E-ISSN: 3025-0994
Halaman 7659-7669
Volume 4 Nomor 3 Tahun 2026

Pertanggungjawaban Direksi Rumah Sakit atas Kebocoran Rekam Medis Elektronik dalam Hukum Korporasi

Ario Bimo Hanggono

Fakultas Kedokteran dan Kesehatan Universitas Muhammadiyah Jakarta
e-mail: ario.hanggono@umj.ac.id

Abstrak

Transformasi digital pelayanan kesehatan mendorong penggunaan Rekam Medis Elektronik (RME), tetapi sekaligus meningkatkan risiko kebocoran data pasien dan menimbulkan persoalan mengenai pertanggungjawaban direksi rumah sakit. Penelitian ini menganalisis konstruksi tanggung jawab direksi terhadap kebocoran RME berdasarkan hukum korporasi Indonesia serta penerapan prinsip tata kelola perusahaan dalam pelindungan data kesehatan. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan konseptual. Bahan hukum primer dan sekunder dianalisis secara kualitatif melalui penafsiran gramatikal, sistematis, dan teleologis. Hasil penelitian menunjukkan bahwa kewajiban direksi tidak berhenti pada pengelolaan operasional rumah sakit, tetapi mencakup pembangunan kebijakan keamanan informasi, pengendalian internal, audit, manajemen risiko, dan kepatuhan terhadap regulasi pelindungan data. Penilaian tanggung jawab direksi bertumpu pada fiduciary duty, duty of care, Business Judgment Rule, dan Good Corporate Governance. Kebocoran data dapat melahirkan tanggung jawab pribadi apabila terjadi kelalaian dalam pengurusan perseroan, sedangkan keputusan yang diambil dengan itikad baik, informasi memadai, dan kehati-hatian dapat memperoleh perlindungan Business Judgment Rule. Harmonisasi hukum korporasi, kesehatan, dan pelindungan data diperlukan untuk memperkuat kepastian hukum dan akuntabilitas rumah sakit.

Kata Kunci: *Pertanggungjawaban Direksi, Rumah Sakit, Rekam Medis Elektronik, Hukum Korporasi, Pelindungan Data, Tata Kelola Perusahaan*

Abstract

The digital transformation of healthcare services has encouraged the adoption of Electronic Medical Records (EMRs), while simultaneously increasing the risk of patient data breaches and raising legal questions concerning the accountability of hospital directors. This study analyzes the legal construction of directors' liability for EMR data breaches under Indonesian corporate law and examines the application of corporate governance principles in protecting health data. This research employs a normative legal method using statutory and conceptual approaches. Primary and secondary legal materials were analyzed qualitatively through grammatical, systematic, and teleological interpretation. The findings demonstrate that the

duties of hospital directors extend beyond operational management and include establishing information security policies, internal controls, audits, risk management systems, and compliance with data protection regulations. The assessment of directors' liability is based on the principles of fiduciary duty, duty of care, the Business Judgment Rule, and Good Corporate Governance. A data breach may result in personal liability when it arises from negligence in managing the company, whereas decisions made in good faith, based on adequate information, and with due care may receive protection under the Business Judgment Rule. Harmonization among corporate law, health law, and data protection law is therefore necessary to strengthen legal certainty and hospital accountability.

***Keywords**: Directors' Liability, Hospitals, Electronic Medical Records, Corporate Law, Data Protection, Corporate Governance*

LATAR BELAKANG

Pendahuluan memuat tentang latar belakang, landasan teori, masalah, rencana Transformasi digital di sektor kesehatan telah mengubah paradigma penyelenggaraan pelayanan kesehatan melalui penggunaan sistem informasi yang terintegrasi. Salah satu bentuk utamanya adalah Rekam Medis Elektronik (RME), yaitu pencatatan informasi kesehatan pasien dalam format digital yang dapat mendukung kesinambungan pelayanan, efisiensi administrasi, dan pengambilan keputusan klinis. Di Indonesia, percepatan penerapan RME memperoleh landasan normatif melalui Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan dan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis [3], [4]. Kajian implementasi menunjukkan bahwa adopsi RME di rumah sakit Indonesia terus berkembang, tetapi masih menghadapi persoalan kesiapan organisasi, sumber daya manusia, infrastruktur, interoperabilitas, dan keamanan data [5].

Karakter data kesehatan yang sangat sensitif membuat kebocoran RME tidak hanya menimbulkan kerugian ekonomi, tetapi juga dapat melanggar hak privasi, merusak reputasi rumah sakit, mengurangi kepercayaan masyarakat, dan mengganggu kesinambungan layanan. Literatur keamanan RME menempatkan kerahasiaan, integritas, ketersediaan, autentikasi, dan akuntabilitas sebagai unsur yang harus dikelola secara bersamaan [8], [9]. Dalam konteks Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menetapkan data kesehatan sebagai data pribadi yang bersifat spesifik dan membebankan kewajiban kepada pengendali data untuk memastikan pemrosesan yang sah, aman, dan bertanggung jawab [2].

Persoalan kebocoran data sering dipahami sebagai kegagalan teknis pada unit teknologi informasi. Pandangan tersebut terlalu sempit karena keputusan mengenai anggaran keamanan, struktur pengendalian, pembagian kewenangan, audit, manajemen risiko, dan respons insiden berada dalam lingkup tata kelola organisasi. Penelitian mengenai keamanan data pasien menunjukkan bahwa risiko tidak hanya berasal dari serangan siber, tetapi juga dari kebijakan internal yang tidak jelas, pengendalian akses yang lemah, keterbatasan kompetensi pegawai, serta budaya keamanan yang belum matang [6], [7]. Dengan demikian,

kebocoran RME perlu dinilai sebagai risiko korporasi yang melekat pada fungsi pengurusan rumah sakit.

Dalam rumah sakit yang diselenggarakan oleh badan hukum perseroan, direksi merupakan organ yang berwenang dan bertanggung jawab penuh atas pengurusan perseroan untuk kepentingan perseroan sesuai maksud dan tujuannya. Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas menempatkan direksi pada posisi sentral dalam pengambilan keputusan, pelaksanaan pengendalian internal, dan representasi perseroan [1]. Posisi tersebut menimbulkan pertanyaan yuridis mengenai batas tanggung jawab direksi apabila terjadi kebocoran data pasien: apakah tanggung jawab cukup dibebankan kepada rumah sakit sebagai badan hukum, atau dapat pula beralih menjadi tanggung jawab pribadi direksi karena kesalahan atau kelalaian dalam pengurusan.

1.1. Landasan Konseptual

Teori pertanggungjawaban hukum menjelaskan bahwa kewajiban untuk menanggung akibat hukum muncul ketika terdapat perbuatan atau kelalaian, pelanggaran terhadap kewajiban hukum, kerugian, dan hubungan kausal. Dalam hukum korporasi, ukuran perilaku direksi berkaitan erat dengan fiduciary duty dan duty of care. Fiduciary duty menuntut loyalitas, itikad baik, serta pengutamaan kepentingan perseroan, sedangkan duty of care menuntut tingkat kehati-hatian dan kecakapan yang wajar dalam pengambilan keputusan. Kewajiban tersebut relevan terhadap keamanan RME karena data pasien merupakan aset informasi sekaligus objek perlindungan hukum yang dapat menimbulkan risiko keuangan, operasional, reputasi, dan kepatuhan.

Di sisi lain, doktrin Business Judgment Rule memberi ruang perlindungan terhadap direksi agar tidak setiap keputusan bisnis yang berakhir merugikan otomatis menimbulkan tanggung jawab pribadi. Perlindungan ini mensyaratkan bahwa keputusan dibuat dengan itikad baik, tanpa benturan kepentingan, berdasarkan informasi yang memadai, dan dengan keyakinan rasional bahwa keputusan tersebut untuk kepentingan perseroan. Dalam kasus kebocoran RME, doktrin tersebut tidak dapat digunakan apabila direksi mengabaikan peringatan risiko, tidak menyediakan pengendalian yang proporsional, atau tidak menindaklanjuti temuan audit. Sebaliknya, insiden yang tetap terjadi setelah penerapan pengamanan yang layak tidak serta-merta membuktikan kelalaian direksi.

Good Corporate Governance (GCG) menjadi kerangka untuk menilai kualitas proses pengurusan. Prinsip transparansi, akuntabilitas, responsibilitas, independensi, dan kewajaran mengharuskan direksi membangun struktur pengambilan keputusan yang dapat ditelusuri dan dipertanggungjawabkan. Prinsip G20/OECD juga menekankan peran dewan dalam pengawasan risiko, kepatuhan, integritas sistem pelaporan, dan ketahanan perusahaan [15]. Pada rumah sakit digital, cakupan tersebut harus diterjemahkan ke dalam tata kelola data, pengelolaan vendor, klasifikasi informasi, pengaturan hak akses, audit berkala, mekanisme pelaporan insiden, serta perlindungan hak pasien.

1.2. Kesenjangan Penelitian dan Tujuan

Penelitian terdahulu lebih banyak membahas keamanan siber, implementasi RME, atau tanggung jawab fasilitas pelayanan kesehatan. Lestari dkk. menunjukkan bahwa perlindungan data pasien membutuhkan integrasi aspek hukum, teknologi, dan tata kelola [6]. Rahmatiqa dkk. menemukan dominasi faktor sumber daya manusia, kebijakan, fasilitas, dan

pendanaan dalam masalah keamanan serta kerahasiaan RME [7]. Faridoon dan Kechadi menempatkan tata kelola data kesehatan sebagai rangkaian kebijakan dan kontrol yang harus mencakup seluruh siklus data [10]. Kajian etik dan hukum di Indonesia juga menegaskan pentingnya kerahasiaan, legitimasi pemrosesan, serta kepatuhan terhadap regulasi RME [11], [12]. Namun, kedudukan direksi sebagai organ perseroan belum banyak ditempatkan sebagai pusat analisis.

Kebaruan penelitian ini terletak pada integrasi hukum korporasi dengan hukum kesehatan dan pelindungan data pribadi untuk merumuskan parameter pertanggungjawaban direksi rumah sakit. Penelitian bertujuan menganalisis pengaturan hukum yang relevan, menjelaskan kondisi yang dapat menimbulkan tanggung jawab pribadi direksi, menilai fungsi Business Judgment Rule, dan merumuskan penerapan GCG dalam pencegahan serta penanganan kebocoran RME. Analisis ini diharapkan memperluas kajian hukum korporasi pada sektor kesehatan digital dan memberi rekomendasi praktis bagi direksi, regulator, serta pembentuk kebijakan.

METODE

Penelitian ini merupakan penelitian hukum normatif yang memandang hukum sebagai norma, asas, doktrin, dan sistem pengaturan yang digunakan untuk menjawab isu hukum. Pendekatan ini dipilih karena fokus penelitian adalah konstruksi kewajiban dan pertanggungjawaban direksi, bukan pengukuran perilaku melalui data lapangan. Penelitian hukum normatif memungkinkan peneliti menelaah konsistensi, hubungan, dan kemungkinan konflik antara hukum perseroan, hukum kesehatan, serta hukum pelindungan data pribadi [16].

Pendekatan yang digunakan terdiri atas pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Pendekatan perundang-undangan dilakukan dengan menganalisis Undang-Undang Perseroan Terbatas [1], Undang-Undang Pelindungan Data Pribadi [2], Undang-Undang Kesehatan [3], dan Peraturan Menteri Kesehatan tentang Rekam Medis [4]. Pendekatan konseptual digunakan untuk menelaah fiduciary duty, duty of care, Business Judgment Rule, corporate risk, corporate compliance, dan Good Corporate Governance.

2.1. Bahan Hukum dan Teknik Pengumpulan

Bahan hukum primer terdiri atas peraturan perundang-undangan yang mengatur perseroan terbatas, kesehatan, pelindungan data pribadi, dan rekam medis. Bahan hukum sekunder meliputi buku penelitian hukum, artikel jurnal nasional dan internasional, serta hasil penelitian mengenai tata kelola data kesehatan, keamanan RME, akses informasi, dan akuntabilitas korporasi. Bahan hukum dikumpulkan melalui studi kepustakaan dengan tahap penelusuran, identifikasi, inventarisasi, klasifikasi, dan evaluasi relevansi.

Keandalan sumber dijaga dengan memprioritaskan regulasi resmi, publikasi ilmiah yang dapat ditelusuri, dan penelitian dalam lima tahun terakhir. Triangulasi kepustakaan dilakukan dengan membandingkan norma hukum, doktrin, serta temuan penelitian mengenai praktik keamanan RME. Proses ini diperlukan karena pertanggungjawaban direksi tidak dapat ditentukan hanya dari keberadaan insiden, tetapi harus dianalisis berdasarkan kewajiban yang berlaku, kualitas pengambilan keputusan, dan tindakan pengendalian yang telah dilakukan.

2.2. Teknik Analisis

Bahan hukum dianalisis secara kualitatif melalui penafsiran gramatikal, sistematis, dan teleologis. Penafsiran gramatikal digunakan untuk memahami rumusan kewajiban direksi, pengendali data, dan fasilitas pelayanan kesehatan. Penafsiran sistematis digunakan untuk menghubungkan norma dalam berbagai rezim hukum, sedangkan penafsiran teleologis digunakan untuk menilai tujuan perlindungan pasien, keberlanjutan rumah sakit, dan akuntabilitas organ perseroan.

Penarikan kesimpulan dilakukan secara deduktif, yaitu dari norma dan prinsip umum menuju jawaban terhadap isu khusus mengenai kebocoran RME. Analisis menilai empat unsur utama: kedudukan direksi, standar kewajiban kehati-hatian, hubungan kausal antara kegagalan tata kelola dan insiden, serta kemungkinan penerapan Business Judgment Rule. Hasilnya disusun dalam bentuk argumentasi preskriptif untuk merumuskan tindakan tata kelola yang seharusnya dilakukan rumah sakit.

HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa pertanggungjawaban direksi terhadap kebocoran RME tidak ditentukan semata-mata oleh terjadinya insiden. Titik tolaknya adalah apakah direksi telah menjalankan pengurusan perseroan dengan itikad baik, kehati-hatian, dan tanggung jawab sebagaimana diwajibkan oleh hukum perseroan [1]. Insiden merupakan indikator awal yang memerlukan pemeriksaan lebih lanjut terhadap kebijakan keamanan, sistem pengendalian, kualitas pengawasan, alokasi sumber daya, kepatuhan, dan respons setelah kejadian.

Kewajiban rumah sakit untuk menjaga kerahasiaan dan keamanan rekam medis memperoleh dasar dari hukum kesehatan dan aturan rekam medis [3], [4]. Pada saat yang sama, rumah sakit yang menentukan tujuan serta kendali pemrosesan data dapat berkedudukan sebagai pengendali data pribadi dengan kewajiban mencegah akses tidak sah, memastikan akurasi, menjaga keamanan, dan memenuhi hak subjek data [2]. Karena direksi mengarahkan strategi dan pengendalian perseroan, kewajiban korporasi tersebut harus diterjemahkan menjadi kebijakan dan tindakan manajerial yang konkret.

3.1. Kebocoran RME sebagai Risiko Korporasi

Kebocoran RME merupakan risiko korporasi karena dampaknya melintasi berbagai dimensi. Kerugian dapat berbentuk biaya pemulihan sistem, gangguan pelayanan, tuntutan pasien, sanksi administratif, paparan pidana, kerusakan reputasi, dan hilangnya kepercayaan. Studi tentang keamanan serta privasi RME menegaskan bahwa ancaman dapat berasal dari serangan eksternal, akses internal yang tidak sah, kesalahan konfigurasi, lemahnya autentikasi, penggunaan perangkat yang tidak aman, dan kegagalan pengelolaan vendor [8], [9]. Oleh karena itu, keamanan data tidak boleh didelegasikan sepenuhnya kepada unit teknologi informasi tanpa pengawasan strategis direksi.

Temuan penelitian di Indonesia memperlihatkan adanya kesenjangan antara kewajiban normatif dan kesiapan implementasi. Keterbatasan sumber daya, ketidakseragaman prosedur, serta budaya keamanan yang belum matang dapat memperbesar risiko [5], [7]. Penelitian Julia dan Aulianto menunjukkan bahwa pelaksanaan prinsip kerahasiaan, integritas, dan ketersediaan membutuhkan kebijakan hak akses, identitas

pengguna, infrastruktur yang stabil, dan prosedur yang konsisten [13]. Dengan demikian, direksi wajib memastikan bahwa kontrol keamanan tidak hanya tertulis, tetapi juga diuji, dipantau, dan diperbaiki secara berkelanjutan.

Dari sisi hukum, kebocoran RME dapat memunculkan beberapa lapis pertanggungjawaban. Pertama, rumah sakit sebagai badan hukum dapat menghadapi kewajiban pemulihan, ganti rugi, atau sanksi administratif karena kegagalan memenuhi kewajiban sebagai penyelenggara pelayanan kesehatan dan pengendali data. Kedua, direksi dapat dimintai pertanggungjawaban secara internal kepada perseroan apabila kerugian timbul karena kesalahan atau kelalaiannya dalam pengurusan. Ketiga, pertanggungjawaban pribadi terhadap pihak ketiga dapat muncul apabila perbuatan direksi memenuhi unsur pelanggaran yang secara langsung menimbulkan kerugian. Pembedaan ini penting agar tidak terjadi otomatisasi tanggung jawab pribadi hanya berdasarkan jabatan.

Tanggung jawab direksi juga memiliki dimensi preventif dan represif. Dimensi preventif mencakup penetapan kebijakan, anggaran, struktur kewenangan, standar vendor, audit, dan pelatihan. Dimensi represif dimulai ketika insiden terdeteksi, yaitu melalui penghentian akses yang tidak sah, pengamanan bukti, pemulihan layanan, penilaian dampak, pemberitahuan sesuai ketentuan, dan evaluasi akar masalah. Keterlambatan atau penyembunyian insiden dapat memperbesar kerugian serta menjadi indikator lemahnya itikad baik dan akuntabilitas.

Tabel 1. Hubungan Rezim Hukum dan Implikasi bagi Direksi

Rezim	Kewajiban Utama	Implikasi bagi Direksi
Hukum perseroan	Pengurusan dengan itikad baik, kehati-hatian, dan tanggung jawab.	Membangun pengawasan, menilai risiko, dan mendokumentasikan keputusan.
Hukum kesehatan	Menjamin mutu pelayanan dan kerahasiaan informasi kesehatan.	Memastikan kebijakan RME mendukung keselamatan pasien dan kesinambungan layanan.
Pelindungan data pribadi	Pemrosesan yang sah, aman, transparan, dan akuntabel.	Menetapkan struktur kepatuhan, respons insiden, dan pemenuhan hak subjek data.
Peraturan rekam medis	Penyelenggaraan RME serta penjagaan kerahasiaan, integritas, dan ketersediaan.	Menyediakan sumber daya, kontrol akses, audit, pencadangan, dan pemulihan.

3.2. Fiduciary Duty dan Duty of Care

Fiduciary duty mengharuskan direksi menempatkan kepentingan perseroan dan keberlanjutan pelayanan di atas kepentingan pribadi. Dalam isu RME, kewajiban tersebut mencakup pencegahan konflik kepentingan dalam pemilihan vendor, penggunaan anggaran secara bertanggung jawab, dan keterbukaan terhadap risiko material. Duty of care mengharuskan direksi memperoleh informasi yang relevan, meminta penilaian ahli apabila diperlukan, membaca laporan audit, dan memastikan adanya tindak lanjut. Kegagalan memahami seluruh aspek teknis tidak otomatis merupakan kelalaian, tetapi mengabaikan

kebutuhan keahlian dan tidak membangun mekanisme pengawasan dapat menjadi pelanggaran kehati-hatian.

Parameter duty of care dapat diwujudkan melalui beberapa bukti tata kelola: kebijakan keamanan yang disetujui direksi, peta risiko digital, penetapan penanggung jawab, audit berkala, pelatihan, pengujian pemulihan, manajemen insiden, dan dokumentasi keputusan. Kerangka tata kelola data menekankan bahwa keamanan perlu diterapkan sejak pengumpulan, penyimpanan, penggunaan, pertukaran, pengarsipan, hingga pemusnahan data [10]. Di tingkat teknis, pengendalian akses berbasis peran, autentikasi berlapis, pencatatan aktivitas, dan evaluasi hak akses merupakan kontrol penting yang didukung oleh tinjauan sistematis terbaru [14].

Delegasi kewenangan kepada direktur bidang, kepala teknologi informasi, petugas pelindungan data, atau vendor tidak menghapus tanggung jawab pengawasan direksi. Delegasi dapat diterima apabila dilakukan kepada pihak yang kompeten, disertai mandat yang jelas, indikator kinerja, saluran pelaporan, dan mekanisme eskalasi. Direksi tetap wajib meminta informasi yang memadai dan bertindak ketika laporan menunjukkan risiko material. Karena itu, pembelaan bahwa masalah sepenuhnya berada pada unit teknis tidak cukup apabila struktur pelaporan dan pengawasan memang tidak pernah dibangun.

Standar kehati-hatian bersifat proporsional terhadap skala, kompleksitas, jenis layanan, volume data, serta profil ancaman rumah sakit. Rumah sakit besar dengan integrasi sistem yang luas diharapkan memiliki kontrol lebih matang dibanding fasilitas kecil. Namun, proporsionalitas tidak boleh dipakai untuk meniadakan kontrol dasar seperti identitas pengguna unik, pembatasan hak akses, pencadangan, pencatatan aktivitas, pembaruan keamanan, dan prosedur respons insiden. Direksi harus dapat menjelaskan mengapa pilihan kontrol tertentu dianggap memadai berdasarkan penilaian risiko yang terdokumentasi.

Tabel 2. Indikator Duty of Care dan Bukti Tata Kelola

Indikator	Bukti yang Dapat Ditelusuri
Penilaian risiko	Peta risiko, klasifikasi data, penilaian dampak, dan prioritas mitigasi.
Pengambilan keputusan	Notulen rapat, rekomendasi ahli, alternatif yang dipertimbangkan, dan alasan keputusan.
Pengendalian akses	Daftar kewenangan, autentikasi, audit log, evaluasi berkala, dan pencabutan akses.
Ketahanan layanan	Pencadangan, pengujian pemulihan, rencana kelangsungan, dan simulasi insiden.
Pengawasan vendor	Uji kelayakan, klausul keamanan, hak audit, pelaporan insiden, dan rencana terminasi.
Perbaikan berkelanjutan	Temuan audit, rencana aksi, penanggung jawab, tenggat, dan verifikasi penyelesaian.

3.3. Business Judgment Rule dan Batas Tanggung Jawab Pribadi

Business Judgment Rule berfungsi menjaga keseimbangan antara akuntabilitas dan ruang diskresi direksi. Direksi tidak seharusnya dimintai tanggung jawab pribadi hanya karena teknologi yang dipilih kemudian mengalami serangan, sepanjang keputusan dibuat melalui proses yang layak. Analisis harus membedakan risiko yang secara wajar tidak dapat dihilangkan dari risiko yang dibiarkan karena kelalaian. Faktor yang relevan meliputi kualitas informasi saat keputusan dibuat, keterlibatan ahli, rasionalitas anggaran, kepatuhan terhadap standar, dokumentasi, dan tindakan korektif.

Perlindungan Business Judgment Rule menjadi lemah apabila direksi mengetahui adanya kerentanan serius tetapi menunda perbaikan tanpa alasan yang dapat dipertanggungjawabkan; tidak merespons insiden sebelumnya; menggunakan sistem tanpa kontrol minimum; mengabaikan kewajiban hukum; atau memiliki benturan kepentingan. Dalam keadaan demikian, kerugian akibat kebocoran dapat dihubungkan dengan kesalahan atau kelalaian dalam pengurusan. Sebaliknya, apabila sistem pengendalian telah proporsional, audit dilakukan, rekomendasi ditindaklanjuti, dan insiden direspons cepat, tanggung jawab utama dapat tetap berada pada perseroan tanpa otomatis beralih menjadi tanggung jawab pribadi direksi.

Analisis kausalitas harus membedakan penyebab langsung insiden dari penyebab tata kelola. Serangan siber mungkin menjadi pemicu langsung, tetapi kerugian yang luas dapat dipengaruhi oleh tidak adanya segmentasi jaringan, pencadangan yang tidak dapat dipulihkan, atau hak akses yang berlebihan. Sebaliknya, serangan yang sangat canggih dapat tetap menembus sistem yang telah dikelola secara wajar. Oleh sebab itu, ukuran tanggung jawab bukan kesempurnaan hasil, melainkan kewajaran proses pengambilan keputusan dan kualitas pengendalian sebelum, selama, dan setelah insiden.

Dokumen rapat direksi, laporan risiko, hasil audit, rekomendasi ahli, keputusan anggaran, catatan tindak lanjut, dan evaluasi pascainsiden menjadi bukti penting. Ketiadaan dokumentasi tidak selalu membuktikan kelalaian, tetapi menyulitkan direksi menunjukkan bahwa keputusan telah dibuat berdasarkan informasi memadai. Sebaliknya, dokumentasi yang hanya bersifat formal tanpa implementasi nyata tidak cukup. Penilaian harus memeriksa kesesuaian antara kebijakan tertulis, praktik operasional, dan respons faktual.

3.4. Good Corporate Governance dalam Pelindungan Data Pasien

Prinsip transparansi mensyaratkan informasi yang jujur kepada pasien dan pemangku kepentingan mengenai pemrosesan data, risiko, serta insiden sesuai batas hukum. Akuntabilitas menuntut kejelasan peran antara direksi, manajemen rumah sakit, komite risiko, petugas pelindungan data, unit teknologi informasi, dan vendor. Responsibilitas berarti kepatuhan terhadap hukum kesehatan, RME, dan pelindungan data. Independensi menuntut keputusan pengamanan bebas dari konflik kepentingan, sedangkan kewajaran mengharuskan perlakuan yang adil terhadap pasien sebagai pemilik kepentingan atas data.

Penerapan GCG pada keamanan RME sejalan dengan prinsip tata kelola korporasi internasional yang menempatkan pengawasan risiko dan sistem kepatuhan sebagai fungsi penting organ pengurus [15]. Dalam konteks nasional, kajian Lestari dkk. menegaskan perlunya integrasi aspek hukum, keamanan, dan kemudahan penggunaan [6]. Larasati dkk.

menekankan konsekuensi etik dan yuridis pengelolaan RME [11], sedangkan Prayuti menunjukkan bahwa pelaksanaan hukum pelindungan data kesehatan memerlukan penanganan yang aman dan rahasia, bukan sekadar pemenuhan dokumen administratif [12].

Model tata kelola yang disarankan mencakup persetujuan kebijakan oleh direksi, pengelompokan data berdasarkan sensitivitas, pembatasan akses berdasarkan fungsi, evaluasi vendor, enkripsi, pencadangan, pengujian pemulihan, audit log, simulasi insiden, pelatihan berulang, dan pelaporan berkala kepada direksi. Setiap keputusan penting perlu didokumentasikan agar dapat menunjukkan proses pengambilan keputusan yang hati-hati. Dokumentasi tersebut tidak hanya mendukung audit dan kepatuhan, tetapi juga menjadi bukti relevan dalam menilai penerapan Business Judgment Rule.

Pengelolaan pihak ketiga perlu memperoleh perhatian khusus karena rumah sakit sering menggunakan penyedia sistem informasi, pusat data, layanan awan, pemeliharaan perangkat, dan integrasi aplikasi. Kontrak harus memuat standar keamanan, pembatasan penggunaan data, kewajiban kerahasiaan, lokasi dan retensi data, hak audit, waktu pelaporan insiden, pemulihan, serta tanggung jawab setelah hubungan berakhir. Direksi perlu memastikan bahwa penilaian vendor tidak hanya mempertimbangkan harga dan fungsi, tetapi juga kemampuan keamanan dan kepatuhan.

Budaya keamanan merupakan bagian dari GCG karena banyak insiden berawal dari kesalahan manusia. Pelatihan tidak cukup dilakukan sekali pada saat orientasi; materi harus disesuaikan dengan peran, diperbarui berdasarkan pola ancaman, dan diuji melalui simulasi. Mekanisme pelaporan internal harus memungkinkan pegawai menyampaikan kelemahan atau insiden tanpa rasa takut. Direksi juga perlu memastikan bahwa indikator keamanan masuk ke dalam evaluasi kinerja manajemen, bukan hanya menjadi tanggung jawab teknis yang tidak terlihat dalam agenda korporasi.

3.5. Harmonisasi Regulasi dan Implikasi

Pengaturan yang berlaku telah menyediakan dasar kewajiban, tetapi masih tersebar dalam rezim hukum perseroan, kesehatan, rekam medis, dan pelindungan data. Hukum perseroan mengatur tanggung jawab direksi secara umum, sedangkan hukum kesehatan dan pelindungan data lebih banyak membebankan kewajiban pada fasilitas pelayanan kesehatan atau pengendali data. Irisan tersebut menimbulkan kebutuhan penafsiran sistematis untuk menentukan kapan kegagalan korporasi berubah menjadi kelalaian pribadi direksi.

Harmonisasi dapat dilakukan melalui pedoman sektoral yang menjelaskan kewajiban minimum direksi rumah sakit dalam tata kelola data, indikator kehati-hatian, mekanisme pelaporan insiden, pembagian tanggung jawab dengan vendor, dan dokumentasi pengambilan keputusan. Pedoman tersebut perlu bersifat berbasis risiko agar rumah sakit dengan skala dan kompleksitas berbeda dapat menerapkan kontrol yang proporsional. Penguatan regulasi juga perlu disertai supervisi, peningkatan kompetensi, dan standar audit yang dapat digunakan secara konsisten.

Pedoman sektoral juga perlu menjelaskan hubungan antara tanggung jawab rumah sakit sebagai badan hukum dan tanggung jawab organ perseroan. Kejelasan ini penting agar sanksi diarahkan kepada pihak yang benar-benar memiliki kewenangan dan melakukan pelanggaran. Pendekatan yang terlalu luas berisiko menimbulkan ketakutan berlebihan dalam pengambilan keputusan, sedangkan pendekatan yang terlalu sempit dapat mendorong direksi

berlindung di balik badan hukum. Keseimbangan dapat dicapai melalui pengujian kewenangan, pengetahuan, tindakan, dan kontribusi kausal setiap pihak.

Secara teoretis, hasil penelitian memperluas penggunaan konsep fiduciary duty dan duty of care ke dalam pengelolaan aset digital serta hak privasi pasien. Secara praktis, direksi perlu menempatkan keamanan informasi sebagai agenda strategis, bukan biaya teknis tambahan. Penelitian ini terbatas pada analisis normatif dan belum menguji praktik tata kelola pada rumah sakit tertentu. Penelitian lanjutan dapat menggunakan pendekatan socio-legal untuk menilai penerapan kebijakan, kualitas pengawasan direksi, dan efektivitas respons insiden pada rumah sakit pemerintah maupun swasta.

KESIMPULAN

Pertanggungjawaban direksi rumah sakit terhadap kebocoran RME lahir dari kedudukannya sebagai organ perseroan yang wajib menjalankan pengurusan dengan itikad baik, kehati-hatian, dan tanggung jawab. Pelindungan data pasien merupakan bagian dari kewajiban strategis direksi karena mencakup pengendalian internal, manajemen risiko, kepatuhan, pengawasan vendor, audit, dan respons insiden. Kebocoran data tidak otomatis menimbulkan tanggung jawab pribadi; penilaiannya bergantung pada ada tidaknya kesalahan atau kelalaian, kualitas proses pengambilan keputusan, dan hubungan kausal dengan kerugian. Business Judgment Rule dapat melindungi direksi yang bertindak berdasarkan informasi memadai, tanpa benturan kepentingan, dan dengan keyakinan rasional untuk kepentingan perseroan.

Penerapan Good Corporate Governance memperkuat pencegahan melalui transparansi, akuntabilitas, responsibilitas, independensi, dan kewajaran. Rumah sakit perlu menjadikan keamanan RME sebagai program tata kelola yang terdokumentasi dan berkelanjutan. Harmonisasi antara hukum perseroan, kesehatan, rekam medis, dan pelindungan data diperlukan agar batas kewajiban direksi lebih pasti, pasien memperoleh perlindungan efektif, dan rumah sakit memiliki pedoman kepatuhan yang proporsional terhadap risiko digital.

REFERENSI

[1] Republik Indonesia, “Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas,” Lembaran Negara Republik Indonesia Tahun 2007 Nomor 106, 2007. https://peraturan.bpk.go.id/

[2] Republik Indonesia, “Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi,” Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, 2022. https://peraturan.bpk.go.id/

[3] Republik Indonesia, “Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan,” Lembaran Negara Republik Indonesia Tahun 2023 Nomor 105, 2023. https://peraturan.bpk.go.id/

[4] Kementerian Kesehatan Republik Indonesia, “Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis,” Berita Negara Republik Indonesia Tahun 2022 Nomor 829, 2022. https://peraturan.bpk.go.id/

[5] A. A. Izza and S. Lailiyah, “Literature Review: Overview of the Implementation of Electronic Medical Records in Indonesian Hospitals Based on Minister of Health Regulation Number 24 of 2022 concerning Medical Records,” Media Gizi Kesmas, vol. 13, no. 1, pp. 549–562, 2024. https://doi.org/10.20473/mgk.v13i1.2024.549-562
[6] A. Y. Lestari, M. Misran, T. Raharjo, M. Annas, D. Riskanita, and A. P. Prabandari, “Improving Healthcare Patient Data Security: An Integrated Framework Model for Electronic Health Records from a Legal Perspective,” Law Reform, vol. 20, no. 2, pp. 329–352, 2024. https://doi.org/10.14710/lr.v20i2.56986
[7] C. Rahmatiqa, W. Werman, M. Arrazy, and N. Abdillah, “Security and Confidentiality of Medical Record Data in Hospitals in the Use of Electronic Medical Records: Literature Review,” Journal of Medical Record and Information Technology, vol. 1, no. 1, pp. 11–18, 2023. https://jurnal.syedzasaintika.ac.id/index.php/jomrit/article/view/2220
[8] I. Keshta and A. Odeh, “Security and Privacy of Electronic Health Records: Concerns and Challenges,” Egyptian Informatics Journal, vol. 22, no. 2, pp. 177–183, 2021. https://doi.org/10.1016/j.eij.2020.07.003
[9] J. Alipour, Y. Mehdipour, A. Karimi, M. Khorashadizadeh, and M. Akbarpour, “Security, Confidentiality, Privacy and Patient Safety in the Hospital Information Systems from the Users’ Perspective: A Cross-Sectional Study,” International Journal of Medical Informatics, vol. 175, Art. no. 105066, 2023. https://doi.org/10.1016/j.ijmedinf.2023.105066
[10] A. Faridoon and M. T. Kechadi, “Healthcare Data Governance, Privacy, and Security: A Conceptual Framework,” in Body Area Networks. Smart IoT and Big Data for Intelligent Health Management, pp. 261–271, 2024. https://doi.org/10.1007/978-3-031-72524-1_19
[11] T. Larasati, A. I. Fardiansyah, D. Saketi, and A. N. Dewiarti, “The Ethical and Legal Aspects of Health Policy on Electronic Medical Records in Indonesia,” Cepalo, vol. 8, no. 2, pp. 103–112, 2024. https://doi.org/10.25041/cepalo.v8no2.3634
[12] Y. Prayuti, “Implications of Personal Data Protection Law in Consumer Health Data Management to Improve Secure and Confidential Handling in Indonesia,” Jurnal Ius Constituendum, vol. 9, no. 3, pp. 461–478, 2024. https://doi.org/10.26623/jic.v9i3.9289
[13] F. Julia and D. R. Aulianto, “Focused Analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data Security Implementation of Electronic Medical Records at Sindangwangi Health Center, Pangandaran, West Java,” Lentera Pustaka, vol. 11, no. 1, pp. 61–74, 2025. https://doi.org/10.14710/lenpust.v11i1.70518
[14] U. N. C. Cobrado, S. Sharief, N. G. Regahal, E. Zepka, M. B. Mamauag, and L. C. Velasco, “Access Control Solutions in Electronic Health Record Systems: A Systematic Review,” Informatics in Medicine Unlocked, vol. 49, Art. no. 101552, 2024. https://doi.org/10.1016/j.imu.2024.101552
[15] OECD, G20/OECD Principles of Corporate Governance 2023. Paris, France: OECD Publishing, 2023. https://doi.org/10.1787/ed750b30-en
[16] P. M. Marzuki, Penelitian Hukum, ed. revisi. Jakarta, Indonesia: Kencana, 2021.