
PERLINDUNGAN DATA PRIBADI DALAM MENCEGAH TINDAK PIDANA PENYALAHGUNAAN HAK PASIEN

Imelda Audry Chandra¹, Vieta Imelda Cornelis², Noenik Soekorini³

^{1,2,3}Program Studi Magister Ilmu Hukum, Fakultas Hukum,
Universitas Dr. Soetomo Surabaya

chandrainelda21@gmail.com

Abstrak

Kebocoran data pribadi, termasuk data pasien, menjadi masalah yang semakin sering muncul di era digital ini. Kasus-kasus pelanggaran privasi, peretasan data, dan penyalahgunaan informasi pribadi untuk kepentingan komersial atau tindakan kriminal lainnya menimbulkan kekhawatiran besar, terutama karena dampaknya yang merugikan pasien dan sistem kesehatan secara keseluruhan. Hal ini menuntut adanya perlindungan hukum yang memadai guna mencegah penyalahgunaan data pribadi pasien.

Pokok permasalahan yang akan dibahas dalam penulisan tesis ini adalah Bagaimana pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi pasien? dan Bagaimana perlindungan data pribadi dalam mencegah tindak pidana penyalahgunaan hak pasien?

Metode Pendekatan yang digunakan dalam penelitian ini adalah pendekatan yuridis normatif. Pendekatan yuridis normatif adalah menggunakan peraturan Perundang Undangan, menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum yang sedang ditangani. Dan pendekatan konseptual yang beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang di dalam ilmu hukum.

Kata Kunci: Perlindungan Data Pribadi, Tindak Pidana, Penyalahgunaan Hak Pasien .

Abstract

Personal data leaks, including patient data, are becoming an increasingly common problem in this digital era. Cases of privacy violations, data hacking, and misuse of personal information for commercial purposes or other criminal acts raise great concerns, especially because of their detrimental impact on patients and the health system as a whole. This requires adequate legal protection to prevent misuse of patient personal data.

The main issues that will be discussed in writing this thesis are: How is the criminal liability for perpetrators of misuse of patient personal data? and How is personal data protection in preventing criminal acts of abuse of patient rights?

The approach method used in this study is the normative legal approach. The normative legal approach is to use statutory regulations, examine all laws and regulations related to the legal issues being handled. And a conceptual approach that starts from the views and doctrines that develop in legal science.

Keywords: *Personal Data Protection, Criminal Acts, Abuse of Patient Rights.*

A. PENDAHULUAN

Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyebutkan bahwa negara Indonesia adalah negara hukum. Ini berarti bahwa Indonesia adalah negara yang berdasarkan atas hukum. Dengan sendirinya perlindungan hukum menjadi unsur esensial serta menjadi konsekuensi dalam negara hukum. Negara wajib menjamin hak-hak hukum warga negaranya. Perlindungan hukum merupakan pengakuan terhadap harkat dan martabat warga negaranya sebagai manusia.

Pembangunan nasional adalah rangkaian upaya pembangunan yang berkesinambungan yang meliputi seluruh aspek kehidupan masyarakat, bangsa dan negara, untuk melaksanakan tugas mewujudkan tujuan nasional sebagaimana dirumuskan dalam Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Rangkaian upaya pembangunan tersebut memuat kegiatan pembangunan yang berlangsung tanpa henti, dengan menaikkan tingkat kesejahteraan masyarakat dari generasi demi generasi. Pelaksanaan upaya tersebut dilakukan dalam konteks memenuhi kebutuhan masa sekarang tanpa mengurangi kemampuan generasi yang akan datang untuk memenuhi kebutuhannya.

Pembangunan kesehatan sebagai bagian integral dari Pembangunan nasional pada hakekatnya adalah penyelenggaraan upaya kesehatan untuk mencapai kemampuan hidup sehat bagi setiap penduduk untuk mewujudkan derajat kesehatan yang optimal dan merupakan andil yang besar bagi pengembangan dan pembinaan Sumber Daya Manusia sebagai Modal Pembangunan Nasional. Adapun salah satu tujuan Pembangunan Nasional adalah menuju Indonesia sehat 2030 yaitu dengan meningkatkan mutu sumber daya masyarakat yang sehat, cerdas dan produktif, serta mampu memelihara dan meningkatkan derajat kesehatan masyarakat disertai komitmen yang tinggi terhadap kemanusiaan, etika dan dilaksanakan dengan semangat pemberdayaan maka pembangunan kesehatan

diselenggarakan dengan prioritas pada upaya peningkatan (promotif), pencegahan (preventif), penyembuhan (kuratif), dan pemulihan (rehabilitasi).

Perlu diketahui bahwa Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 sebetulnya menata tentang perlindungan data pribadi yang dijelaskan pada Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang berbunyi bahwa setiap orang berhak atas perlindungan data pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.

Persoalan perlindungan terhadap data pribadi muncul karena keprihatinan akan pelanggaran privasi yang dapat dialami oleh orang dan atau badan hukum. Pelanggaran privasi tersebut dapat menimbulkan kerugian yang tidak hanya bersifat materiil tetapi juga moral yaitu berupa hancurnya nama baik seseorang atau lembaga.

Data pribadi di bidang kesehatan pun tidak terlepas dari kemungkinan penyalahgunaan. Akan lebih bahaya lagi apabila data pribadi tersebut merupakan suatu data jejak rekam medis pasien yang memang bersifat sangat rahasia, sehingga ada beberapa peraturan khusus seperti diantaranya Undang-Undang Nomor 29 tahun 2004 tentang Praktik Kedokteran yang mengatur bahwa setiap Dokter dan Dokter Gigi dalam menyelenggarakan praktik kedokteran harus membuat rekam medis dan rekam medis ini harus dijaga kerahasiaannya oleh Dokter atau Dokter Gigi dan pimpinan sarana pelayanan kesehatan. Kemudian, Peraturan Menteri Kesehatan Nomor 269 tahun 2008 tentang Rekam Medis menyebutkan bahwa meskipun informasi tentang identitas, diagnosis, riwayat penyakit, riwayat pemeriksaan dan riwayat pengobatan pasien harus dijaga kerahasiaannya oleh klinisi, petugas pengelola dan pimpinan sarana kesehatan, namun informasi ini dapat dibuka antara lain untuk memenuhi permintaan aparat penegak hukum atas perintah pengadilan dan memenuhi permintaan institusi/lembaga sesuai dengan ketentuan perundang-undangan.

Permintaan tersebut harus disampaikan secara tertulis kepada pimpinan Rumah Sakit. Selain itu, Permenkes ini juga mengatur mengenai kepemilikan, manfaat dan tanggung jawab dalam mengelola Rekam Medis. Berkas rekam medis adalah milik sarana pelayanan kesehatan dan isinya yang berupa ringkasan rekam medis merupakan milik pasien. Ringkasan tersebut dapat diberikan, dicatat atau dicopy oleh pasien atau orang

yang diberi kuasa atau atas persetujuan tertulis pasien atau keluarganya yang berhak untuk itu.

Kebocoran data pribadi, termasuk data pasien, menjadi masalah yang semakin sering muncul di era digital ini. Kasus-kasus pelanggaran privasi, peretasan data, dan penyalahgunaan informasi pribadi untuk kepentingan komersial atau tindakan kriminal lainnya menimbulkan kekhawatiran besar, terutama karena dampaknya yang merugikan pasien dan sistem kesehatan secara keseluruhan. Hal ini menuntut adanya perlindungan hukum yang memadai guna mencegah penyalahgunaan data pribadi pasien.

Untuk menjawab tantangan ini, pemerintah Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini diharapkan menjadi dasar hukum yang kuat dalam melindungi data pribadi warga negara, termasuk data kesehatan. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mengatur berbagai ketentuan yang berkaitan dengan pemrosesan, penyimpanan, dan pengamanan data pribadi, serta sanksi bagi pihak yang melanggar aturan tersebut.

Perlindungan hukum adalah semua langkah guna melengkapi kebebasan serta membantu menjamin keadaan tenang kepada saksi ataupun korban yang sangat terjamin. Perlindungan regulasi dalam lingkungannya mencakup secara luas dalam segi tata hukumnya. Mencakup dari bidang hukum, ekonomi, sosial, dan budaya. Informasi atau data pribadi sudah dianggap sangat penting untuk dijaga kerahasiannya, bahkan informasi atau data pribadi sudah menjadi salah satu kunci dalam sebuah komponen beberapa bidang. Perlindungan data pribadi saat ini semakin penting karena adanya perkembangan teknologi informasi yang memungkinkan pengumpulan dan pengolahan data dalam skala besar. (Mahrani, P, Maulina, N. 2020:1-8)

Berdasarkan uraian latar belakang permasalahan tersebut, mendorong penulis melakukan penelitian dan untuk itu tertarik memilih judul” Perlindungan Data Pribadi dalam Mencegah Tindak Pidana Penyalahgunaan Hak Pasien”

Berdasarkan uraian yang telah dikemukakan di atas, maka permasalahan yang timbul dalam penelitian ini adalah:

- a. Bagaimana pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi pasien?

- b. Bagaimana perlindungan data pribadi dalam mencegah tindak pidana penyalahgunaan hak pasien?

B. METODE PENELITIAN

Didalam penelitian hukum terdapat beberapa pendekatan akan tetapi dalam penelitian ini pendekatan yang digunakan adalah pendekatan yuridis normatif. pendekatan yuridis normatif merupakan pendekatan peraturan perundang-undangan (*Statute Approach*), di lakukan dengan menelaah semua Undang-undang dan regulasi yang bersangkutan paut dengan isu hukum yang sedang ditangani. Dan pendekatan konseptual (*Conceptual Approach*), beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum.

C. HASIL DAN PEMBAHASAN

Pertanggungjawaban Pidana Terhadap Pelaku Penyalahgunaan Data Pribadi Pasien

Pertanggungjawaban pidana adalah pengenaan hukuman kepada pencipta atas perbuatan yang melanggar larangan atau menciptakan keadaan yang dilarang. Pertanggungjawaban pidana dengan demikian mengacu pada proses pemidahan pidana yang ada dalam suatu tindak pidana kepada pelakunya. Tanggungjawab seseorang dalam hukum pidana terdiri atas kelanjutan dari pemindaan yang telah ada secara obyektif atas tindak pidana secara subyektif bagi penciptanya.

Pertanggungjawaban pidana ditentukan berdasarkan pada kesalahan pembuat dan bukan hanya dengan dipenuhinya seluruh unsur tindak pidana. Dengan demikian kesalahan ditempatkan sebagai faktor penentu pertanggungjawaban pidana dan tak hanya dipandang sekedar unsur mental dalam tindak pidana.

Seseorang dinyatakan mempunyai kesalahan merupakan hal yang menyangkut masalah pertanggungjawaban pidana. (Admaja Priyatno, 2004:15) Untuk dapat mengenakan pidana pada pelaku karena melakukan tindak pidana, aturan hukum mengenai pertanggungjawaban pidana berfungsi sebagai penentu syarat-syarat yang harus ada pada diri seseorang sehingga sah jika dijatuhi hukuman. Pertanggungjawaban pidana mengacu pada pertanyaan tentang siapa yang melakukan kejahatan, sedangkan aturan pertanggungjawaban pidana adalah aturan tentang bagaimana menangani pelaku. Perbuatan yang dilarang oleh masyarakat harus dikaitkan dengan pelakunya, yang berarti

bahwa hukuman obyektif untuk hukuman tersebut kemudian diteruskan kepada terdakwa. Pertanggungjawaban pidana bukan karena kesalahan pelaku tidak dapat dimintai pertanggungjawaban. Jadi ada orang yang tidak dapat diadili dan dipidana kecuali melakukan tindak pidana. Tetapi meskipun dia melakukan perbuatan pidana tidak selalu dia dapat dipidana.

Pertanggungjawaban pidana mengandung pengertian bahwa setiap orang yang melakukan suatu kejahatan atau melanggar hukum, sebagaimana ditentukan dalam undang-undang, orang itu harus mempertanggungjawabkan perbuatannya menurut kesalahannya, dengan kata lain orang yang melakukan suatu kejahatan, akan bertanggungjawab. Untuk fakta dengan kejahatan jika memiliki kesalahan, seseorang memiliki kesalahan jika, pada saat melakukan tindakan, dari sudut pandang masyarakat, ia memiliki sudut pandang normative sehubungan dengan kesalahan yang telah dilakukannya.

Pertanggungjawaban Pidana dapat diberikan apabila memenuhi syarat-syarat dari sebuah kesalahan yang dimana kesalahannya terdapat dalam kegagalan melindungi sebuah Data Pribadi, jika dilihat kesalahan tersebut sudah memenuhi unsur-unsur dari sebuah kesalahan sebagaimana yang telah dijelaskan dalam Bab 2 tentang Pertanggungjawaban Pidana.

Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi ini jika terjadinya sebuah kegagalan dalam melindungi Data Pribadi hanya dikenakan sebuah sanksi administrasi saja sebagaimana yang telah tertulis dalam Pasal 57

Pasal 57

- 1) Pelanggaran terhadap ketentuan Pasal 20 ayat (1), Pasal 21, Pasal 24, Pasal 25 ayat (2), Pasal 26 ayat (3), Pasal 27, Pasal 28, Pasal 29, Pasal 30, Pasal 31, Pasal 32 ayat (1), Pasal 33, Pasal 34 ayat (1), Pasal 35, Pasal 36, Pasal 37, Pasal 38, Pasal 39 ayat (1), Pasal 40 ayat (1), Pasal 41 ayat (1) dan ayat (3), Pasal 42 ayat (1), Pasal 43 ayat (1), Pasal 44 ayat (1), Pasal 45, Pasal 46 ayat (1), Pasal 49, Pasal 51 ayat (1) dan ayat (5), Pasal 52, Pasal 53 ayat (1), Pasal 55 ayat (2), dan Pasal 56 ayat (2) sampai dengan ayat (4) dikenakan sanksi administrative.
- 2) Sanksi administratif sebagaimana yang dimaksud pada ayat (1) berupa:
 - a. peringatan tertulis.
 - b. penghentian sementara kegiatan pemrosesan Data Pribadi.

- c. penghapusan atau pemusnahan Data Pribadi; dan/atau
 - d. denda administratif.
- 3) Sanksi administratif berupa denda administrative sebagaimana dimaksud pada ayat (2) huruf d paling tinggi 2 (dua) persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.
 - 4) Penjatuhan sanksi administratif sebagaimana dimaksud pada ayat (2) diberikan oleh lembaga.
 - 5) Ketentuan lebih lanjut mengenai tata cara pengenaan sanksi administratif sebagaimana dimaksud pada ayat (3) diatur dalam Peraturan Pemerintah.

Untuk mencegah penyalahgunaan data pribadi, ini harus menjadi titik kritis/poin penting dalam Undang-Undang Perlindungan Data Pribadi. Pihak rumah sakit melakukan penyalahgunaan data pribadi pasien dan tidak dapat melindungi Data Pribadi pasien maka dapat diberikan sanksi pidana karena melakukan kesalahannya dan dapat mempertanggungjawabkan perbuatannya. Dalam hal ini pihak rumah sakit dapat di jerat dengan Pasal 67 Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Pasal 67

- 1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
- 2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp 4.000.000.000,00 (empat miliar rupiah)
- 3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana

dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Dalam analisis yuridis, ketentuan ini dapat dijelaskan sebagai berikut:

a. Setiap orang

Ketentuan ini menunjukkan bahwa siapapun baik perseorangan ataupun lembaga hukum, termasuk organisasi pemerintah atau swasta, harus mematuhi ketentuan ini

b. Dilarang secara melawan hukum

Ketentuan ini menunjukkan bahwa tindakan mengungkapkan atau menunjukkan data yang bersifat pribadi atau privasi bukan miliknya harus dianggap sebagai pelanggaran hukum. Tindakan melanggar ketentuan ini dapat dikenakan sanksi pidana dan/atau perdata

c. Mengungkapkan data pribadi yang bukan miliknya

Ketentuan ini menunjukkan bahwa tindakan mengungkapkan data pribadi yang bukan milik seseorang, walaupun itu dengan sengaja atau tidak, merupakan tindakan dilarang.

Ketentuan sanksi pidana sebagaimana dijelaskan di atas diberikan bagi orang yang secara sadar dan melawan hukum memperoleh atau mengumpulkan Data Pribadi, mengungkapkan Data Pribadi, menggunakan Data Pribadi milik pasien. Kegagalan dalam melindungi data pribadi dapat menyebabkan sebuah kesalahan yang dimana rumah sakit maupun orang lain dapat dengan sengaja menggunakan Data Pribadi pasien dengan sembarangan yang dapat menyebabkan kerugian bagi pemilik Data Pribadi.

Setiap orang maupun korporasi seperti Rumah Sakit harus memahami bahwa data pribadi adalah hak privasi yang harus dilindungi. Karena itu, penggunaan, pengungkapan, dan pemrosesan data pribadi harus dijalankan dengan langkah yang sah serta wajar, kemudian tidak merugikan pemilik data pribadi. Ketentuan ini juga menunjukkan bahwa setiap tindakan dilarang terhadap ketentuan ini bisa dikenai sebuah sanksi pidana dan/atau perdata. Hal ini menunjukkan betapa pentingnya hak privasi dan keamanan data pribadi bagi masyarakat dan negara, sehingga diperlukan perlindungan yang kuat untuk menghindari penyalahgunaan dan pelanggaran atas hak privasi ini

Perlindungan Data Pribadi Dalam Mencegah Tindak Pidana Penyalahgunaan Hak Pasien

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang pada tahun 2022 diundangkan di Indonesia, telah membawa perubahan signifikan bagaimana cara data pribadi harus dikelola, terutama dalam konteks fasilitas kesehatan. Data pribadi dalam sektor kesehatan mencakup informasi yang sangat sensitif tentang pasien, seperti riwayat medis, hasil tes laboratorium, kondisi kesehatan, dan data identifikasi pribadi. Keamanan data ini sangat penting karena dapat digunakan untuk mengidentifikasi individu, dan jika jatuh ke tangan yang salah, dapat memiliki konsekuensi serius. Oleh karena itu, perlindungan data pribadi pasien adalah kunci dalam menjaga privasi, keamanan, dan kepercayaan dalam layanan kesehatan.

Adapun langkah konkret dalam mencegah Penyalahgunaan Data Pribadi hak Pasien di Rumah Sakit, langkah konkret yang bisa dilakukan oleh rumah sakit untuk melindungi data pribadi pasien sebagai berikut:

a. **Enkripsi Data**

Data pasien yang disimpan dalam sistem rumah sakit harus dienkripsi, baik saat data tersebut disimpan (data at rest) maupun saat sedang dikirimkan (data in transit). Dengan enkripsi, meskipun data berhasil diakses oleh pihak yang tidak berwenang, mereka tidak bisa memahami isi data tersebut tanpa kunci dekripsi. Enkripsi data dapat membantu melindungi data pribadi dari akses yang tidak sah.

b. **Akses Terbatas dan Otentikasi Multi-Faktor (MFA)**

Hanya petugas yang berwenang yang diizinkan untuk mengakses data pasien, dan hal ini perlu diperkuat dengan otentikasi multi-faktor (MFA). Setiap pengguna harus memasukkan lebih dari satu faktor untuk membuktikan identitasnya, seperti kata sandi dan kode verifikasi yang dikirimkan melalui SMS atau email.

c. **Pemantauan Aktivitas Sistem dan Audit Berkala**

Rumah sakit harus memantau secara aktif aktivitas yang terjadi di sistem manajemen data pasien. Sistem keamanan yang baik akan mencatat siapa yang mengakses data, kapan, dan untuk tujuan apa. Audit berkala diperlukan untuk mendeteksi potensi pelanggaran dan memastikan bahwa kebijakan keamanan diterapkan dengan baik.

d. **Penggunaan Firewall dan *Intrusion Detection System* (IDS)** Firewall digunakan untuk melindungi jaringan rumah sakit dari akses yang tidak sah, sedangkan

Intrusion Detection System (IDS) berfungsi untuk mendeteksi aktivitas mencurigakan atau serangan terhadap sistem. Kedua teknologi ini membantu menjaga data pasien dari serangan siber eksternal.

e. **Pelatihan Rutin untuk Staf Kesehatan**

Sumber daya manusia di rumah sakit merupakan faktor krusial dalam menjaga keamanan data. Pelatihan rutin mengenai praktik keamanan siber, seperti cara menghindari email phishing dan menjaga kerahasiaan akses, sangat penting untuk memastikan bahwa seluruh staf memahami peran mereka dalam menjaga data pasien.

f. **Pembaruan Sistem secara Teratur**

Sistem manajemen data pasien harus selalu diperbarui agar tetap aman dari kerentanan. Pembaruan perangkat lunak dan patch keamanan harus dilakukan sesegera mungkin begitu tersedia untuk menutup celah yang bisa dimanfaatkan oleh penyerang.

g. **Kebijakan Privasi dan Persetujuan Pasien**

Sistem harus memungkinkan Fasilitas Kesehatan untuk mengelola persetujuan pasien dengan baik. Ini mencakup pemantauan persetujuan, pembaruan, dan penghapusan persetujuan jika diperlukan.

h. **Backup Data Berkala**

Data pasien harus secara rutin dibackup di tempat yang aman. Ini penting agar rumah sakit memiliki salinan data yang bisa dipulihkan jika terjadi serangan siber, bencana, atau kegagalan sistem.

Selanjutnya Untuk memitigasi risiko kebocoran data, rumah sakit harus memiliki rencana tanggap darurat yang komprehensif, termasuk:

a. **Penilaian Risiko Secara Berkala**

Rumah sakit harus melakukan penilaian risiko siber secara berkala untuk mengidentifikasi potensi ancaman baru dan kelemahan dalam sistem keamanan yang ada.

b. **Rencana Pemulihan Bencana (Disaster Recovery Plan)**

Rencana ini memastikan bahwa data pasien dapat dipulihkan dengan cepat setelah insiden seperti serangan ransomware atau bencana alam. Hal ini melibatkan proses backup otomatis, tes pemulihan, dan dokumentasi yang rinci.

c. **Penunjukan Petugas Keamanan Data (Data Protection Officer/DPO)**

Rumah sakit wajib memiliki petugas yang bertanggung jawab khusus terhadap keamanan data pasien. DPO akan memastikan bahwa regulasi dan kebijakan yang terkait dengan perlindungan data pribadi diterapkan dengan benar.

d. **Respons Insiden yang Cepat dan Terencana**

Jika terjadi pelanggaran data, rumah sakit harus memiliki tim respons insiden yang dapat segera mengidentifikasi, mengisolasi, dan mengatasi masalah sebelum menjadi lebih besar. Komunikasi dengan pasien yang terdampak harus dilakukan secara transparan sesuai aturan.

Adapun Langkah-langkah perlindungan data pasien di atas harus didukung dengan pemahaman dan penerapan regulasi yang berlaku di Indonesia. Beberapa aturan utama terkait perlindungan data pasien meliputi:

- a. **Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)** Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang disahkan pada tahun 2022 menjadi dasar hukum utama dalam perlindungan data pribadi di Indonesia. Dalam konteks rumah sakit, Undang-undang ini mengatur bahwa data pasien hanya boleh diakses, digunakan, dan disimpan dengan persetujuan pasien, dan harus ada langkah-langkah teknis serta organisasi yang memadai untuk melindungi data tersebut.
- b. **Peraturan Menteri Kesehatan No. 269/MENKES/PER/III/2008** Peraturan ini mengatur rekam medis dan kewajiban rumah sakit dalam menjaga kerahasiaan data pasien. Setiap data medis yang dikumpulkan harus dijaga kerahasiaannya, dan hanya boleh dibuka dengan izin pasien atau jika diharuskan oleh hukum.
- c. **Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik** Peraturan ini mewajibkan penyelenggara sistem elektronik, termasuk rumah sakit yang menggunakan sistem elektronik untuk manajemen data pasien, untuk menjaga keamanan sistem tersebut dan memastikan bahwa data pribadi yang diproses dijaga kerahasiaannya.
- d. **Peraturan Menteri Kominfo Nomor 20 Tahun 2016** Regulasi ini mengatur perlindungan data pribadi dalam sistem elektronik, yang juga mencakup layanan kesehatan berbasis teknologi informasi. Rumah sakit harus memastikan bahwa sistem elektronik yang mereka gunakan mematuhi standar keamanan yang ditetapkan dalam peraturan ini.

Perlindungan data pasien adalah prioritas utama bagi setiap rumah sakit di era digital. Dengan menerapkan langkah-langkah konkret dalam mencegah Penyalahgunaan Data Pribadi Pasien di Rumah Sakit seperti enkripsi, pembatasan akses, pemantauan sistem, dan pelatihan staf, rumah sakit dapat mengurangi risiko kebocoran data. Selain itu, pemahaman dan penerapan regulasi yang ada di Indonesia, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi PDP, sangat penting untuk memastikan bahwa data pasien dilindungi sesuai dengan hukum yang berlaku. Perlindungan data bukan hanya soal teknologi, tetapi juga tanggung jawab bersama para jajaran management setiap rumah sakit.

D. KESIMPULAN

Kesimpulan

Pihak rumah sakit apabila melakukan penyalahgunaan data pribadi pasien dan tidak dapat melindungi Data Pribadi pasien maka dapat diberikan sanksi pidana karena melakukan kesalahannya dan dapat mempertanggungjawabkan perbuatannya. Dalam hal ini pihak rumah sakit dapat di jerat dengan Pasal 67 Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Perlindungan data pribadi dalam mencegah tindak pidana penyalahgunaan hak pasien maka rumah sakit melakukan perlindungan enkripsi data, akses terbatas dan otentikasi Multi-Faktor (MFA), Pemantauan aktivitas sistem dan audit berkala, penggunaan firewall dan *Intrusion Detection System* (IDS), pelatihan rutin untuk staf Kesehatan, Pembaruan Sistem secara Teratur, Kebijakan Privasi dan Persetujuan Pasien, Backup Data Berkala, Selain itu untuk memitigasi risiko kebocoran data rumah sakit juga harus memiliki rencana tanggap darurat yang komprehensif seperti penilaian risiko secara berkala, rencana pemulihan bencana (Disaster Recovery Plan), penunjukan petugas keamanan data (Data Protection Officer/DPO), respons insiden yang cepat dan terencana. Disamping itu pemahaman dan penerapan regulasi yang ada di Indonesia, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, sangat penting untuk memastikan bahwa data pasien dilindungi sesuai dengan hukum yang berlaku.

Saran

Adanya peraturan yang tegas dan memadai untuk dapat memberikan keamanan bagi pengguna teknologi informasi guna meningkatkan pelayanan kesehatan berbasis teknologi, penting juga pembentukan lembaga yang berfungsi sebagai regulator, pengawas, dan pengendali (independent regulatory body), atau sebuah komisi perlindungan data pribadi. Tugas pengawasan ini justru diserahkan kepada pemerintah, sesuai dengan sektornya masing-masing, dengan berkoordinasi kepada Menteri Komunikasi dan Informatika. Ini berarti Kementerian Dalam Negeri akan mengawasi data pribadi yang terkait dengan kependudukan, OJK akan mengawasi data pribadi yang terkait dengan keuangan dan perbankan, dan Kementerian Kesehatan akan mengawasi data pribadi yang terkait dengan rekam medis pasien

Diharapkan dengan adanya peraturan yang tegas dan memadai dapat memberikan keamanan bagi pengguna teknologi informasi dan juga khususnya dapat meningkatkan pelayanan kesehatan berbasis teknologi dengan adanya sanksi pidana juga dapat memberikan efek jera terhadap pelaku penyalahgunaan data pribadi. Serta disarankan adanya kerja sama antara 2 aspek, yaitu aspek dari platform media sosial itu sendiri dan pemerintah selaku pembuat kebijakan dalam hal perlindungan data pribadi.

DAFTAR PUSTAKA

Admaja Priyatno, (2004). *Kebijakan Legislasi Tentang Sistem Pertanggungjawaban Pidana Korporasi di Indonesia*, CV. Utomo, Bandung.

Jurnal

Maharani, P, Maulina, N. (2020). Perlindungan data pribadi dalam perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). *Jurnal Kajian Informasi dan Perpustakaan*, Vol. 8, No. 1: 1-8

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Pidana (KUHP).

Kitab Undang-Undang Hukum Acara Pidana (KUHAP)

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor
11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)