya Wacana, Indonesia, olivianiyanto01@gmail.com
[2] Fakultas Hukum, Universitas Kristen Satya Wacana, Indonesia
[3] Fakultas Hukum, Universitas Kristen Satya Wacana, Indonesia

ABSTRACT

The primary objective of this research is to analyze legal liability in breach of patient's medical record in SatuSehat platform that provides Cloud Computing-based electronic medical record. This research is a document study or normative legal research that uses conceptual approach and statute approach. The Omnibus Health Law and Minister of Health Regulation about Medical Records require in implementation of medical records must be in electronic form or electronic medical records. As a result of this obligation, legal issue arises related to the protection and confidentiality of patient data which stored and managed by electronic medical record's administrator. Focus of this research is the implementation of a cloud computing-based electronic system through a system developed by the Ministry of Health which is SatuSehat. This research shows that the party who legally liable for the implementation of Cloud Computing-based electronic medical records is the Ministry of Health, the reason is because there is a transfer of legal liability from healthcare facility to the Ministry of Health because initially the patient data is received by the healthcare facility, and then integrated into the Cloud Computing-based electronic medical record. So because of that, Ministry of Health as a party who has full authority of the data that has been received and integrated in SatuSehat system must held the responsibility if there is a problem with the data. Therefore, the purpose of this study is not only to analyze of the legal responsibility but also to provide legal basis for the protection of hospitals, doctors and patients in the event of a data leak in the SatuSehat Platform. In addition, authors analyzes the protection principles applied in Indonesia with three pillars of patient health data protection applied in the United States.

MANUSCRIPT INFO

Manuscript History:
Received:
May 13, 2024

Accepted:
March 13, 2025

Corresponding Author:
Oliviani Yanto,
olivianiyanto01@gmail.com

***Keywords*:**
Health Data; Healthcare Facilities; Right to Privacy; Ministry of Health; Electronic Medical Records.

Cite this paper Yanto, O., Putri, K. A., & Prananingrum, D. H. (2025). Rekam Medis Elektronik Berbasis Cloud Computing: Pertanggungjawaban Hukum Akibat Kebocoran Data Pasien. *Widya Yuridika: Jurnal Hukum, 8*(1).

Layout Version:
v.7.2024

PENDAHULUAN

Tulisan ini hendak mengkaji pertanggungjawaban hukum akibat kebocoran data pasien dalam rekam medis elekronik berbasis *Cloud Computing*. Menurut Warren dan Brandeis yang dikutip oleh Siti Yuniarti, privasi merupakan "*the right to enjoy life and the right to be left alone".* [1] Berdasarkan hal tersebut, hak privasi adalah hak yang dimiliki setiap

[1] Siti Yuniarti. (2019). Perlindungan Hukum Data Pribadi di Indonesia. *Jurnal Business Economic, Communication, and Social Sciences, 1(1),* 147-154. Doi: https://doi.org/10.21512/becossjournal.v1i1.6030

individu untuk menjaga informasi tentang dirinya agar tidak diungkapkan kepada orang lain, tuntutan dari individu untuk dapat dibiarkan sendiri, dari pengawasan atau campur tangan orang lain, organisasi maupun pemerintah. Adapun kerahasiaan bahwa setiap data atau informasi klinis dari tiap pasien selalu dianggap sebagai rahasia dan harus dilindungi. Dalam ranah perumahsakitan, informasi pasien yang harus dijaga kerahasiaannya adalah data pribadi, diagnosis, catatan pengobatan dan kemajuan hingga hasil laboratorium yang tercatat dalam rekam medis elektronik (RME).

Secara normatif pada intinya RME merupakan sebuah dokumen berisi data pribadi dari pasien. Data pribadi ini berisi data pasien mulai dari isi pemeriksaan, obat yang diberikan, bahkan tindakan yang dilakukan, dimana data tersebut disimpan dengan menggunakan sistem elektornik.[2] Pada perkembangannya, Kementerian Kesehatan melakukan akselerasi digital yakni dengan mengembangkan SatuSehat yang merupakan *platform* penghubung antara pasien, fasilitas pelayanan kesehatan, dan tenaga kesehatan. SatuSehat adalah perkembangan aplikasi PeduliLindungi per tanggal 1 Maret 2023.[3] SatuSehat merupakan *platform* yang diperuntukan bagi pasien khususnya dalam mengakses data kesehatannya. Salah satu fitur yang dihadirkan oleh SatuSehat adalah *resume* medis yang akan menampilkan riwayat pemeriksaan pasien serta data lain yang dikirimkan oleh fasilitas pelayanan kesehatan termasuk data pribadi pasien. Dengan adanya SatuSehat, memberikan kemudahan dari aspek efisiensi dan biaya bagi fasilitas pelayanan kesehatan. Selain itu juga memberi kemudahan kepada pasien dalam mendapatkan pelayanan kesehatan.

Model penyimpanan rekam medis yang digunakan pada *platform* SatuSehat adalah penyimpanan berbasis *online* yang terhubung dengan internet atau biasa disebut sebagai *Cloud Computing*. Sistem *Cloud Computing* merupakan suatu sistem *based on internet*, artinya pasien dapat secara mudah mengakses *resume* medis serta tenaga kesehatan juga dimudahkan dalam mengakses RME dimana pun dan setiap saat dengan terhubung pada jaringan internet (Dewi, 2016).[4] Dengan kata lain, SatuSehat menjadi wadah terselenggaranya RME berbasis *Cloud Computing*. Hal tersebut menunjukkan bahwa teknologi memegang fungsi penting dalam pelaksanaan rekam medis. Disamping memberi kemudahan, model *Cloud Computing* yang digunakan dalam RME juga memiliki risiko yang tidak dapat dikesampingkan. Hadirnya *Artificial Intelligence* berimplikasi langsung terhadap penyimpanan data pasien dalam RME berbasis *Cloud Computing*. *Artificial Intelligence* mempunyai peran ganda yakni dapat digunakan untuk mengolah data pasien namun juga dapat digunakan sebagai alat untuk menyalahgunakan data pasien untuk kepentingan individu atau korporasi tertentu.

Data pasien tergolong sebagai data sensitif yang menjadi sasaran serangan siber mengingat penyimpanan RME dilakukan melalui *Cloud Computing* sehingga akan sangat mudah bagi peretas untuk membajak data pasien.[5] Para peretas akan semakin dimudahkan dengan adanya *Artificial Intelligence* untuk melakukan pembajakan data pasien. Selain itu, data pasien yang disimpan melalui sistem *Cloud Computing* juga mampu berisiko untuk hilang dalam penyimpannya .[6] Di saat yang bersamaan, dalam pelaksanaan RME, kewajiban

[2] Pasal 1 angka 1 jo. Pasal 1 angka 2 Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis.
[3] Erwina Puspapertiwi dan Rizal Setyo Nugroho. 2023. PeduliLindungi Jadi Satu Sehat Mulai 1 Maret 2023, Apa Saja Fiturnya?. Diambil Februari 1, 2024. Dari https://www.kompas.com/tren/read/2023/02/28/173000965/pedulilindungi-jadi-satu-sehat-mulai-1-maret-2023-apa-saja-fiturnya-?page=all
[4] Sinta Dewi Rosadi. (2016). Konsep Perlindungan Hukum atas Privasi dan Data Pribadi dikaitkan dengan Penggunaan Cloud Computing di Indonesia. *Yustitia, 5(1),* 22-30. Doi: https://dx.doi.org/10.20961/yustisia.v5i1.8712
[5] Rodrigo Tertulino, Nuno Antunes dan Higor Morais. (2024). Privacy in Electronic Health Records: A systematic Mapping Study. *Journal of Public Health*, 32, 435-454. Doi: https://doi.org/10.1007/s10389-022-01795-z
[6] Arum Fatmawati dan Budi Hermono. (2016). Perlindungan Hukum atas Data Pengguna oleh Penyedia Layanan Cloud Computing ditinjau dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Novum: Jurnal, 3(3), 1-10.

dari fasilitas pelayanan kesehatan adalah untuk melindungi data pasien yang merupakan hak privasi pasien. Atas dasar tersebut, isu hukum yang hendak dibahas dalam tulisan ini adalah apakah fasilitas pelayanan kesehatan dapat dikenai pertanggungjawaban ketika terjadi kebocoran data pasien penyelenggaraan RME berbasis *Cloud Computing* yang dikelola oleh Kementerian Kesehatan.

Pada dasarnya pihak yang bertanggung jawab penuh terhadap hak privasi pasien dalam RME adalah fasilitas pelayanan kesehatan sebagai penyelenggara RME karena penyelenggara merupakan pihak yang pertama kali meminta akses data pasien dan penyelenggara memiliki kewajiban penuh dalam melindungi data pasien. Namun, tanggung jawab fasilitas pelayanan kesehatan menjadi beralih ke Kementerian Kesehatan, ketika fasilitas pelayanan kesehatan mengintegrasikan RME ke dalam *platform* SatuSehat milik Kementerian Kesehatan. Proses integrasi tersebut dilakukan saat fasilitas pelayanan kesehatan melakukan pendaftaran para portal rekam medis SatuSehat. Dalam hal ini, Kementerian Kesehatan adalah pihak yang mengelola *platform* SatuSehat sehingga sejatinya Kementerian Kesehatanlah yang bertanggung jawab penuh atas data pasien yang ada di dalam *platform* tersebut. Sebagai gagasan tulisan ini mendorong adanya pengaturan soal penyimpanan data pasien dalam penyelenggaraan RME berbasis *Cloud Computing* dimana didalamnya mencakup prinsip penggunaan *Artificial Intelligence* dalam mengolah data pasien mengingat ke depan seluruh fasilitas pelayanan kesehatan diwajibkan untuk mengintegrasikan seluruh data RME ke dalam SatuSehat dan wajib untuk melaksanakan RME.

Penelitian serupa telah dilakukan oleh Andika Putra dan Redyanto, dimana tulisan tersebut berkesimpulan bahwa pihak ketiga (pengembang RME) tidak dapat dikenai pertanggungjawaban hukum ketika timbul permasalahan yang mengganggu hak privasi pasien, seperti kebocoran data pribadi pada sistem RME.[7] Penelitian tersebut dilakukan sebelum lahirnya Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis (PMK 2022),[8] sedangkan tulisan ini dikaji pasca PMK 2022 yakni pada saat seluruh fasilitas pelayanan kesehatan di Indonesia diwajibkan untuk menggunakan RME. Penelitian serupa lainnya dilakukan oleh Calvin Anthony Putra dan Muh. Ali Masnun, dimana tulisan tersebut berkesimpulan bahwa berdasarkan Pasal 46 Undang-Undang Nomor 44 tahun 2009 tentang Rumah Sakit[9] didukung dengan doktrin *vicarious liability*, rumah sakit dapat dikenai pertanggungjawaban hukum atas kelalaian yang terjadi pada RME.[10] Sedangkan tulisan ini akan berfokus pada penyelenggaraan RME berbasis *Cloud Computing* dengan menempatkan Kementerian Kesehatan sebagai pihak yang dikenai pertanggungjawaban hukum apabila terjadi kebocoran data pasien yang terintegrasi dalam *platform* SatuSehat. Maka dari itu, tulisan ini memiliki unsur urgensi dimana setiap fasilitas pelayanan kesehatan dituntut untuk menyelenggarakan RME dengan risiko hukum yang cukup tinggi sehingga diperlukan langkah hukum dalam rangka memberi perlindungan hukum terhadap rumah sakit, dokter, sekaligus pasien.

---

[7] Andika Putra, Redyanto Sidi dan Syaiful Asmi Hasibuan. (2023). Tanggungjawab Hukum Pihak Ketiga dan Rumah Sakit terhadap Penyelenggaraan Electronic Medical Record. Jurnal Ilmiah Ilmu Pendidikan, 6(8), 6280-6289.

[8] *Ibid.*

[9] Undang-Undang Nomor 44 tahun 2009 tentang Rumah Sakit telah dicabut dengan Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan. Penelitian yang dilakukan oleh Calvin Anthony Putra dan Muh. Ali Masnun dilakukan sebelum adanya Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan.

[10] Calvin Anthony Putra dan Muhammad Ali Masnun. (2022). Analisis Pertanggungjawaban Rumah Sakit terkait Potensi Kebocoran Data Rekam Medis Elektronik Akibat Cyber Crime. *Novum: Jurnal Hukum Membudayakan Literasi Hukum*, *9(2),* 1-14. Doi: https://doi.org/10.2674/novum.v0i0.41286

Di samping itu pula, tulisan ini dikaji pasca adanya kewajiban bagi setiap rumah sakit untuk melakukan RME, oleh karena itu dapat dipastikan bahwa tulisan ini mengandung unsur kebaruan. Sehubungan dengan hal tersebut, terdapat dua masalah yang dikemukakan dalam penelitian ini yaitu yang pertama adalah Bagaimana hubungan hukum antara pasien, *platform* RME, dan fasilitas pelayanan kesehatan dan rumusan masalah kedua adalah Apakah fasilitas pelayanan kesehatan dapat dikenai pertanggungjawaban hukum manakala terjadi kebocoran data pasien yang sudah terintegrasi dalam *platform* yang dikelola oleh Kementerian Kesehatan. Selanjutnya akan dijelaskan secara komperhensif dalam bagian pembahasan.

METODE

Penelitian hukum yang dilakukan adalah penelitian hukum normatif (*normative legal research*) guna menghasilkan argumentasi sebagai anjuran dalam menyelesaikan masalah hukum yang dihadapi.[11] Bertolak pada hal tersebut, tulisan ini juga dikaji dengan menggunakan 2 (dua) pendekatan yaitu *pertama*, pendekatan konseptual (*conceptual approach*) yang berdasar dengan doktrin yang berkembang dalam dunia ilmu hukum[12] *Kedua*, adalah pendekatan perundang-undangan (*statute approach*) yang merupakan pendekatan terhadap peraturan perundang-undangan yang memiliki kaitanmya terhadap isu hukum yang dianalisis.[13] Sebagai tambahan, bahan hukum yang dipakai dalam penelitian ini adalah peraturan perundang-undangan atau biasa disebut bahan hukum primer. Bahan hukum berikutnya adalah buku, jurnal ilmiah maupun hasil penelitian para ahli yang biasa disebut bahan hukum sekunder.

HASIL DAN PEMBAHASAN

Hubungan Hukum dalam Pelaksanaan RME berbasis Cloud Computing

Berkenaan dengan pelaksanaan RME, Indonesia melalui Pasal 45 PMK 2024 telah mewajibkan penyelenggaraan RME selambat-lambatnya akhir tahun 2023 (31 Desember 2023) untuk seluruh fasilitas pelayanan kesehatan (fasyankes). Penyelenggaraan RME dapat dilakukan oleh unit kerja dalam fasyankes maupun disesuaikan dengan kebutuhan dari tiap fasyankes. Dalam hal ini, pelaksanaan RME tidak dapat dipisahkan dari sistem elektronik yang mana dalam pelaksanaannya berbentuk sistem yang dikembangkan oleh Kementerian Kesehatan maupun dibangun sendiri oleh fasyankes. Dalam hal membangun sistem RME fasyankes juga dapat bekerja sama dengan pihak ketiga yakni penyelenggara sistem elektronik. Tulisan ini hanya berfokus pada kerja sama antar fasyankes dengan Kementerian Kesehatan dalam rangka penyelenggaraan RME berbasis *Cloud Computing*.

Sebelum beranjak lebih jauh berkenaan dengan pertanggungjawaban hukum terhadap kebocoran data pasien dalam RME berbasis *Cloud Computing* yang dikelola oleh Kementerian Kesehatan, perlu untuk dibahas terlebih dahulu mengenai hubungan hukum antar para pihak dalam RME berbasis *Cloud Computing*. Pihak-pihak tersebut antara lain pasien, fasyankes, dan Kementerian Kesehatan. Hubungan hukum menjadi hal yang esensial untuk dikaji sebab hubungan hukum menjadi kunci utama dalam menentukan siapa pihak yang dapat dikenai pertanggungjawaban. Menurut Soeroso hubungan hukum (*recht betrekkingen*) adalah suatu hubungan yang lebih dari satu subyek hukum di mana setiap pihak mempunyai hak dan kewajiban terhadap satu dengan yang lain.[14]

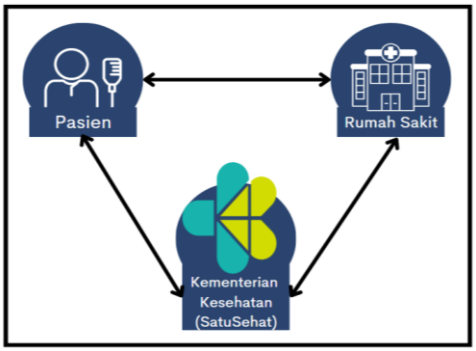
[11] Muhaimin. (2020). *Metode Penelitian Hukum.* Nusa Tenggara Barat: Mataram University Press, 46.

[12] *Ibid.* 29.

[13] *Ibid*. 56.

[14] Dewa Gede Brahmanta dan Anak Agung Sri Utari. (2017). Hubungan Hukum Antara Pelaku Usaha Dengan Konsumen. Jurnal Kertha Semaya, 5(1), 1-5.

Terjadinya peristiwa hukum dilandaskan dengan adanya hubungan hukum para pihak. Peristiwa hukum adalah perbuatan yang dilakukan subjek hukum dengan kesadaran penuh sehingga berimplikasi hak dan kewajiban.[15] Sejalan dengan Sudikno Mertokusumo bahwa peristiwa dapat disebut sebagai peristiwa hukum apabila mempunyai akibat hukum.[16] Penyelenggaraan RME berbasis *Cloud Computing* merupakan peristiwa hukum sebab dengan terselenggaranya RME berbasis *Cloud Computing* melahirkan hubungan hukum antar pasien dengan fasyankes, fasyankes dengan Kementerian Kesehatan, serta Kementerian Kesehatan dan pasien. Hubungan hukum tersebut digambarkan dengan ilustrasi berbentuk segitiga pada Gambar 1 seperti di bawah ini :



Gambar 1 Hubungan Hukum dalam Penyelenggaraan RME berbasis *Cloud Computing*

Hubungan antara pasien dan fasyankes dilandaskan pada Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan ("UU Kesehatan"). Hubungan tersebut tergambarkan dari hak dan kewajiban antara pasien dan fasyankes yang saling bersinggungan. Fasyankes wajib untuk menyelenggarakan dan memberikan pelayanan kesehatan dengan kualitas yang baik kepada pasien, serta melindungi kerahasiaan data yakni RME sesuai dengan Pasal 297 UU Kesehatan. Sedangkan, hak pasien adalah untuk menerima pelayanan kesehatan yang mencukupi sebanding dengan kebutuhannya. Dengan demikian, bahwa hubungan antara pasien dan fasyankes lahir dari undang-undang yang mempunyai hubungan hukum sehingga masing-masing pihak memegang hak dan kewajiban sesuai uraian di atas. Bahwa fasyankes adalah pemberian pelayanan Kesehatan sedangkan pasien penerima pelauanan kesehatan.

Hubungan antara fasyankes dan Kementerian Kesehatan juga didasarkan UU Kesehatan dimana hadirnya fasyankes merupakan sebagai bentuk upaya Pemerintah dalam rangka melaksanakan dan mewujudkan bagi masyarakat demi mencapai derajat kesehatan setinggi-tingginya. Selain memenuhi kewajibannya dalam menyelenggarakan upaya kesehatan, Pemerintah yang dimaksud adalah Kementerian Kesehatan yang mempunyai kewajiban juga untuk mengelola sistem informasi kesehatan nasional berupa mengintegrasikan dan menstandarisasi seluruh sistem informasi kesehatan guna menunjang pembangunan sistem Kesehatan di Indonesia. Sistem informasi kesehatan nasional adalah suatu sistem yang menggabungkan berbagai tahapan yang dilakukan demi meningkatkan efisiensi dan efektivitas pelayanan kesehatan. Tahapan tersebut terdiri dari tahapan pemrosesan, pelaporan, dan penggunaan informasi. Dalam hal ini, Kementerian Kesehatan diberi kewenangan untuk mengelola sistem informasi kesehatan Nasional yang dimana sistem tersebut terhubung dengan fasyankes. Hubungan tersebut tergambar ketika fasyankes melakukan pendaftaran untuk pengintegrasian rekam medis ke dalam sistem

[15] Hadi Fardiansyah, et al. (2023). *Pengantar Ilmu Hukum.* Badung: CV Intelektual Manifes Media.
[16] Mochammad Fahruz Rizqy. (2015). Implikasi Yuridis Putusan MK Nomor 46/PUU-VIII/2010 Terkait Perlindungan Hak Anak. *Yuridika, 30(2),* 278-306. https://doi.org/10.20473/ydk.v30i2.4652

informasi kesehatan Nasional. Penyelenggaraan RME berbasis Cloud Computing salah satu bagian dari rangkaian integrasi tahapan dalam sistem informasi kesehatan nasional. Dalam praktik, proses integrasi tersebut dilakukan oleh fasyankes melalui registrasi pada portal rekam medis SatuSehat. Sehingga, Kementerian Kesehatan berhak atas data pasien yang dikirimkan dari fasyankes. Hal tersebut secara implisit tersirat dalam Pasal 350 UU Kesehatan pada intinya sistem informasi kesehatan terdapat di dalamnya data dan informasi yang bersifat pribadi maupun publik yang bersumber dari fasyankes. Lebih lanjut, fasyankes memiliki kewajiban untuk melakukan pendaftaran pada portal rekam medis SatuSehat dalam rangka melakukan integrasi rekam medis pasien. Berkenaan dengan hal tersebut, pada Pasal 190 UU Kesehatan, rumah sakit sebagai salah satu fasyankes mempunyai kewajiban untuk mengimplementasi sistem informasi kesehatan RS dimana sistem ini terhubung dengan sistem informasi kesehatan nasional. Tidak hanya terbatas pada rumah sakit, Pasal 345 ayat (2) UU Kesehatan membuka peluang bagi fasyankes lainnya yang menyelenggarakan sistem informasi kesehatan untuk wajib mengintegrasikannya ke dalam sistem informasi kesehatan Nasional. Artinya, sistem yang dibangun oleh fasyankes wajib terhubung dengan sistem yang dikelola oleh Kementerian Kesehatan. Maka dari itu, ketika fasyankes sudah terdaftar pada portal rekam medis SatuSehat, data pasien yang diterima oleh fasynakes selanjutnya akan diterima oleh Kementerian Kesehatan untuk masuk ke SatuSehat.

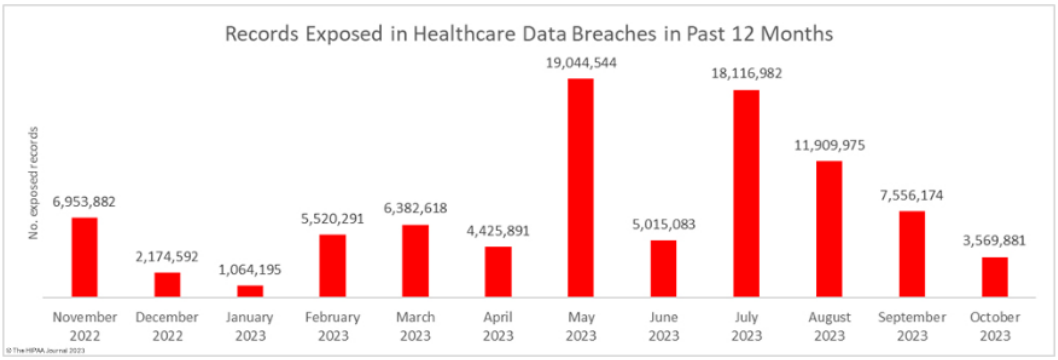
Hubungan antara Kementerian Kesehatan dengan pasien sejatinya implementasi dari pemenuhan hak bagi warga negara sebagaimana diamanatkan dalam UUD 1945. SatuSehat yang dikelola oleh Kementerian Kesehatan merupakan bentuk pemenuhan hak-hak yang dijamin oleh konstitusional untuk masyarakat atas penyediaan pelayanan kesehatan yang pantas yakni berlandaskan pada Pasal 28G ayat (1) dan Pasal 34 ayat (3) UUD 1945 . Pada umumnya, hak pasien dalam hubungannya dengan Kementerian Kesehatan adalah memperoleh edukasi dan informasi tentang kesehatan; serta mendapatkan pemenuhan kebutuhan akan layanan kesehatan yang berkualitas, aman, dan terjangkau sesuai dengan regulasi pelayanan kesehatan.Tidak hanya itu, Kementrian Kesehatan juga memiliki kewajiban terhadap pasien dengan cara menjaga kerahasiaan data sebagai bentuk perlindungan hak asasi manusia. Dalam hubungannya dengan penyelenggaraan RME berbasis *Cloud Computing* yang dilaksanakan Kementerian Kesehatan melalui SatuSehat, pasien berhak untuk mendapatkan pelindungan data dan informasi kesehatan. Sesuai Pasal 16 huruf a dan b UU ITE yang pada pokoknya Penyelenggara Sistem Elektronik baik Kementrian Kesehatan maupun fasyankes memiliki kewajiban memberikan informasi elektronik secara utuh dalam sistem elektronik serta memberikan perlindungan kerahasiaan maupun keteraksesan pada informasi elektronik. Selain itu, UU PDP pada Pasal 36 secara konkrit mengatakan bahwa pengendali data pribadi yakni fasyankes dan Kementrian Kesehatan wajib menjaga kerahasiaan data pribadi pada konteks ini RME. Selain itu, pasien berhak untuk mengakses resume medis. Dalam hal pemrosesan data, hak pasien sebagai pemilik data antara lain: memperoleh informasi mengenai maksud pengumpulan data milik pasien; mengakses serta dapat melakukan perbaikan data dan informasi; dan meminta Kementerian Kesehatan sebagai penyelenggara SatuSehat untuk menghapus data yang tidak benar.

Berkenaan dengan hal tersebut, Kewajiban Kementerian Kesehatan sebagai penyelenggara sistem informasi kesehatan nasional adalah menjamin pelindungan informasi dan data kesehatan pasien serta menginformasikan kepada pasien jika terdapat ketidakberhasilan pelindungan data dan informasi kesehatan.

Pertanggungjawaban Hukum terhadap Kebocoran Data Pasien dalam RME berbasis Cloud Computing

Transformasi digital dalam pelayanan kesehatan sejatinya dimaksudkan untuk memajukan akses dalam memberi kemudahan masyarakat dalam menerima layanan kesehatan. Penggunaan teknologi dalam pelayanan kesehatan khususnya melalui RME dinilai jauh lebih efektif dan memberikan banyak manfaat seperti penurunan biaya, peningkatan kualitas pelayanan kesehatan, membantu dalam penyimpanan dan mobilitas data.[17] Namun permasalahan keamanan dalam menggunakan teknologi dalam layanan kesehatan dapat memberi pengaruh signifikan terkait masalah keamanan data.[18] Kebocoran data merupakan suatu risiko dari penyelenggaraan RME yang tidak bisa terelakkan. Indonesia pernah gentar mengalami kebocoran data pada aplikasi PeduliLindungi yang saat ini bertransformasi menjadi SatuSehat. Berdasarkan fakta yang diperoleh dari Kemenkominfo menunjukkan bahwa pada 2022, terdapat 3,2 miliar data PeduliLindungi yang dinyatatakan bocor.[19] Berkaca pada kasus kebocoran data melalui PeduliLindungi menunjukkan bahwa terdapat potensi kebocoran data pada SatuSehat yang merupakan *platform* yang dikembangkan dari PeduliLindungi. Kasus kebocoran data sejatinya merupakan kasus dalam lingkup mendunia. Amerika Serikat sebagai negara yang sudah terlebih dahulu menyelenggarakan RME berbasis *Cloud Computing* juga pernah mengalami kebocoran data pasien.[20] Dalam kurun waktu Januari hingga Oktober 2023, berdasarkan fakta yang diperoleh dari United States Department of Health and Human Services, tercatat 82.600.000 penduduk Amerika Serikat yang datanya tersimpan dalam RME mengalami kebocoran data (Alder, 2023). Grafik pelanggaran kebocoran data pasien RME di Amerika Serikat nampak pada Tabel 1. di bawah ini:

Tabel 1 Grafik Kebocoran Data Pasien dalam RME[21]



Data di atas yang telah memperlihatkan potensi kebocoran data pasien dalam penyelenggaraan RME berbasis *Cloud Computing* cukup tinggi. Melihat adanya transformasi kesehatan berbasis digital menjadikan data pasien sejatinya harus terintegrasi dalam satu kesatuan sistem sehingga mudah untuk diakses dan pasien dapat secara mudah mendapatkan pelayanan kesehatan.

[17] Ismail Keshta dan Ammar Odeh. (2021). Security and Privacy of Electronic Health Records: Concerns and Challenges. *Egyptian Informatics Journal, 22, 177*-183. Doi: https://doi.org/10.1016/j.eij.2020.07.003
[18] Md Mahbub Hossain dan Y Alicia Hong. (2020). Trends and Characteristics of Protected Health Information Breaches in the United States. AMIA Annual Symposium Proceedings, 1081-1090.
[19] Lenny Septiani. 2022. Kominfo Selidiki 33 Dugaan Data Bocor Tahun Ini, Ada PeduliLindungi. Diambil Februari 1, 2024, Dari https://katadata.co.id/desysetyowati/digital/637f2d191631e/kominfo-selidiki-33-dugaan-data-bocor-tahun-ini-ada-pedulilindungi#google_vignette
[20]Steve Alder. 2023. October 2023 Healthcare Data Breach Report. Diambil Januari 19, 2024. Dari https://www.hipaajournal.com/october-2023-healthcare-data-breach-report
[21] *Ibid.*

Terkait dengan data pasien yang dimaksud merupakan data pribadi yang dijustifikasi melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi ("UU PDP") dimana data yang di-input ke dalam RME berbasis *Cloud Computing* adalah data pribadi yang bersifat umum maupun spesifik. Sejatinya isi RME serupa dengan rekam medis konvensional hanya yang membedakan wadah penyimpanannya. Pasal 26 ayat (6) PMK No.24 Tahun 2024 tentang Rekam Medis telah menetapkan paling tidak terdapat 4 (empat) isi rekam medis antara lain identitas pasien; hasil pemeriksaan pasien; proses mengidentifikasi penyakit, penyembuhan, dan perencanaan pelayanan kesehatan; serta nama dan juga tanda tangan tenaga kesehatan pemberi pelayanan kesehatan.

Sehubungan dengan ini, identitas pasien dikategorikan sebagai data pribadi yang bersifat umum, sedangkan hasil pemeriksaan pasien, proses mengidentifikasi penyakit , pengobatan, dan rencana tindak lanjut pelayanan kesehatan tergolong sebagai bagian dari informasi kesehatan yang merupakan data pribadi pasien yang bersifat spesifik. Dalam penjelasan Pasal 4 ayat (2) huruf a UU PDP, dijelaskan data dan informasi kesehatan merupakan catatan/keterangan kesehatan (fisik dan/atau mental) maupun pelayanan kesehatan milik individu. Hal tersebut menunjukkan bahwasannya isi dari RME milik pasien wajib dilindungi karena merupakan hak privasi pasien yang dijamin oleh Pasal 28G ayat (1) UUD 1945 dan UU PDP.

RME dalam penyelenggaraan berbasis *Cloud Computing* berpotensi untuk bocor atau hilang secara keseluruhan (bukan hanya resume medis). Sebab, data yang dikirimkan oleh fasyankes ke dalam sistem yang dikelola oleh Kementerian Kesehatan tidak hanya terbatas pada *resume* medis. Dalam hal ini, tenaga kesehatan juga diberikan akses oleh fasynakes untuk mengakses RME pasien melalui sistem rekam medis yang dikelola oleh Kementerian Kesehatan tersebut. Ketika data pasien dalam RME milik seluruh masyarakat Indonesia yang sudah terintegrasi dalam satu sistem lalu kemudian diretas, hal tersebut mengganggu hak privasi pasien.[22]Dengan kata lain, hak privasi pasien dengan adanya RME berbasis *Cloud Computing* semakin terancam. Jika pasien tidak dijamin privasinya dalam penyelenggaraan RME, konsekuensi yang timbul adalah pemberian pelayanan kesehatan akan menjadi terhambat. Selain hak privasi yang terancam, hak mendapat pelayanan kesehatan seperti terjamin dalam Pasal 28H ayat (1) UUD 1945 juga secara beriringan akan terancam. Hal tersebut menimbulkan pertanyaan terkait siapa pihak yang bertanggung jawab ketika data pasien dalam RME berbasis *Cloud Computing* bocor atau hilang.

Pertanggungjawaban hukum menjadi hal yang krusial ditengah-tengah perkembangan teknologi. Tingginya risiko sistem *Cloud Computing* dimana dengan adanya sistem tersebut data pasien seluruh Indonesia dapat dihimpun menjadi satu kesatuan. Akibatnya, jika terjadi kebocoran data, bukan hanya pasien dalam 1 (satu) rumah sakit yang terancam melainkan pasien di seluruh Indonesia. Terjadinya suatu kebocoran ataupun hilangnya data merupakan hal yang tidak dapat diduga dan dapat terjadi sewaktu-waktu.[23] Maka dari itu, penting untuk dilakukannya mitigasi risiko hukum dengan menentukan pihak yang bertanggung jawab atas kebocoran data dalam RME berbasis *Cloud Computing*.

Penyelenggaraan RME berbasis *Cloud Computing* tidak terlepas dari pengaturan terkait UU Informasi dan Transaksi Elektronik (UU ITE) baik itu UU No. 11 tahun 2008 maupun UU No. 1 Tahun 2024. Bertolak pada pembahasan pada bagian sebelumnya dimana pihak yang pertama kali menerima data pasien untuk dimasukkan ke RME adalah fasyankes. Namun,

[22] Fanny Priscyllia. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. Jatiswara, 34(3), 239-249.

[23] Naik Nithesh, et al. (2022). Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility. *Frontiers in Surgery*, 9, 862322, 1-6. Doi: 10.3389/fsurg.2022.862322

fasyankes mengalihkan data pasien tersebut ke dalam RME berbasis *Cloud Computing* yang merupakan suatu sistem layanan kesehatan yang sudah terintegrasi. Sistem tersebut diciptakan oleh Kementerian Kesehatan melalui SatuSehat, sehingga data pasien yang semula berada di bawah pengawasan fasyankes menjadi beralih ke Kementerian Kesehatan mana kala fasynakes sudah mengintegrasikan RME ke dalam RME yang sudah berbasis *Cloud Computing*. Peralihan data itu terjadi sejak fasyankes berhasil melakukan pendaftaran pada portal rekam medis dalam *platform* SatuSehat yang dikelola oleh Kementerian Kesehatan. Sehingga, data pasien dalam *platform* SatuSehat sepenuhnya berada dalam pengawasan Kementerian Kesehatan sebagai penyelenggara sistem elektronik berdasarkan Pasal 1 angka 6a UU ITE sejak fasyankes berhasil terhubung dengan portal rekam medis SatuSehat.

Sekalipun Kementerian Kesehatan mempekerjakan pihak lain untuk mengelola RME, tanggung jawab utama dalam penyelenggaraan RME tetap berada di bawah pengawasan Kementerian Kesehatan. Bertolak pada Pasal 15 ayat (1) UU ITE, Kementerian Kesehatan harus menyelenggarakan RME berbasis *Cloud Computing* secara aman dan bertanggung jawab secara hukum. Dengan kata lain, pihak yang bertanggung jawab dalam kebocoran data pasien dalam RME berbasis *Cloud Computing* adalah Kementerian Kesehatan.

Privasi merupakan suatu unsur esensial dalam penyelenggaraan RME. Oleh karena itu, pada hakikatnya terdapat 2 (dua) prinsip yang harus diperhatikan dalam penyelenggaraan RME antara lain, *pertama*, kerahasiaan (*confidentiality*) yang dimaknai sebagai pembatasan informasi kepada orang yang tidak berwenang untuk mengakses data selama penyimpanan, pengiriman, atau mana kala data tersebut diolah.[24] Artinya, Kementerian Kesehatan sebagai pihak yang mengendalikan sistem RME berbasis *Cloud Computing* wajib memberikan batasan-batasan terhadap siapa saja yang berhak mengakses RME. Sehingga, hanya pasien yang sejatinya dapat mengakses *resume* rekam medis. Namun, tidak terbatas pula pada tenaga kesehatan yang membutuhkan informasi kesehatan pasien untuk dapat RME dalam rangka memberikan pelayanan kesehatan. Dalam hal ini, tenaga kesehatan juga tetap harus memperhatikan aspek kerahasiaan dengan menggunakan data kesehatan pasien dengan penuh tanggung jawab.

Kedua, ketersediaan (*availability*) dimana data pasien dalam RME berbasis *Cloud Computing* harus bisa diakses setiap saat oleh pihak yang membutuhkan atau hendak menggunakannya (dibaca: pasien dan/atau tenaga kesehatan). Termasuk pula skalabilitas sekaligus ketahanan (*recoverability*) jika sewaktu-waktu data pasien dalam sistem tersebut hilang. Artinya, Kementerian Kesehatan berkewajiban untuk mengembalikan data pasien yang bocor serta kembali memberi perlindungan secara utuh terhadap data pasien dalam RME berbasis *Cloud Computing.*

Dua prinsip pada penjelasan di atas sejalan dengan 3 (tiga) pilar yang digunakan oleh Amerika Serikat dalam memastikan perlindungan data kesehatan pasien dalam RME. 3 (tiga) pilar tersebut termuat dalam *the Health Insurance Portability and Accountability* (HIPAA) Act, antara lain:

A. *administrative safeguard*,dimaknai sebagai tindakan administratif serta kebijakan dan prosedur guna mengelola pemilihan, pengembangan, penerapan, dan pemeliharaan langkah-langkah keamanan untuk melindungi informasi kesehatan pasien secara elektronik. Selain itu pula dipergunakan untuk mengelola perilaku tenaga kerja entitas yang berhubungan langsung dengan penyelenggaraan RME (dibaca: provider, fasyankes, pasien, Pemerintah termasuk Kementerian Kesehatan);

[24]Nada Saddig Almaghrabi, dan Bussma Ahmed Bugis. (2022). Patient Confidentiality of Electronic Health Records: A Recent Review of the Saudi Literature. *Dr. Sulaiman Al Habib Medical Journal Volume, 4,* 126-135. Doi: https://doi.org/10.1007/s44229-022-00016-9

B. *physical safeguards*, langkah fisik yang ditempuh dalam melindungi sistem informasi elektronik serta perangkat terkait yang digunakan dalam penyelenggaraan RME. Sistem tersebut patut dilindungi dari bahaya/gangguan pihak-pihak yang berkeinginan untuk mencuri data yang ada dalam sistem;
C. *technical safeguards*, menangani kontrok akses serta pergerakan data. Pihak yang ditugaskan wajib menerapkan kebijakan dan prosedur teknis yang tersedia untuk memberi pembatasan akses hanya kepada orang-orang yang telah diberikan hak ases. Sehingga, RME tidak dapat diakses oleh sembarang orang.

Dengan demikian dapat disimpulkan bahwa Kementerian Kesehatan memegang kendali penuh atas data pasien dalam penyelenggaraan RME melalui SatuSehat. Akibatnya Kementerian Kesehatan dapat dikenai pertanggungjawaban hukum manakala terjadi kebocoran data terhadap data pasien yang sudah masuk ke dalam RME berbasis *Cloud Computing* yang dikelola oleh Kementerian Kesehatan. Bentuk pertanggungjawaban hukum penyelenggara RME dalam Satusehat jika terjadi kebocoran data akan dikenakan sanksi administratif sesuai Pasal 57 UU PDP karena secara eksplisit pada Pasal 351 ayat (5) UU Kesehatan jika terjadi kegagalan pelindungan data informasi kesehatan maka tunduk pada UU PDP. Tanggung jawab tersebut timbul ketika fasyankes berhasil terdaftar dan terintegrasi pada portal rekam medis SatuSehat. Maka dari itu sudah seharusnya Kementerian Kesehatan memperhatikan prinsip-prinsip penyelenggaraan RME berbasis *Cloud Computing* sebagaimana yang telah diterapkan oleh Amerika Serikat. Dengan adanya sistem berbasis *Cloud Computing* prinsip tersebut harus disesuaikan dengan kondisi *existing* atau kondisi yang saat ini terjadi.

PENUTUP

Perkembangan pelayanan kesehatan berbasis teknologi di Indonesia sudah mengalami kemajuan dan tidak bisa disangkal kehadirannya. Perkembangan tersebut telah didukung dengan hadirnya UU Kesehatan yang baru. Fasyankes merupakan pihak pertama yang terhubung dengan pasien dalam hal penyelenggaraan rekam medis elektonik. Sebab, data pasien dalam RME pertama kali diterima oleh fasyankes. Hadirnya UU Kesehatan mendorong seluruh fasyankes untuk mengintegrasikan data pasien ke dalam sistem informasi nasional kesehatan (SatuSehat) yang dioperasikan oleh Kementerian Kesehatan. Sistem yang digunakan tersebut mencakup penyelenggaraan RME berbasis *Cloud Computing*. Akibatnya tanggung jawab pengelolaan data pasien berada di bawah pengawasan Kementerian Kesehatan. Atas dasar tersebut, dalam hal terjadi kebocoran atau hilangnya data pasien dalam penyelenggaraan RME berbasis *Cloud Computing*, pihak yang bertanggung jawab adalah Kementerian Kesehatan. Pertanggungjawaban tersebut timbul ketika fasyankes terdaftar pada portal rekam medis SatuSehat. Berkaca pada praktik di Amerika Serikat berkenaan dengan penyelenggaraan RME berbasis *Cloud Computing*, prinsip yang digunakan adalah *administrative safeguard, physical safeguards,* dan *technical safeguards.* Prinsip tersebut dapat digunakan diadopsi oleh Kementerian Kesehatan mengingat data pasien tergolong sebagai data yang sensitif dan rentan terjadinya kebocoran data. Maka, Kementerian Kesehatan harus mengambil tindakan secara hati-hati dan penuh tanggung jawab dalam mengelolah data pasien yang sudah terintegrasi dalam SatuSehat. Sebagai saran tulisan ini mendorong adanya pengaturan dalam batas-batas penggunaan *Artificial Intelligence* manakala digunakan dalam sistem yang dikelola oleh Kementerian Kesehatan yaitu SatuSehat. Dengan adanya pembatasan-pembatasan yang dikoridori oleh hukum akan menjadi *guideline* bagi Kementerian Kesehatan dalam mengolah data pasien yang sudah terintegrasi.

DAFTAR PUSTAKA

Buku

Fardiansyah , H., Rizkia, D. N., Sadi , M., Busroh, F. F., Lobo, F., Pratama, F., . . . Sinaga, L. B. (2023). *Pengantar Ilmu Hukum.* Badung: CV Intelektual Manifes Media.

Muhaimin. (2020). *Metode Penelitian Hukum*. Nusa Tenggara Barat: Mataram University Press.

Jurnal

Almaghrabi, N, S., & Bugis, B, A. (2022). Patient Confidentiality of Electronic Health Records: A Recent Review of the Saudi Literature. *Dr. Sulaiman Al Habib Medical Journal*, 4,126-135.

Bramanta, D, G., & Utari, A, A, S. 2017. Hubungan Hukum Antara Pelaku Usaha Dengan Konsumen. Jurnal Kertha Semaya, 5(1), 1-5.

Fatmawati, A., & Hermono, B. (2016). Perlindungan Hukum atas Data Pengguna oleh Penyedia Layanan Cloud Computing ditinjau dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Novum: Jurnal Hukum, 3(3), 1-10.

Hossain, M., & Hong, Alicia. (2020). Trends and Characteristics of Protected Health Information Breaches in the United States. AMIA Annual Symposium Proceedings Archive, 1081-1090.

Keshta, I., & Odeh, A. (2021). Security and Privacy of Electronic Health Records: Concerns and Challenges. *Egyptian Informatics Journal*, 22, 177-183. Doi: https://doi.org/10.1016/j.eij.2020.07.003

Naik, N., Hameed, Z., Shetty, D., Swain , D., Shah, M., Paul, R., . . . Somani, B. (2022). Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility. *Frontiers in Surgery*, 9(862322), 1-6. Doi: https://doi.org/10.3389/fsurg.2022.862322

Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. Jatiswara*,* 34 (3), 239-249.

Putra, A., & Sidi, S. (2023). Tanggungjawab Hukum Pihak Ketiga dan Rumah Sakit terhadap Penyelenggaraan Electronic Medical Record. Jurnal Ilmiah Ilmu Pendidikan, 6(8), 6280-6289.

Putra, C, A., & Masnu, M, A. (2022). Analisis Pertanggungjawaban Rumah Sakit terkait Potensi Kebocoran Data Rekam Medis Elektronik Akibat Cyber Crime. *Novum: Jurnal Hukum Membudayakan Literasi Hukum* , 9(2), 1-14. Doi: https://doi.org/10.2674/novum.v0i0.41286

Rizqy, M, F. (2015). Implikasi Yuridis Putusan MK Nomor 46/PUU-VIII/2010 Terkait Perlindungan Hak Anak. *Yuridika, 30(2),* 278-306. Doi: https://doi.org/10.20473/ydk.v30i2.4652

Rosadi, S, D. (2016). Konsep Perlindungan Hukum atas Privasi dan Data Pribadi dikaitkan dengan Penggunaan *Cloud Computing* di Indonesia. *Yustitia*, 5(1), 22-30. Doi: https://dx.doi.org/10.20961/yustisia.v5i1.8712

Tertulino, R., Antunes, N., & Morais, H. (2023). Privacy in Electronic Health Records: "A systematic Mapping Study". *Journal of Public Health*, 32, 435-454. Doi: https://doi.org/10.1007/s10389-022-01795-z

Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi di Indonesia. *Jurnal Business Economic, Communication, and Social Sciences*, 1(1), 147-154. Doi: https://doi.org/10.21512/becossjournal.v1i1.6030

Website

Alder, Steve. 2023. October 2023 Healthcare Data Breach Report. Diambil Januari 19, 2024. Dari https://www.hipaajournal.com/october-2023-healthcare-data-breach-report

Puspapertiwi, E., & Nugroho, R, S. 2023. PeduliLindungi Jadi Satu Sehat Mulai 1 Maret 2023, Apa Saja Fiturnya?. Diambil Februari 1, 2024. Dari https://www.kompas.com/tren/read/2023/02/28/173000965/pedulilindungi-jadi-satu-sehat-mulai-1-maret-2023-apa-saja-fiturnya-?page=all

Septiani, L. 2022. Kominfo Selidiki 33 Dugaan Data Bocor Tahun Ini, Ada PeduliLindungi. Diambil Februari 1, 2024, Dari https://katadata.co.id/desysetyowati/digital/637f2d191631e/kominfo-selidiki-33-dugaan-data-bocor-tahun-ini-ada-pedulilindungi#google_vignette