

BAB III

ANALISIS HASIL PENELITIAN

A. Analisis Penegakan Hukum Positif di Indonesia Terkait Perlindungan Data Rekam Medis Elektronik Pasien di Fasilitas Kesehatan Tingkat Pertama

Kegiatan medis tak luput dari kemajuan teknologi yang begitu cepat. Kemajuan tersebut tak jarang meninggalkan celah atau kekosongan norma yang dapat mengakibatkan kepentingan para pihak tidak terjamin dan dilindungi baik dari segi rekam medis elektronik hingga perlindungan data pribadi Masyarakat yang rawan disalahgunakan. Pemerintah Indonesia juga adaptif mengundang peraturan tentang rekam medis yang di atur dalam Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis membentuk satu kerangka normatif yang saling melengkapi dalam mengatur perlindungan data rekam medis elektronik pasien.³⁸

Undang Undang Nomor 17 Tahun 2023 tentang Kesehatan menempatkan kerahasiaan data dan informasi kesehatan sebagai bagian integral dari hak pasien atas pelayanan kesehatan yang bermutu, dengan mewajibkan tenaga kesehatan, tenaga medis, dan penyelenggara fasilitas pelayanan kesehatan untuk menjaga kerahasiaan data dan informasi pasien, Sebagaimana tercermin dalam Undang-

³⁸ Arief Budiman *et.al*, “Analisis Risiko Dan Tindakan Pencegahan Kebocoran Data Rekam Medis Elektronik Pasien Di RS P Surakarta”, *jurnal ranah research*, Vol. 7 No. 3/2025, hlm. 402

Undang Republik Indonesia Nomor 17 Tahun 2023 Tentang Kesehatan Pasal 189 huruf h yaitu menyelenggarakan rekam medis. Undang Undang ini menjadi dasar sektor kesehatan (*lex specialis*) yang menetapkan bahwa rekam medis, termasuk dalam bentuk elektronik, adalah instrumen pemenuhan hak pasien dan sekaligus objek kewajiban hukum bagi fasilitas pelayanan Kesehatan termasuk fasilitas Kesehatan Tingkat pertama seperti puskesmas dan atau klinik kesehatan.

Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis merupakan pengaturan teknis yang memberikan acuan bagi fasilitas pelayanan kesehatan dalam melakukan pencatatan, penyimpanan, dan pemanfaatan data pasien. Regulasi ini menegaskan bahwa rekam medis bukan hanya sekadar dokumen administratif, melainkan juga instrumen hukum yang memuat informasi pribadi bersifat rahasia sehingga harus mendapatkan perlindungan yang ketat. Seluruh keterangan dalam rekam medis merupakan milik pasien yang wajib dijaga kerahasiaannya oleh tenaga medis, tenaga kesehatan, maupun penyelenggara fasilitas kesehatan.³⁹ Ketentuan ini mengukuhkan prinsip *confidentiality* sebagai pilar utama dalam penyelenggaraan pelayanan kesehatan, dengan menempatkan pasien sebagai pemegang hak atas data, sementara tenaga kesehatan memikul kewajiban untuk menjaga kerahasiaan informasi yang melekat pada data medis tersebut.

Permenkes Nomor 24 Tahun 2022 pada dasarnya membangun standar ideal penyelenggaraan Rekam Medis Elektronik (RME), di mana setiap Fasilitas

³⁹ Lailiyah A, "Gambaran Implementasi Rekam Medis Elektronik di Rumah Sakit Indonesia berdasarkan Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis", *Jurnal Media Gizi Kesmas*, Vol.13, No.1/2024, hlm. 549

Pelayanan Kesehatan, termasuk Fasilitas Kesehatan Tingkat Pertama (FKTP) seperti puskesmas, diwajibkan menyelenggarakan RME sebagaimana ditegaskan dalam Undang-Undang Republik Indonesia Nomor 17 Tahun 2023 Tentang Kesehatan Pasal 173 ayat (1) Fasilitas Pelayanan Kesehatan wajib pada huruf c yaitu *menyelenggarakan rekam medis*. Kewajiban ini tidak hanya bersifat administratif, tetapi juga mencerminkan perubahan paradigma pelayanan kesehatan menuju ekosistem digital yang terintegrasi. Hal yang terkesan tak dipikirkan atau lebih tepat diabaikan, puskesmas diposisikan setara dengan fasilitas lain dalam hal kewajiban menjaga kerahasiaan, integritas, dan ketersediaan data, tanpa selalu memperhitungkan ketersediaan kapasitas teknologi dan sumber daya manusia dalam prakteknya.

Ruang lingkup kegiatan yang diatur Permenkes, mulai dari registrasi pasien (Pasal 12 ayat (1), pendistribusian data, pengisian informasi klinis, pengolahan, penginputan klaim, penyimpanan, penjaminan mutu, hingga transfer isi RME untuk rujukan, menuntut adanya sistem informasi kesehatan yang stabil, aman, dan interoperabel. Ruang lingkup kegiatan yang diatur Permenkes, mulai dari registrasi pasien (Pasal 12 ayat (1), pendistribusian data, pengisian informasi klinis, pengolahan, penginputan klaim, penyimpanan, penjaminan mutu, hingga transfer isi RME untuk rujukan, menuntut adanya sistem informasi kesehatan yang stabil, aman, dan interoperable. Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 berusaha untuk memberikan landasan hukum atau legalitas terhadap penyelenggaraan rekam medis elektronik. Secara garis besar, ada tiga hal baru yang diatur di dalam Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun

2022, yaitu sistem elektronik rekam medis elektronik, kegiatan penyelenggaraan rekam medis elektronik, keamanan dan perlindungan data rekam medis elektronik.⁴⁰

Sistem elektronik rekam medis elektronik dapat berupa: sistem elektronik yang dikembangkan oleh Kementerian Kesehatan Republik Indonesia, sistem elektronik yang dikembangkan oleh fasilitas pelayanan kesehatan sendiri, sistem elektronik yang dikembangkan oleh Penyelenggara Sistem Elektronik (PSE) yang telah terdaftar sebagai Penyelenggara Sistem Elektronik (PSE) pada sektor kesehatan di Kementerian Komunikasi dan Informatika Republik Indonesia. Sistem elektronik yang dipergunakan dalam penyelenggaraan rekam medis elektronik harus memiliki kemampuan kompatibilitas (kesesuaian sistem elektronik yang satu dengan sistem elektronik yang lainnya) dan/atau interoperabilitas (kemampuan sistem elektronik yang berbeda untuk dapat bekerja secara terpadu melakukan komunikasi atau pertukaran data dengan salah satu atau lebih sistem elektronik yang lain, yang menggunakan standar pertukaran data).

Interoperabilitas yang artinya kemampuan aplikasi dan sistem untuk secara aman dan otomatis bertukar data tanpa memandang batas-batas geografis, dalam hal ini mengacu kepada standar sistem elektronik yang diselenggarakan oleh Kementerian Kesehatan Republik Indonesia. Sistem elektronik harus mengacu kepada variabel (elemen data yang terdapat pada sistem elektronik rekam medis elektronik) dan meta data (definisi, format dan kodifikasi) yang ditetapkan oleh

⁴⁰ Putri *et.al*, "Tantangan SIMRS dalam penerapan rekam medis elektronik berdasarkan Permenkes 24 Tahun 2022", *Jurnal Medika Nusantara*, vol.1,no. 1/2023, hlm. 8

Kementerian Kesehatan Republik Indonesia. Oleh karena itu, fasilitas pelayanan kesehatan yang menyelenggarakan rekam medis elektronik atau Penyelenggara Sistem Elektronik (PSE) wajib melakukan registrasi sistem elektronik yang digunakannya di Kementerian Kesehatan Republik Indonesia.⁴¹

Kepemilikan dan isi rekam medis elektronik, mengandung dua makna. Pertama adalah dokumen rekam medis merupakan milik dari fasilitas pelayanan kesehatan. Oleh karena itu, fasilitas pelayanan kesehatan bertanggung jawab atas hilang, rusak, pemalsuan dan/atau penggunaan oleh orang, dan/atau badan yang tidak berhak terhadap dokumen rekam medis. Makna yang kedua adalah isi rekam medis merupakan milik pasien, dan dapat disampaikan kepada keluarga terdekat atau pihak lain setelah mendapat persetujuan dari pasien. Isi rekam medis elektronik wajib dijaga kerahasiaannya oleh semua pihak yang terlibat dalam pelayanan kesehatan dan pelayanan medis di fasilitas pelayanan kesehatan (tidak hanya tenaga kesehatan dan tenaga medis, tetapi juga meliputi yang bertugas di fasilitas pelayanan kesehatan, pimpinan fasilitas pelayanan kesehatan, tenaga yang berkaitan dengan pembiayaan pelayanan kesehatan dan pelayanan medis, pihak lain yang memiliki akses terhadap data dan informasi kesehatan pasien di fasilitas pelayanan kesehatan), walaupun pasien telah meninggal dunia.⁴²

Terkait dengan pembukaan isi rekam medis elektronik, ada dua hal yang harus dijadikan pedoman yaitu: permintaan pembukaan isi rekam medis harus dilakukan secara tertulis atau secara elektronik dan pembukaan isi rekam medis dilakukan

⁴¹ *Ibid*, hlm. 9

⁴² *Ibid*

terbatas sesuai dengan kebutuhan. Pada dasarnya, pembukaan isi rekam medis elektronik harus dengan persetujuan pasien. Pembukaan isi rekam medis elektronik tanpa persetujuan pasien, harus mendapatkan persetujuan Menteri Kesehatan Republik Indonesia. Persetujuan Menteri Kesehatan Republik Indonesia dikecualikan untuk pembukaan isi rekam medis elektronik yang dilakukan atas dasar perintah pengadilan. Pasien dikategorikan telah melepaskan hak atas isi rekam medis elektronik apabila pasien dan/atau keluarga pasien menginformasikan isi rekam medis elektronik kepada publik melalui media massa. Implikasinya, hal ini memberikan kewenangan kepada fasilitas pelayanan kesehatan untuk mengungkapkan rahasia isi rekam medis elektronik sebagai hak jawab dari fasilitas pelayanan kesehatan.

1. Ketimpangan infrastuktur penerapan rekam medis elektronik di fasilitas Kesehatan pertama

Penerapan rekam medis dengan fasilitas elektronik memaksa fasilitas Kesehatan pertama seperti klinik, puskesmas, praktek dokter mandiri harus bergantung pada sistem yang dibangun oleh pihak ketiga atau paket aplikasi siap pakai tanpa didahului uji keamanan yang memadai. Ketika konfigurasi server, mekanisme backup, dan pengelolaan hak akses tidak dikendalikan secara ketat oleh pengelola fasilitas, risiko kebocoran data meningkat, baik melalui celah teknis maupun melalui praktik tidak aman seperti penggunaan akun bersama atau kata sandi yang mudah ditebak. Dalam konteks ini, kewajiban normatif untuk menyelenggarakan RME dapat tercapai secara formal, tetapi kualitas perlindungan data yang menyertai penyelenggaraan

tersebut jauh dari standar yang diharapkan regulasi. Banyak factor yang mempengaruhi rekam medis elektronik menjadi hal yang kurang ideal bahkan terkesan kurang realistis jika fasilitas Kesehatan seperti puskesmas atau klinik diwajibkan, beberapa faktor tersebut ialah:

a. Keterbatasan perangkat pendukung

Pada puskesmas atau klinik yang perangkat kerasnya terbatas, jaringan sering tidak stabil, dan belum menerapkan enkripsi maupun kontrol akses berlapis, setiap tahapan ini justru berpotensi menjadi titik lemah keamanan. Kegiatan yang idealnya terintegrasi dengan alur klinis dapat berubah menjadi “kelemahan” operasional, misalnya ketika petugas harus berulang kali login, memindahkan data secara manual, atau menyimpan data sementara di perangkat pribadi karena keterbatasan perangkat computer. Belum lagi jika koneksi internet terkendala karen keterbatasan provider yang belum bisa menjangkau daerah tersebut akan menghambat pencatatan rekam medis elektronik di puskesmas atau klinik tersebut rentan tidak terlaksana dengan baik. Faktor sumber daya manusia memperdalam kerentanan tersebut.⁴³

b. Sumber daya manusia

Tenaga kesehatan dan administrasi di puskesmas atau klinik pada umumnya dididik untuk fokus pada pelayanan klinis, bukan pada keamanan siber dan tata kelola data pribadi. Tanpa pelatihan

⁴³ Lihat Anonim, “Kesehatan Masyarakat yang Tertinggal: Tantangan Akses Layanan Kesehatan yang Tidak Merata” dalam <https://binus.ac.id/character-building/2025/04/kesehatan-masyarakat-yang-tertinggal-tantangan-akses-layanan-kesehatan-yang-tidak-merata/>, diakses tgl. 11 Desember 2025

berkelanjutan atau pelatihan khusus yang memadai mengenai prinsip kerahasiaan digital, keamanan informasi, dan prosedur respons insiden, pelanggaran kerahasiaan sering terjadi melalui human error: salah input alamat email, mengunduh file ke perangkat pribadi, meninggalkan komputer dalam keadaan login terbuka, atau membagikan akun antarpetugas. Dengan demikian, meskipun alur operasional perlindungan data secara normatif terintegrasi dengan alur pelayanan klinis, integrasi tersebut di tingkat puskesmas seringkali hanya tertulis di atas kertas, belum benar-benar diberlakukan dalam budaya kerja sehari-hari.⁴⁴

2. Resiko penerapan rekam medis elektronik di fasilitas Kesehatan pertama

Penerapan rekam medis elektronik (RME) di fasilitas kesehatan tingkat pertama seperti puskesmas pada satu sisi menawarkan kemudahan akses informasi dan peningkatan mutu layanan, namun pada sisi lain mengandung risiko serius ketika didukung oleh infrastruktur keamanan siber yang lemah. Berbagai studi menunjukkan bahwa risiko kebocoran RME bersumber tidak hanya dari kesalahan manusia, tetapi juga dari kelemahan fisik ruang server, perangkat keras yang tidak memadai, serta sistem komputer yang usang atau tidak terkonfigurasi dengan baik. Di banyak puskesmas, keterbatasan anggaran menyebabkan penggunaan perangkat dengan spesifikasi

⁴⁴ *Ibid*

rendah, jaringan yang tidak tersegmentasi, serta ketiadaan mekanisme audit log yang memadai, sehingga setiap upaya peretasan atau akses tidak sah menjadi lebih sulit terdeteksi dan lebih mudah berhasil. Dalam kondisi demikian, data kesehatan pasien yang seharusnya dilindungi dengan standar keamanan tinggi berisiko besar terekspos tanpa disadari.

Lemahnya keamanan siber di fasilitas kesehatan dasar ini diperparah oleh kurangnya penerapan kontrol akses, enkripsi, dan autentikasi berlapis sebagaimana direkomendasikan dalam kebijakan dan praktik terbaik pengamanan RME. keamanan data RME di beberapa puskesmas menemukan masih adanya kelemahan mendasar, misalnya tidak adanya fitur logout otomatis, penggunaan akun bersama, dan kata sandi yang mudah ditebak, yang semuanya meningkatkan peluang penyalahgunaan dan akses tidak sah terhadap data pasien. Padahal, Permenkes No. 24 Tahun 2022 secara eksplisit menuntut agar RME dikelola dengan menjamin kerahasiaan, integritas, dan ketersediaan data, antara lain melalui pembatasan hak akses dan larangan akses tidak sah terhadap rekam medis elektronik. Ketika ketentuan normatif ini tidak diimbangi dengan kesiapan teknis di lapangan, puskesmas menjadi titik lemah dalam ekosistem data kesehatan nasional.

Risiko keamanan di fasilitas pertama juga perlu dilihat dalam konteks insiden kebocoran data kesehatan berskala besar yang pernah

terjadi. Pada 2022, terjadi kasus dugaan kebocoran sekitar 6 juta data pasien Covid-19 milik Kementerian Kesehatan yang dijual di forum peretas RaidForums, dengan total file sekitar 720 GB berisi NIK, data anamnesis, hasil laboratorium, CT-scan, dan informasi medis sangat sensitif lainnya. Lebih parahnya Beberapa pakar keamanan siber menyatakan bahwa data yang bocor “mungkin bukan hanya pasien Covid-19”, melainkan data lebih luas dan berasal dari berbagai rumah sakit.⁴⁵ Kasus ini menunjukkan bahwa kelemahan pada satu titik dalam rantai sistem informasi Kesehatan baik di level pusat dengan fasilitas yang bisa dibilang *uptodate* dapat terjadi, lalu bagaimana pada fasilitas Kesehatan Tingkat pertama seperti puskesmas atau klinik yang infrastruktur dan sumberdaya manusianya belum siap menerapkan rekam medis elektronik. Bagi pasien, peristiwa semacam ini bukan sekadar isu teknis, melainkan pengalaman yang dapat menimbulkan rasa takut, hilangnya kepercayaan terhadap layanan kesehatan, dan potensi stigma sosial ketika informasi medis yang sangat pribadi tersebar secara tidak sah.

Pada kasus kebocoran data peserta BPJS Kesehatan di awal investigasi pada tahun 2021, tiga Lembaga yaitu Kemkominfo, BSSN, dan BPJS Kesehatan membentuk tim khusus untuk menelusuri dugaan kebocoran data ratusan juta peserta, mengidentifikasi data yang bocor

⁴⁵ Lihat Anonim, “**Pakar Keamanan Siber Sebut Dugaan Kebocoran Data Pasien sebagai Kejadian Fatal**” dalam <https://www.liputan6.com/health/read/4853250/data-pasien-covid-19-diduga-bocor-kemenkes-koordinasi-dengan-bssn>, diakses tgl. 11 Desember 2025

mencakup NIK, nama, alamat, dan riwayat kesehatan. Analisis menunjukkan faktor utama kebocoran adalah lemahnya kontrol akses, kurangnya edukasi keamanan siber, dan belum optimalnya penerapan standar keamanan. Sebagai tindak lanjut, Pemerintah melakukan pemutusan akses tautan yang menjual data dan mendorong penguatan keamanan data kesehatan. Sehingga dalam kasus ini walaupun UU Perlindungan Data Pribadi (UU PDP) sudah ada, implementasinya masih lemah, dan belum ada pihak yang dimintai pertanggungjawaban hukum secara spesifik karena proses investigasi digital yang kompleks.

Perkembangan Implikasi kasus terkini dan pengambilan langkah sebagai lanjutan kasus dimana kasus belum tuntas.⁴⁶ Proses hukum dan pertanggungjawaban atas kebocoran data BPJS Kesehatan 2021 belum selesai secara publik, menunjukkan kompleksitas penanganan kejahatan siber di Indonesia. Kasus ini menjadi pengingat terus-menerus akan kerentanan data kesehatan, mendorong penguatan tata kelola dan kontrol keamanan pada infrastruktur informasi kesehatan nasional, seperti yang ditegaskan dalam berbagai riset dan analisis. Kasus ini juga menegaskan tanggung jawab BPJS Kesehatan sebagai pengendali data dan perlunya perbaikan pengawasan serta penerapan hukum untuk menjamin privasi data pribadi warga negara.

⁴⁶ Lihat Yudianto Singgih, "Menelusuri Jejak Insiden Kebocoran Data Kesehatan" dalam <https://cyberhub.id/berita/jejak-insiden-kebocoran-data-kesehatan>, diakses ^{pada} tanggal 15 November 2025

Kasus kebocoran data BPJS Kesehatan 2021 masih menjadi sorotan, menegaskan urgensi implementasi hukum perlindungan data pribadi yang lebih efektif dan penguatan sistem keamanan siber di sektor kesehatan Indonesia, meskipun proses hukum dan pertanggungjawaban konkret masih terus berjalan dalam investigasi internal dan eksternal, kelemahan keamanan siber dalam penerapan RME di FKTP tidak boleh dipandang semata sebagai persoalan teknologi, tetapi sebagai persoalan perlindungan martabat manusia dan kepercayaan masyarakat terhadap sistem kesehatan. kurangnya infrastruktur teknologi dan pelatihan keamanan data pada tenaga kesehatan masih menjadi tantangan utama, dan menyerukan pentingnya penilaian dampak privasi serta penguatan tata kelola data pada seluruh fasilitas kesehatan. Dengan demikian, setiap upaya digitalisasi rekam medis di fasilitas kesehatan pertama harus disertai investasi yang memadai pada perangkat keras yang aman, sistem keamanan yang mutakhir (enkripsi, otentikasi berlapis, segmentasi jaringan), serta pelatihan berkelanjutan bagi tenaga kesehatan, agar manfaat RME akses cepat, data terintegrasi, pelayanan lebih baik tidak dibayar dengan mahal melalui kebocoran dan penyalahgunaan data yang merugikan pasien yang justru paling membutuhkan perlindungan .⁴⁷

⁴⁷ Lihat Anonim “**Tantangan Transformasi Digital dan Akses Layanan Kesehatan di Indonesia**” dalam <https://www.kompasiana.com/bemfisipunmul2025/68eb2616c925c44bc52a4c82/tantangan-transformasi-digital-dan-akses-layanan-kesehatan-di-indonesia>, diakses tgl. 13 Desember 2025

Situasi ini menggambarkan kesenjangan yang tajam antara regulatif dan kemampuan implementatif. Di satu sisi, Permenkes Nomor 24 Tahun 2022 menuntut puskesmas atau klinik mencapai standar tata kelola RME yang canggih. di sisi lain, negara belum sepenuhnya menjamin prasyarat minimum berupa infrastruktur, dukungan teknis, dan peningkatan kapasitas SDM. Akibatnya, kewajiban hukum yang semula dimaksudkan untuk memperkuat kualitas layanan dan melindungi hak pasien justru berpotensi menimbulkan risiko baru berupa kebocoran rekam medis elektronik. Kondisi ini menuntut adanya kebijakan afirmatif: penyesuaian bertahap (*phased implementation*), dukungan anggaran, template sistem yang aman, serta program pelatihan wajib, agar FKTP tidak hanya patuh secara formal terhadap pasal-pasal Permenkes, tetapi benar-benar mampu menyelenggarakan RME yang aman, dan berpihak pada hak privasi pasien.

B. Analisis Pertanggung Jawaban Hukum Terhadap Pihak Yang Menyebabkan Kebocoran Data Rekam Medis Elektronik Pasien di fasilitas Kesehatan pertama

Perkembangan teknologi informasi dan komunikasi telah memberikan pengaruh besar terhadap perubahan sosial, sikap, gaya hidup, dan pola perilaku manusia. Dalam konteks pelayanan kesehatan, salah satu isu penting yang mengemuka adalah hubungan antara kerentanan kebocoran rekam medis elektronik dan tata kelola kelembagaan, khususnya di tengah proses konsolidasi sistem kesehatan dan penegakan prinsip akuntabilitas. Di Indonesia, meskipun telah ada pengaturan sektoral, persoalan penegakan perlindungan rekam medis elektronik

masih menyisakan banyak celah, sehingga potensi penyalahgunaan data kesehatan oleh institusi ataupun pihak lain menjadi problem hukum yang belum sepenuhnya terjawab.⁴⁸

Teknologi informasi yang digunakan dalam layanan Kesehatan seperti sistem rekam medis elektronik berbasis komputer dan jaringan internet pada dasarnya dirancang untuk mempermudah proses pelayanan, meningkatkan efisiensi, dan mendukung pengambilan keputusan klinis. Namun, kehadiran teknologi ini sekaligus membawa dampak positif dan negatif yang signifikan bagi perlindungan hak pasien. Di satu sisi, rekam medis elektronik berkontribusi besar terhadap peningkatan mutu dan kesinambungan layanan kesehatan. Di sisi lain, teknologi yang sama dapat menjadi sarana efektif bagi terjadinya pelanggaran, seperti akses ilegal, manipulasi data, penyebaran informasi medis tanpa izin, hingga pemanfaatan data kesehatan untuk kepentingan komersial maupun diskriminatif yang merugikan pasien.⁴⁹ Gambaran konkret tentang besarnya risiko kebocoran data kesehatan tampak pada laporan awal Januari 2022 mengenai dugaan kebocoran sekitar 6 juta data pasien dari server Kementerian Kesehatan yang dijual di forum peretas “Raid Forums”, dengan ukuran file sekitar 720 GB yang diklaim berisi identitas pasien, hasil pemeriksaan radiologi, CT-scan, pemeriksaan laboratorium, rujukan BPJS, serta data medis lainnya.⁵⁰

⁴⁸ Akila Nuranisa, Diana Lukitasari, “Tindak Pidana Pencurian Data Dan Privasi Pengguna Dalam Transaksi E-Commerce (Studi Kasus Pada Aplikasi Tokopedia)”, *Jurnal Ilmu pertahanan, Politik dan Hukum Indonesia*, Vol.1, No.2/2024, hlm. 116

⁴⁹ *Ibid*, hlm. 116

⁵⁰ Lihat Agustinus Mario Damar, “Kemkominfo Usut Dugaan Kebocoran Data Pasien Milik Kemenkes”, dalam <https://www.liputan6.com/tekno/read/4853228/kemkominfo-usut-dugaan-kebocoran-data-pasien-milik-kemenkes>, diakses tgl. 13 Desember 2025

Peristiwa tersebut menunjukkan bahwa data Kesehatan termasuk yang berasal dari fasilitas kesehatan tingkat pertama dapat terkonsolidasi dalam sistem pusat dan menjadi target serangan berskala besar, sehingga setiap kelemahan pada level fasilitas (misalnya puskesmas yang tidak mengamankan kredensial akses) maupun pada level pusat memperkuat risiko kebocoran sistemik. Dalam situasi demikian, apabila terdapat bukti keterlibatan aktif atau pembiaran yang disengaja oleh pegawai fasilitas kesehatan dalam kebocoran rekam medis elektronik, misalnya dengan sengaja membocorkan atau memperjualbelikan data pasien, maka pola pertanggungjawaban yang mendekati strict liability terhadap lembaga dan/atau pelaku dapat dipertimbangkan, sepanjang unsur perbuatan, terjadinya kebocoran, dan kerugian atas data pasien terbukti secara objektif, sementara aspek pengaturan internal, pengawasan, dan pemenuhan standar keamanan menjadi parameter penting untuk menilai tingkat kesalahan dan cakupan pertanggungjawaban pidana.

Dalam konteks kebocoran rekam medis elektronik di fasilitas kesehatan tingkat pertama seperti puskesmas, terdapat beberapa pihak yang berperan dalam pengendalian dan pemrosesan data pasien, mulai dari tenaga kesehatan, pengelola rekam medis, hingga pengelola sistem informasi kesehatan yang mengatur proses input, pemrosesan, keluaran, penyimpanan, dan pengendalian data dalam aplikasi atau server internal. Kebocoran sering kali tidak hanya bergantung pada sistem internal puskesmas, tetapi juga melibatkan pihak ketiga, misalnya penyedia layanan komputasi awan atau vendor aplikasi rekam medis elektronik, yang turut mengelola infrastruktur dan keamanan data, sehingga setiap celah keamanan pada level ini dapat menjadi faktor penyebab insiden. Dalam kebocoran data akibat serangan

peretas dapat dikualifikasikan sebagai bentuk kelalaian dari pengendali atau pemroses data yang tidak menyediakan langkah pengamanan yang memadai, sehingga membuka peluang pertanggungjawaban pidana terhadap pengelola fasilitas maupun penyedia sistem.

1. Pertanggungjawaban hukum dalam kebocoran rekam medis elektronik medis elektronik

Dalam Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi pasal 35 yang berbunyi *Pengendali Data Pribadi wajib melindungi dan memastikan keamanan Data Pribadi yang diprosesnya, dengan melakukan: a. penyusunan dan penerapan langkah teknis 'operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan; dan b. penentuan tingkat keamanan Data Pribadi dengan memperhatikan sifat dan risiko dari Data Pribadi yang harus dilindungi dalam pemrosesan Data Pribadi.*

Untuk tindakan kebocoran rahasia yang terdapat dalam rekam medis elektronik oleh fasilitas Kesehatan Tingkat pertama dan jenis tanggung jawab yang terhadap kerahasiaan rekam medis adalah sebagai berikut:

a. Tanggung jawab perdata

Dalam hukum perdata yang bersifat privat dikenal prinsip umum bahwa setiap orang yang menimbulkan kerugian terhadap orang lain berkewajiban untuk memberikan ganti rugi. Prinsip ini menjadi landasan filosofis pertanggungjawaban

perdata ketika terjadi pelanggaran hak atau kepentingan hukum pihak lain oleh suatu perbuatan. Dalam konteks hubungan dokter dan pasien maupun fasilitas Kesehatan dan pasien, prinsip tersebut berfungsi sebagai mekanisme pemulihan bagi pasien yang dirugikan.

Dasar gugatan ganti rugi tercantum dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata yang mengatur mengenai perbuatan melawan hukum. Pasien yang merasa dirugikan dapat mengajukan gugatan perdata dengan mendalilkan bahwa pihak yang digugat telah melakukan suatu perbuatan melawan hukum yang menimbulkan kerugian baginya. Gugatan ini tidak hanya terbatas pada kerugian materiil, tetapi juga dapat mencakup kerugian immateriil sepanjang dapat dibuktikan dan dinilai secara hukum.

Agar tuntutan ganti rugi berdasarkan Pasal 1365 KUH Perdata dapat dikabulkan, terdapat beberapa unsur yang harus dibuktikan secara kumulatif. Pertama, pasien benar-benar mengalami kerugian. Kedua, terdapat perbuatan melawan hukum yang dilakukan pihak tergugat. Ketiga, terdapat kesalahan pada pihak pelaku, baik dalam bentuk kesengajaan maupun kelalaian. Keempat, harus ada hubungan kausal (sebab-akibat) antara perbuatan melawan hukum tersebut dengan kerugian yang timbul. Tanpa terpenuhinya unsur-unsur

ini, pertanggungjawaban perdata untuk pemberian ganti rugi tidak dapat dibebankan secara yuridis sah.⁵¹

b. Tanggungjawab administrasi

Dalam hubungan hukum antara fasilitas pelayanan kesehatan dan pasien, implikasi hukum administrasi terutama berkaitan dengan kebijakan dan ketentuan administratif yang menjadi prasyarat penyelenggaraan pelayanan kesehatan yang bermutu. Kebijakan ini mencakup, antara lain, kewajiban pemenuhan standar pelayanan, pemeliharaan sarana dan prasarana, pengelolaan rekam medis, serta pemenuhan hak pasien atas informasi dan kerahasiaan data kesehatan. Ketidakpatuhan terhadap ketentuan administratif tersebut tidak hanya menunjukkan rendahnya tata kelola, tetapi juga dapat dipandang sebagai pelanggaran terhadap kewajiban hukum fasilitas kesehatan dalam menjamin pelayanan yang aman dan berkualitas.

Pelanggaran terhadap kewajiban atau ketentuan hukum administrasi ini dapat menimbulkan sanksi administratif bagi fasilitas kesehatan, sanksi dapat berupa teguran, pembinaan khusus, pembekuan hingga pencabutan izin operasional, atau pencabutan status badan hukum apabila pelanggaran dinilai

⁵¹ I Susilowati *et.al*, “**Perlindungan Hukum terhadap Hak Privasi dan Data Medis Pasien di Rumah Sakit X Surabaya**”, *Jurnal Wiyata*, Vol.5, No.1/2018, hlm. 10

berat dan berulang. Sementara itu, bagi dokter dan tenaga kesehatan lainnya, pelanggaran kewajiban administrative termasuk kewajiban merahasiakan kondisi medis pasien dapat berujung pada sanksi berupa teguran lisan atau tertulis, hingga pencabutan surat izin praktik, sebagaimana selaras dengan pengaturan kewajiban menyimpan rahasia kedokteran dalam peraturan perundang-undangan yang berlaku.⁵²

c. Tanggungjawab pidana korporasi

Definisi korporasi menurut pasal 1 ayat 1 Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi adalah kumpulan orang dan atau kekayaan yang terorganisasi baik merupakan badan hukum maupun bukan badan hukum. Sementara menurut Undang Undang nomor 1 tahun 2023 tentang KUHP baru yang berlaku 3 tahun sejak tanggal diundangkan, yaitu tahun 2026, korporasi mencakup badan hukum yang berbentuk perseroan terbatas, yayasan, koperasi, badan usaha milik negara, badan usaha milik daerah, atau yang disamakan dengan itu, serta perkumpulan baik yang berbadan hukum maupun tidak berbadan hukum, badan usaha yang berbentuk firma, persekutuan komanditer, atau yang disamakan dengan itu sesuai dengan ketentuan peraturan perundang-undangan.

⁵² *Ibid*

Puskesmas atau klinik pada hakikatnya merupakan lembaga layanan kesehatan yang memenuhi kualifikasi sebagai subjek hukum berbentuk korporasi dalam arti luas, yakni organisasi yang memiliki struktur, kewenangan, dan fungsi yang diatur oleh peraturan perundang-undangan. Sebagai entitas yang mengelola sumber daya manusia, anggaran, serta sistem informasi, puskesmas tidak hanya menjalankan fungsi administratif dan pelayanan kesehatan, tetapi juga memegang tanggung jawab yuridis atas setiap tindakan yang lahir dari kebijakan, prosedur, maupun kelalaiannya.⁵³ Dalam perspektif hukum pidana, korporasi tidak lagi dipandang sekadar sebagai kumpulan individu, melainkan sebagai pelaku yang dapat melakukan tindak pidana dan oleh karenanya dapat dimintai pertanggungjawaban pidana ketika terjadi pelanggaran⁵⁴, termasuk dalam konteks kebocoran data rekam medis elektronik.

Apabila kebocoran data terjadi karena fasilitas kesehatan tingkat pertama tidak menyusun atau menerapkan prosedur keamanan yang layak, membiarkan celah akses tanpa pengawasan, atau lalai melakukan audit dan pelatihan, maka kegagalan tersebut

⁵³ Dinda Riskanita, “Tanggung Jawab Fasilitas Pelayanan Kesehatan terhadap Kerahasiaan Rekam Medis Pasien” *journal naureendigiton*, Vol.1, No.5/2023, hlm. 1128

⁵⁴ H.Setiyono, *Kejahatan Korporasi-Analisa Viktimologis dan Pertanggungjawaban Korporasi Dalam Hukum Pidana Indonesia*, Averroes Press, Malang, 2002, hlm. 16

mencerminkan kesalahan pada level kelembagaan,⁵⁵ sehingga wajar bila puskesmas diposisikan sebagai pelaku tindak pidana melalui konstruksi pertanggungjawaban korporasi.

Namun dalam penelitian yang dilakukan oleh peneliti kebocoran yang terjadi disebabkan oleh adanya keterlibatan tenaga kesehatan dalam kejadian kebocoran data, pertanggungjawabannya harus secara *Strict Liability* sesuai Pasal 36 KUHP yang mengatur *akibat yang disebabkan sebagian oleh perbuatan dan sebagian oleh kelalaian. Jika suatu perbuatan atau upaya untuk menyebabkan akibat tertentu merupakan perbuatan pidana, maka harus dipahami bahwa perbuatan yang menyebabkan akibat tersebut sebagian oleh perbuatan dan sebagian oleh kelalaian adalah perbuatan pidana yang sama dan juga dapat dijerat pasal 322 KUHP tentang rahasia jabatan: maka membocorkan rahasia jabatan, dalam hal ini rahasia kedokteran, adalah suatu tindak pidana yang dituntut atas pengaduan (klachdelict), apabila kejahatan itu ditujukan pada seseorang tertentu..*

Apabila kesalahan terjadi secara tidak sengaja, konsep vicarious liability dapat digunakan sebagai pertanggungjawaban dengan pembuktian kesalahan korporasi. Dalam hal ini, keterlibatan puskesmas dan vendor penyimpanan datanya menunjukkan

⁵⁵ Dinda Riskanita, *Op.Cit*, hlm. 1129

adanya kelalaian dalam sistem keamanan data. Kealpaan dalam tinjauan hukum pidana dapat dibagi menjadi kealpaan perbuatan dan kealpaan akibat, di mana kealpaan akibat menjadi relevan dalam konteks ini karena peristiwa pencurian data yang menyebabkan kerugian bagi pasien.⁵⁶ Dimana hal tersebut diatur dalam Pasal 70 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi ayat (1). Serta Pasal 46 ayat (1) Permenkes No. 24 Tahun 2022: *“Pimpinan Fasilitas Pelayanan Kesehatan bertanggung jawab terhadap penyelenggaraan dan keamanan rekam medis di fasilitas pelayanan kesehatan.”*

2. Upaya Pasien terhadap Kebocoran Informasi Kesehatan dalam Rekam Medis elektronik

Pasien sebagai penerima pelayanan kesehatan selalu dikaitkan dengan dibuatnya catatan riwayat medis dalam bentuk rekam medis. Pengaturan mengenai kepemilikan data rekam medis terdapat dalam UU Nomor 29 Tahun 2004 tentang Praktik Kedokteran dan Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis, yang menegaskan bahwa berkas rekam medis secara fisik merupakan milik fasilitas pelayanan kesehatan, sedangkan isi atau informasi yang tercantum di dalamnya adalah milik pasien. Ketentuan ini sejalan dengan Pasal 28H ayat (4) UUD 1945 yang menyatakan bahwa setiap orang berhak atas hak milik

⁵⁶ *Ibid*

pribadi dan hak tersebut tidak boleh dirampas secara sewenang-wenang oleh siapa pun, serta dengan prinsip umum hukum perdata tentang hak milik yang tetap berlaku berdasarkan Aturan Peralihan UUD 1945. Pasal 570 KUH Perdata, yang mengatur wewenang dan batas-batas pemegang hak milik, pada dasarnya juga dapat diterapkan terhadap kepemilikan atas isi rekam medis, sehingga kelalaian fasilitas kesehatan dalam menjaga kerahasiaan dan keamanan informasi dalam rekam medis bukan hanya melanggar hak privasi, tetapi sekaligus melanggar hak milik pasien atas data medisnya sendiri.

Hadirnya Undang Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi telah menjadi pedoman utama terkait pelanggaran atas kebocoran data pribadi. Undang-undang ini setidaknya membagi 2 pihak dalam pemrosesan data pribadi yaitu pertama, pengendali data pribadi yaitu "setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi. Kedua, Subjek data pribadi yaitu orang perseorangan yang pada dirinya melekat data pribadi. Dalam kaitannya dengan perlindungan data rekam medis pasien, tenaga kesehatan atau instansi kesehatan sebagai pengendali data pribadi dan pasien sebagai subjek data pribadi.⁵⁷

⁵⁷ M. R Faqy, "Urgensi Realisasi Peran Data Protection Officer (DPO) Pada Sektor Kesehatan Ditinjau Dari Hukum Perlindungan Data Pribadi", *Padjajaran Law Review*, Vol.10, No.1/2022, hlm. 173

Seorang pasien yang merasa dirugikan akibat kebocoran data pribadinya pada prinsipnya berhak menempuh upaya hukum melalui mekanisme hukum acara yang tersedia dalam peraturan perundang-undangan, baik perdata, pidana, maupun administrasi. Pilihan jalur ini memungkinkan pasien menuntut klarifikasi, pemulihan, dan pertanggungjawaban atas kerugian yang dialami, sepanjang dapat menunjukkan adanya pelanggaran kewajiban perlindungan data oleh lembaga pengelola. Dalam kerangka tersebut, pasien tidak ditempatkan sebagai pihak pasif, melainkan sebagai subjek hukum yang memiliki hak untuk menggugat, melapor, dan meminta pertanggungjawaban secara formal.

Hadirnya Undang-Undang Perlindungan Data Pribadi (UU PDP) memperkenalkan mekanisme tahapan yang perlu diperhatikan sebelum menempuh upaya hukum lebih jauh. Undang Undang ini mengatur kewajiban pengendali dan prosesor data untuk memberitahukan insiden kebocoran, melakukan penanganan insiden, serta menyediakan akses bagi subjek data untuk mengajukan keberatan, pengaduan, atau permintaan ganti rugi. Bagi pasien, pemahaman atas tahapan ini penting agar langkah yang diambil terarah mulai dari meminta penjelasan kepada pengendali data, mengajukan keberatan atau pengaduan, hingga menggugat ganti rugi jika kerugian nyata dapat dibuktikan. Secara ideal, tahapan ini menjadi jembatan antara pelanggaran teknis dan pemulihan hak secara substantif.⁵⁸

Masalahnya, hingga kini pemerintah belum sepenuhnya membentuk lembaga pengawas khusus yang diberi mandat operasional penuh melalui peraturan

⁵⁸ M.B. Bagaskara, “**Tanggung Jawab Rumah Sakit Terhadap Kerahasiaan Rekam Medis (Medical Record) di Masa Pandemi Covid-19**”, *Jurnal Analogi Hukum*, Vol.4, No1/2022. Hlm. 26

pemerintah untuk menangani pelanggaran pemrosesan data pribadi dan mengatur tata cara pengenaan ganti rugi secara rinci. Kekosongan kelembagaan ini membuat banyak ketentuan UU PDP bersifat “setengah jalan” dalam implementasi: norma ada, tetapi kanal penegakannya belum kokoh. Dalam praktik, pengaduan pasien sering kali kembali diarahkan ke kementerian atau lembaga pengendali data itu sendiri atau ke aparat penegak hukum umum, sehingga menimbulkan potensi konflik kepentingan dan ketidakpastian prosedural bagi korban kebocoran data.

Dengan kata lain, untuk saat ini beban pertanggungjawaban secara penuh baik secara teknis maupun kelembagaan masih lebih banyak berada pada kementerian atau lembaga terkait yang menjadi pengendali data, termasuk di sektor kesehatan. Situasi ini terlihat jelas dalam kasus dugaan kebocoran sekitar 6 juta data pasien Covid-19 milik Kementerian Kesehatan yang mencuat pada 2022, di mana penanganannya yang tampak lebih banyak berupa klarifikasi, penelusuran internal, dan koordinasi antar-instansi, tanpa kejelasan proses penetapan pelanggaran dan skema ganti rugi bagi pasien. Bagi korban, kondisi ini menimbulkan kesan bahwa lembaga yang seharusnya melindungi data justru menjadi satu-satunya pintu pengaduan, tanpa ada pengawas independen yang dapat menilai objektivitas dan kecukupan langkah yang diambil.⁵⁹

Keterbatasan infrastruktur digital dan perangkat teknologi di fasilitas kesehatan tingkat pertama (FKTP), terutama yang terletak di daerah pelosok, menjadi salah satu faktor utama yang menyebabkan kesenjangan antara regulasi

⁵⁹ Lihat Wahyu Andrianto, “Catatan Sederhana untuk Permenkes No. 24 Tahun 2022 tentang Rekam Medis” dalam <https://www.hukumonline.com/berita/a/catatan-sederhana-untuk-permenkes-no-24-tahun-2022-tentang-rekam-medis-lt6347ad6eb872d/?page=all>, diakses tgl. 16 Desember 2025

yang sudah ditetapkan dan kenyataan di lapangan. Meskipun undang-undang seperti UU Kesehatan, UU Perlindungan Data Pribadi (PDP), dan Permenkes 24 Tahun 2022 sudah memberikan pedoman yang jelas untuk melindungi data pasien, kenyataannya banyak FKTP yang belum memiliki infrastruktur yang memadai untuk mengimplementasikan perlindungan data sesuai standar yang telah ditentukan. Hal karena memang ketidakmampuan fasilitas kesehatan untuk menjalankan aturan tersebut dengan baik, sehingga data pasien tetap rentan.⁶⁰

Salah satu masalah utama yang sering muncul adalah minimnya sistem keamanan berlapis di FKTP. Keamanan data yang seharusnya mencakup lebih dari sekadar proteksi fisik perangkat, tetapi juga enkripsi data, autentikasi pengguna, dan pemantauan yang terus-menerus, sering kali tidak ada. Di banyak FKTP, terutama di daerah pelosok, perangkat yang digunakan masih terbatas dan tidak dilengkapi dengan fitur keamanan yang memadai. Tanpa perlindungan yang cukup, data rekam medis pasien lebih mudah diakses oleh pihak yang tidak berwenang, yang tentu saja bisa mengungkapkan informasi sensitif dan merugikan pasien.

Selain itu, kurangnya pemeliharaan server di FKTP juga menjadi masalah yang serius. Server yang tidak dikelola dengan baik atau tidak mendapatkan pembaruan sistem secara rutin membuka celah bagi potensi serangan dari luar. Tanpa pemeliharaan yang baik, data pasien menjadi rentan terhadap ancaman yang dapat merusak integritasnya. Bahkan, tanpa adanya backup data secara teratur, potensi kehilangan data yang sangat penting menjadi semakin besar, dan itu tentu

⁶⁰ Mellynia Yuniarti, *et.al*, “Implementasi Teori Organisasi Modern dalam Digitalisasi Pelayanan Publik: Studi Kasus BPJS Kesehatan”, *Management Studies and Entrepreneurship Journal*, Vol. 6, No.4/2025, hlm. 717

dapat berdampak negatif pada keselamatan pasien dan reputasi fasilitas kesehatan tersebut.

Keterbatasan sarana dan prasarana pada FKTP menggambarkan betapa tidak idealnya peraturan tentang rekam medis ini. Banyak FKTP yang masih mengandalkan perangkat yang tidak memenuhi standar keamanan yang diperlukan, seperti komputer jadul tanpa enkripsi dan jaringan internet yang tidak stabil. Tanpa adanya kontrol akses yang baik dan ruang server yang aman, akses oleh pihak yang tidak berwenang menjadi lebih mudah.⁶¹ Semua ini menciptakan sebuah situasi di mana data pasien yang sangat sensitif, seperti rekam medis, lebih mudah bocor dan jatuh ke tangan yang salah.

Dampak dari keterbatasan infrastruktur ini adalah tingginya risiko kebocoran data pasien. Tanpa perlindungan yang memadai, data rekam medis yang sangat pribadi dan penting bisa bocor atau jatuh ke tangan yang salah, baik karena kelalaian, kesalahan teknis, atau serangan siber. Jika kebocoran data terjadi, selain merugikan pasien, ini juga merusak reputasi fasilitas kesehatan dan dapat berujung pada sanksi hukum, baik berupa denda atau tindakan administratif berdasarkan UU PDP. Inilah mengapa penting untuk segera memperbaiki sarana dan prasarana di FKTP agar perlindungan data pasien bisa lebih maksimal.

Meskipun UU Perlindungan Data Pribadi (PDP) telah menyediakan mekanisme pertanggungjawaban pidana bagi pengendali data yang lalai, implementasinya di lapangan masih menghadapi banyak kendala. Salah satu

⁶¹ Budi Raharjo, *Analisis Bisnis secara Real Time dalam transformasi Digital*, Yayasan Prima Teknik, Semarang, 2024, hlm. 37

kendala utama adalah belum adanya peraturan pelaksana yang mengatur pedoman secara rinci mengenai penanganan kebocoran data, terutama yang berkaitan dengan rekam medis elektronik. Tanpa peraturan yang lebih spesifik, proses penanganan kasus kebocoran data menjadi tidak terstruktur dan membingungkan, sehingga sulit bagi aparat penegak hukum untuk mengambil langkah yang tepat, termasuk memberikan sanksi yang sesuai.

Selain itu, keterbatasan kapasitas aparat penegak hukum dalam melakukan forensik digital memperburuk situasi ini. Mengungkap dan menyelidiki kasus kebocoran data yang melibatkan rekam medis elektronik memerlukan keahlian teknis yang mendalam. Sayangnya, banyak aparat penegak hukum yang belum memiliki keterampilan atau alat yang cukup untuk melakukan investigasi forensik digital yang efektif.⁶² Akibatnya, banyak kasus kebocoran data yang hanya ditindaklanjuti secara administratif, tanpa adanya tindakan hukum yang jelas atau sanksi yang dapat memberikan efek jera kepada pelaku.

Semua ini menunjukkan kesenjangan besar antara regulasi yang ada dan pelaksanaannya di lapangan. Meskipun UU PDP sudah menetapkan mekanisme pertanggungjawaban pidana, ketidakmampuan dalam menangani kebocoran data secara teknis dan administrasi membuat penerapan sanksi hukum menjadi tidak efektif. Oleh karena itu, untuk mengatasi masalah ini, perlu ada peraturan pelaksana yang lebih rinci, serta peningkatan kapasitas aparat penegak hukum dalam bidang

⁶² Dwi Nurmayanti, Hudi Yusuf, “**Penerapan Digital Forensik Dalam Kasus Medikolegal**”, *Jurnal Intelek Insan Cendikia*, Vol .2, No. 8/ 2025, hlm. 4482

forensik digital. penegakan hukum terhadap kebocoran data bisa lebih efisien sehingga perlindungan data pasien bisa lebih terjamin.