Jurnal Hukum Siber
dan Regulasi Teknologi

SAH PUBLISHER

e-ISSN 3123-8114
Vol. 1, No. 3, September 2026

Keamanan Siber *Internet of Medical Things* sebagai Elemen Ketahanan Kesehatan Nasional

Boydo Saragih
Fakultas Hukum Universitas Sam Ratulangi, Indonesia

Email: boydosaragih071@student.unsrat.ac.id

Abstrak. Penelitian ini bertujuan menganalisis urgensi keamanan siber *Internet of Medical Things* (IoMT) sebagai infrastruktur kritis ketahanan kesehatan nasional dan membandingkan kerangka regulasi Indonesia dengan Amerika Serikat. Melalui metode penelitian hukum yuridis normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan komparatif (*comparative approach*), penelitian ini menemukan bahwa instrumen hukum Indonesia (UU Pelindungan Data Pribadi dan Perpres Infrastruktur Informasi Vital) masih bersifat reaktif dan *data-centric*, menyisakan kekosongan hukum terkait kewajiban sertifikasi pra-pasar (*pre-market*) dan pengawasan pasca-pasar (*post-market*) bagi perangkat IoMT. Sebaliknya, Amerika Serikat melalui *Food and Drug Administration* (FDA) menerapkan pendekatan *device-centric* yang mewajibkan produsen mengadopsi *Secure Product Development Framework* (SPDF) sebagai prasyarat mutlak penerbitan izin edar. Kekosongan standar teknis yang mengikat di Indonesia menciptakan kerentanan asimetris yang mengancam stabilitas demografi dan kedaulatan negara. Penelitian ini merekomendasikan perlunya transformasi paradigma hukum melalui revisi Rancangan Undang-Undang Keamanan dan Ketahanan Siber untuk mengakomodasi standardisasi *security by design* serta pembentukan Unit Verifikasi Keamanan Siber Medis secara lintas sektoral.

Kata Kunci: *Internet of Medical Things*, Keamanan Siber, Ketahanan Nasional

PENDAHULUAN

Sebagai negara kepulauan terbesar di dunia dengan 17.504 pulau dan garis pantai sepanjang 108.000 km, konsepsi ketahanan nasional Indonesia senantiasa dibangun di atas fondasi geostrategis yang memadukan aspek kesejahteraan dan keamanan secara simultan.[1] Dinamika lingkungan strategis abad ke-21, terutama pesatnya transformasi digital di sektor publik, telah

Received Jun 2026 / Revised Jul 2026 / Accepted Jul 2026
*Corresponding author.
Email addresses: boydosaragih071@student.unsrat.ac.id (saragih)

menggeser sumber ancaman dari invasi militer konvensional menuju eksploitasi infrastruktur kritis berbasis teknologi informasi.[2]

Di sektor kesehatan, pergeseran ini termanifestasi melalui adopsi massal *Internet of Medical Things* (IoMT) seperti perangkat pacu jantung nirkabel, pompa insulin otomatis, dan *smartwatch* kesehatan canggih yang terus-menerus mengirimkan data fisiologis pengguna secara *real-time*.[3] Transformasi digital di sektor kesehatan Indonesia, yang ditandai dengan integrasi ratusan aplikasi ke dalam platform nasional SATUSEHAT serta penerapan Sistem Informasi Manajemen Rumah Sakit (SIMRS), diproyeksikan guna meningkatkan efisiensi layanan sekaligus membuka kemungkinan terhadap serangan (*attack surface*) yang sebelumnya tidak pernah terbayangkan.[4]

Urgensi pengarusutamaan keamanan IoMT ke dalam agenda ketahanan kesehatan nasional lahir dari maraknya kasus siber di bidang kesehatan. Lebih dari 133 juta anomali lalu lintas siber terjadi pada semester pertama tahun 2025 dengan sektor kesehatan menjadi sasaran prioritas serangan *ransomware* dan *malware*.[5] Berdasarkan siaran pers Badan Siber dan Sandi Negara (BSSN), jumlah serangan siber di Indonesia sepanjang 2025 mencapai 5,5 miliar serangan, melonjak tujuh kali lipat atau naik 714 persen dibandingkan rata-rata tahunan selama periode 2020-2024, dan tren peningkatan ini berlanjut pada awal 2026 dengan tercatat 1,52 miliar serangan selama 1 Januari hingga 15 April 2026.[6]

Berdasarkan laporan AwanPintar.id, sektor kesehatan menjadi sektor yang paling banyak menerima serangan siber pada periode Q1 2024 hingga Q2 2025, dengan total 10,6 juta serangan. Serangan terbanyak terjadi pada Q1 2024 (2,3 juta), sedangkan pada Q1 dan Q2 2025 masing-masing tercatat 1,3 juta serangan. Jenis serangan yang paling banyak menimpa sektor kesehatan adalah web application attacks (13.857 insiden), malware (3.615 insiden), dan ransomware (1.779 insiden). Rumah Sakit Umum Daerah (RSUD) menjadi target paling sering, dengan kasus RSUD Majalengka yang mengalami serangan ransomware selama 4 hari yang melumpuhkan sistem pendaftaran dan rekam medis elektronik.[7]

Serangan terhadap alat pacu jantung nirkabel tidak lagi sekadar mencuri data, melainkan dapat diprogram untuk mengirimkan kejutan listrik mematikan atau menghentikan fungsi jantung secara tiba-tiba.[8] Dalam perspektif geostrategi, ketidakmampuan suatu negara menjamin keamanan siber atas infrastruktur kesehatan digitalnya merupakan kerentanan strategis yang dapat dieksploitasi oleh aktor negara maupun non-negara untuk mencapai tujuan non-militer di luar medan perang konvensional.[9]

Jika dilihat dari tatanan hukum positif, Indonesia sesungguhnya tidak berada dalam kondisi *legal vacuum*. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) mengategorikan data kesehatan sebagai data pribadi bersifat spesifik dan mewajibkan pengendali data untuk menerapkan langkah-langkah keamanan teknis operasional.[10] Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Perpres IIV) secara tegas memasukkan sektor kesehatan sebagai bagian dari Infrastruktur Informasi Vital yang harus dilindungi, dengan BSSN sebagai koordinator.[11] Namun demikian, kedua instrumen hukum ini memiliki cacat struktural yang sama dimana keduanya bersifat umum dan tidak secara spesifik mengatur keamanan siber perangkat IoMT sepanjang siklus hidupnya, mulai dari keharusan *security by design* dalam uji pra-pasar (*pre-market*), standardisasi protokol komunikasi, hingga kewajiban pemantauan kerentanan pasca-pasar (*post-market*).

Ketiadaan standar teknis yang mengikat ini nyata terlihat ketika Kementerian Kesehatan meluncurkan *Regulatory Sandbox* 2025 untuk menguji inovasi kecerdasan buatan, tetapi nyaris tidak menyentuh aspek keamanan siber IoMT.[12] Sementara itu, Rancangan Undang-Undang Keamanan dan Ketahanan Siber yang hingga kini masih bergulir di pembahasan dan sangat didesak pengesahannya oleh BSSN belum secara eksplisit mengatur IoMT sebagai objek perlindungan khusus.[13]

Penelusuran terhadap penelitian terdahulu menunjukkan bahwa kajian tentang keamanan IoMT selama ini didominasi oleh pendekatan teknis. Sebuah *systematic literature review* terhadap 72 studi internasional (2015–2025) menemukan enam kategori utama pengamanan IoMT: kriptografi, otentikasi, kecerdasan buatan, pelestarian privasi, desain arsitektur, serta analisis dan evaluasi keamanan.[8] Studi-studi ini, meskipun penting, tidak pernah mengaitkan temuannya dengan kerangka ketahanan nasional atau geostrategi.

Di Indonesia, beberapa studi telah mengkaji penerapan prinsip perlindungan data pribadi pada aplikasi telemedicine dan menemukan bahwa belum semua aplikasi secara efektif mengadopsi prinsip-prinsip tersebut.[14]

Amerika Serikat yang dipilih sebagai negara pembanding dalam penelitian ini telah memiliki kerangka regulasi yang paling maju dan terperinci. *Final Guidance* yang direvisi terakhir kali pada bulan Februari 2026 mewajibkan produsen perangkat medis untuk menyertakan rencana keamanan siber tertulis dalam setiap pengajuan *pre-market*, serta untuk melakukan pemantauan dan penanganan kerentanan sepanjang siklus hidup perangkat.[15] Section 524B dari *Federal Food, Drug, and Cosmetic Act* bahkan memberikan

kewenangan kepada FDA untuk menolak perangkat medis yang tidak memenuhi persyaratan keamanan siber tertentu.[16] Dengan demikian, perbandingan antara sistem hukum sipil (Indonesia) dan *common law* (Amerika Serikat) diharapkan dapat memperkaya diskursus akademik dan menawarkan rekomendasi kebijakan yang konkret bagi penyusunan standar teknis IoMT di Indonesia dan penguatan RUU Keamanan Siber.

Bertolak dari identifikasi masalah di atas, penelitian ini bertujuan menjawab dua rumusan masalah utama. Pertama, bagaimana konstruksi hukum perlindungan *Internet of Medical Things* sebagai bagian integral dari infrastruktur kritis dalam arsitektur ketahanan kesehatan nasional di Indonesia saat ini? Kedua, bagaimana disparitas kerangka regulasi dan standardisasi keamanan siber perangkat medis antara instrumen hukum Indonesia dan Amerika Serikat?

METODE

Penelitian ini merupakan penelitian hukum yuridis normatif yang menggunakan pendekatan perundang-undangan (*statute approach*) dan pendekatan komparatif (*comparative approach*). Bahan hukum primer dan sekunder dikumpulkan melalui studi kepustakaan, dengan batasan dokumen regulasi serta literatur yang diterbitkan dalam rentang tahun 2015 hingga 2026. Batasan periode ini ditetapkan untuk memastikan analisis tetap relevan dengan dinamika terkini adopsi teknologi IoMT dan perkembangan regulasi keamanan siber.

Pendekatan komparatif menjadikan Amerika Serikat sebagai negara pembanding karena yurisdiksi tersebut telah memiliki kerangka regulasi keamanan siber perangkat medis yang paling terperinci. Analisis difokuskan pada dua instrumen hukum utama, yaitu *Final Guidance* FDA (Juni 2025) dan *Section 524B Federal Food, Drug, and Cosmetic Act*. Perbandingan antara kerangka hukum Indonesia dan Amerika Serikat ini menyoroti beberapa aspek utama, meliputi: orientasi regulasi, mekanisme pengawasan pra-pasar dan pasca-pasar, kewajiban produsen, standar teknis, serta sanksi dan kewenangan lembaga.

Tahapan analisis bahan hukum dalam penelitian ini dilakukan melalui tiga langkah berurutan. Pertama, menginventarisasi dan mengevaluasi celah perlindungan perangkat IoMT pada instrumen hukum Indonesia, khususnya Undang-Undang Nomor 27 Tahun 2022 dan Peraturan Presiden Nomor 82 Tahun 2022. Kedua, melakukan komparasi pasal dan standar teknis antara kelemahan regulasi Indonesia dengan kerangka proaktif FDA Amerika Serikat.

Ketiga, menganalisis temuan tersebut menggunakan interpretasi sistematis dan teleologis untuk merumuskan preskripsi kebijakan yang konkret bagi penguatan Rancangan Undang-Undang Keamanan Siber di Indonesia .

HASIL DAN PEMBAHASAN

Konstruksi Hukum Perlindungan *Internet of Medical Things* (IoMT)

Konstruksi hukum perlindungan *Internet of Medical Things* (IoMT) sebagai bagian integral dari infrastruktur kritis dalam arsitektur ketahanan kesehatan nasional Indonesia harus dibaca dari tiga lapis instrumen hukum yang berlaku: (1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), (2) Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Perpres IIV), dan (3) peraturan teknis di bawah Kementerian Kesehatan serta Badan Siber dan Sandi Negara (BSSN). Ketiga lapis ini membentuk sebuah kerangka yang secara formal mengakui bahwa data kesehatan dan sistem elektronik di sektor kesehatan merupakan objek yang dilindungi, namun analisis interpretasi sistematis menunjukkan bahwa kerangka tersebut masih menyisakan ketidakjelasan yang fundamental ketika dihadapkan pada karakteristik spesifik IoMT sebagai perangkat medis yang terhubung secara permanen ke jaringan dan dapat memengaruhi keselamatan fisik pasien secara langsung.

UU PDP mengategorikan data dan informasi kesehatan sebagai data pribadi yang bersifat spesifik, sehingga memerlukan perlindungan yang lebih ketat dibandingkan data pribadi umum.[11] Pasal 35 UU PDP mewajibkan setiap Pengendali Data Pribadi untuk menyusun dan menerapkan langkah-langkah teknis operasional guna melindungi data dari gangguan pemrosesan yang bertentangan dengan ketentuan peraturan perundang-undangan, serta menentukan tingkat keamanan data dengan memperhatikan sifat dan risiko data yang diproses.[11]

Namun, ketentuan ini tidak pernah menyebut secara eksplisit perangkat medis yang terhubung (*connected medical devices*) sebagai objek perlindungan. UU PDP memandang IoMT hanya sebagai sumber data, bukan sebagai sistem yang jika diganggu dapat mengakibatkan cedera fisik atau kematian.[17]

Perpres Nomor 82 Tahun 2022 mengambil langkah lebih maju dengan secara tegas mencantumkan sektor kesehatan sebagai salah satu sektor Infrastruktur Informasi Vital (IIV) yang jika mengalami gangguan, kerusakan, atau kehancuran dapat berdampak serius terhadap kepentingan umum,

pelayanan publik, pertahanan dan keamanan, atau perekonomian nasional.[18] Pasal 4 ayat (1) huruf e Perpres ini menunjuk kementerian yang menyelenggarakan urusan pemerintahan di bidang kesehatan sebagai Kementerian atau Lembaga yang bertanggung jawab atas sektor kesehatan. Selanjutnya, Pasal 9 ayat (2) mewajibkan Penyelenggara IIV yang dalam konteks ini mencakup rumah sakit, klinik, dan fasilitas pelayanan kesehatan lainnya untuk menerapkan standar keamanan informasi dan/atau standar keamanan lain yang ditetapkan oleh Kementerian atau Lembaga dan/atau BSSN.[18] Pada tataran ini, Perpres IIV telah mengakui bahwa sistem elektronik di sektor kesehatan tidak hanya membawa data sensitif tetapi juga merupakan infrastruktur yang kelangsungannya harus dijamin negara.

Akan tetapi, ketika ditelusuri lebih jauh, Perpres IIV tidak pernah menyebut istilah IoMT, *medical device*, atau *wearable health device*. Pengaturan dalam Perpres IIV masih berada pada tingkat sektor dan sistem elektronik secara umum, bukan pada tingkat perangkat individual yang terhubung.

Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis (Permenkes RM) mewajibkan setiap fasilitas pelayanan kesehatan untuk menyelenggarakan Rekam Medis Elektronik (RME) paling lambat 31 Desember 2023, dan RME tersebut harus memenuhi prinsip keamanan data dan informasi yang meliputi kerahasiaan, integritas, dan ketersediaan.[19] Pasal 29 Permenkes RM menyatakan bahwa kerahasiaan merupakan jaminan keamanan data dari gangguan pihak internal maupun eksternal yang tidak memiliki hak akses, integritas adalah jaminan keakuratan data, dan ketersediaan adalah jaminan data dapat diakses oleh pihak yang memiliki hak akses.

Namun demikian, regulasi ini tetap berfokus pada data rekam medis, bukan pada keamanan perangkat IoMT itu sendiri. Tidak ada satu pun pasal dalam Permenkes RM yang mengatur tentang kewajiban rumah sakit untuk memastikan bahwa alat pacu jantung nirkabel yang digunakan pasiennya memiliki mekanisme autentikasi yang memadai atau bahwa perangkat tersebut dapat menerima pembaruan keamanan dari produsen. Dengan kata lain, tanggung jawab fasilitas kesehatan dibatasi pada pengelolaan data di dalam sistem informasinya sendiri, sementara keamanan perangkat medis yang sudah terpasang pada pasien berada di luar jangkauan regulasi tersebut.

Di sisi lain, BSSN telah mengeluarkan Peraturan BSSN Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber, yang mewajibkan Penyelenggara IIV untuk melakukan pengukuran mandiri terhadap empat domain: identifikasi, proteksi, deteksi, serta penanggulangan dan pemulihan.[20] Dalam domain proteksi, terdapat kewajiban untuk melindungi

data dan melindungi jaringan. Namun, instrumen penilaian yang digunakan oleh BSSN tidak secara spesifik menguji apakah suatu fasilitas kesehatan memiliki kebijakan khusus untuk mengamankan IoMT yang terhubung ke jaringannya. Kemudian, Peraturan BSSN Nomor 9 Tahun 2021 tentang Perubahan atas Peraturan BSSN Nomor 8 Tahun 2021 tentang Penyelenggaraan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001 Menggunakan Indeks Keamanan Informasi hanya mewajibkan Penyelenggara Sistem Elektronik untuk menilai kesiapan mereka dalam menerapkan standar manajemen keamanan informasi internasional.[21] Standar ISO/IEC 27001 bersifat umum dan tidak dirancang khusus untuk mengatasi keunikan IoMT, seperti keterbatasan sumber daya komputasi pada perangkat medis yang dapat ditanamkan atau protokol komunikasi nirkabel yang rentan terhadap *replay attack* dan *spoofing*.

Dari penelusuran ini, dapat dikemukakan bahwa konstruksi hukum perlindungan IoMT di Indonesia saat ini bersifat *fragmentaris* dan berlapis namun tidak terintegrasi. Ada pengakuan bahwa sektor kesehatan adalah infrastruktur kritis (Perpres IIV), ada pengakuan bahwa data kesehatan adalah data sensitif (UU PDP), dan ada kewajiban bagi fasilitas kesehatan untuk menerapkan manajemen keamanan informasi (Perka BSSN serta Permenkes RM). Namun, kerangka tersebut belum cukup untuk menjawab tantangan spesifik yang ditimbulkan oleh perkembangan IoMT.

Kelemahan konstruksi ini menjadi semakin nyata ketika dikaitkan dengan bukti empiris serangan siber terhadap infrastruktur kesehatan di Indonesia dan di dunia. Penelitian simulasi terhadap rumah sakit menengah di Indonesia menunjukkan probabilitas insiden *ransomware* tahunan mencapai 0,38 (38%), dengan rata-rata *downtime* sistem elektronik antara 48 hingga 72 jam per insiden dan biaya pemulihan langsung rata-rata USD 120.000.[9] Dampak operasional dari serangan tersebut mencakup pembatalan operasi elektif, keterlambatan pelaporan laboratorium yang memperpanjang masa rawat inap, hingga pengalihan pasien ke rumah sakit lain.[9] Namun, yang lebih mengkhawatirkan adalah potensi serangan yang secara langsung menargetkan IoMT. Laporan *Federal Trade Commission* (FTC) Amerika Serikat telah mengidentifikasi bahwa perangkat medis yang terhubung memiliki tiga kerentanan utama: (1) memungkinkan akses tidak sah dan penyalahgunaan informasi pribadi, (2) memfasilitasi serangan terhadap sistem lain melalui perangkat yang dikompromikan, dan (3) menciptakan risiko keselamatan fisik, termasuk kemungkinan pengendalian jarak jauh terhadap perangkat seperti pompa insulin.[17]

Dalam perspektif ketahanan nasional, kerentanan IoMT merupakan ancaman non-militer yang secara langsung dapat mengganggu stabilitas demografi dan keamanan negara. Sebagaimana dirumuskan dalam doktrin pertahanan negara, ancaman nirmiliter didefinisikan sebagai setiap usaha dan kegiatan dari luar maupun dalam negeri yang dinilai membahayakan kedaulatan negara, keutuhan wilayah negara, dan keselamatan segenap bangsa, dengan menggunakan faktor-faktor nirmiliter seperti teknologi dan informasi.[1]

Ancaman berdimensi teknologi dan informasi disebutkan secara eksplisit dalam Buku Strategi Pertahanan Negara Indonesia sebagai salah satu bentuk ancaman nirmiliter yang perlu diantisipasi, karena kemajuan teknologi informasi dapat dimanfaatkan untuk kejahatan siber yang sulit dideteksi dan dapat mengakibatkan kerusakan fisik. Dalam klasifikasi ancaman militer sekalipun disebutkan bahwa sabotase terhadap objek vital nasional dan instalasi strategis yang menggunakan kemajuan ilmu pengetahuan dan teknologi dapat memiliki intensitas yang lebih tinggi dan kompleks, dan aksi teror bersenjata dapat menyasar siapa saja termasuk fasilitas kesehatan.

Dalam kerangka geostrategi Indonesia, konsepsi ketahanan nasional dibangun di atas dua pendekatan yang saling terkait: pendekatan kesejahteraan (*welfare approach*) dan pendekatan keamanan (*security approach*).[10] Pendekatan kesejahteraan bertujuan mengembangkan potensi bangsa menjadi kemakmuran yang adil dan merata, sedangkan pendekatan keamanan bertujuan melindungi eksistensi dan nilai-nilai bangsa dari ancaman.[10] Kedua pendekatan ini tidak dapat dipisahkan.

Dalam konteks IoMT, jika suatu negara gagal menjamin keamanan siber atas perangkat medis yang digunakan oleh warganya, maka pendekatan keamanan menjadi hampa karena nyawa pasien yang menggunakan alat pacu jantung atau pompa insulin dapat terancam oleh serangan dari jarak jauh. Di sisi lain, pendekatan kesejahteraan juga terganggu karena biaya pemulihan dari serangan siber membebani sistem kesehatan nasional dan pada akhirnya membebani anggaran negara. Penelitian di Amerika Serikat menunjukkan bahwa serangan siber terhadap rumah sakit selain menimbulkan kerugian finansial langsung juga merusak kepercayaan publik terhadap sistem kesehatan, menurunkan efisiensi pelayanan, dan dalam kasus ekstrem dapat menyebabkan kematian yang seharusnya dapat dicegah.[22]

Ketahanan kesehatan nasional, sebagai salah satu pilar dari ketahanan nasional secara keseluruhan, tidak mungkin terwujud jika infrastruktur kesehatan digitalnya rentan terhadap eksploitasi. Prinsip sistem pertahanan semesta yang dianut Indonesia yang melibatkan seluruh warga negara, wilayah,

dan sumber daya nasional lainnya menuntut bahwa perlindungan terhadap IoMT harus menjadi tanggung jawab bersama antara pemerintah (sebagai regulator dan pengawas), produsen perangkat (sebagai perancang dan pembuat), penyedia layanan kesehatan (sebagai pengguna dan pengelola), serta pasien (sebagai pengguna akhir).[1] Namun, tanggung jawab bersama ini tidak akan efektif tanpa adanya standar teknis yang mengikat dan mekanisme penegakan hukum yang jelas. Saat ini, belum ada satu pun peraturan di Indonesia yang mewajibkan produsen alat pacu jantung untuk membuktikan bahwa perangkatnya tahan terhadap serangan siber sebelum mendapatkan izin edar. Ini adalah kekosongan hukum yang sangat berbahaya, karena konsekuensi dari kegagalan keamanan bukanlah kebocoran data semata, melainkan kematian.

Beberapa penelitian menunjukkan bahwa di negara-negara maju, perkembangan tanggung jawab produk (*product liability*) untuk perangkat IoT telah mulai mendapat perhatian, meskipun putusan pengadilan yang berhasil masih sangat terbatas.[22] Di Amerika Serikat, gugatan hukum terhadap produsen mobil atas kerentanan keamanan siber pada sistem infotainment ditolak karena pengadilan menilai bahwa ancaman yang belum terwujud tidak memenuhi syarat *standing* untuk mengajukan gugatan.[23] Namun, untuk perangkat medis, argumen bahwa kerentanan siber merupakan cacat desain (*design defect*) dapat dibangun dengan lebih kuat karena tingkat risikonya jauh lebih tinggi dan dapat diukur secara medis.

Di Uni Eropa, Directive (UE) 2024/2853 tentang tanggung jawab produk telah diperbarui dan mulai berlaku pada 9 Desember 2024 dan wajib diimplementasikan pada 9 Desember 2026, secara eksplisit memasukkan perangkat lunak sebagai produk dan mengakui bahwa kemampuan untuk belajar atau memperoleh fitur baru setelah dipasarkan dapat menjadi indikator cacat produk.[24] Ketentuan ini sangat relevan untuk IoMT yang menggunakan kecerdasan buatan atau *machine learning*, karena perilaku algoritma yang berubah seiring waktu dapat menimbulkan risiko baru yang tidak terdeteksi pada saat perangkat pertama kali dipasarkan.

Indonesia, dengan sistem hukum sipil yang menganut *statute orientation*, tidak dapat secara otomatis mengadopsi putusan-putusan pengadilan sebagai preseden yang mengikat. Namun, setidaknya perkembangan di negara lain menunjukkan bahwa pertanggungjawaban hukum atas kegagalan keamanan siber IoMT adalah sebuah keniscayaan yang akan terus berkembang. Oleh karena itu, konstruksi hukum perlindungan IoMT di Indonesia saat ini harus dinilai sebagai belum memadai untuk menjamin ketahanan kesehatan nasional,

tetapi bukan berarti tidak ada sama sekali. Yang ada adalah kerangka awal yang masih sangat umum dan belum menyentuh persoalan teknis yang paling krusial.

Di Amerika Serikat, Pada tahun 2017, Badan Pengawas Obat dan Makanan Amerika Serikat (FDA) menarik 465.000 unit alat pacu jantung produksi Abbott (sebelumnya St. Jude Medical) setelah ditemukan kerentanan siber pada protokol komunikasi nirkabel perangkat tersebut.[25] Kerentanan itu memungkinkan pihak tidak berwenang dalam jarak dekat untuk mengirimkan perintah yang dapat menguras baterai secara cepat atau mengubah parameter pacu jantung secara tidak semestinya.

Meskipun belum ada laporan bahwa kerentanan tersebut benar-benar dieksploitasi untuk merugikan pasien, FDA mengklasifikasikan tindakan penarikan ini sebagai *corrective action* preventif karena potensi bahaya yang ditimbulkan dinilai signifikan dan dapat mengancam nyawa.[26] Preseden ini menunjukkan bahwa bahkan produsen global sekalipun dapat mengabaikan aspek keamanan siber ketika tidak ada kewajiban regulasi yang mengikat.

Jika Amerika Serikat merespons melalui penguatan kewenangan administratif FDA, Uni Eropa memilih jalur yang berbeda dengan merevisi secara fundamental rezim tanggung jawab produk. Directive (EU) 2024/2853 tentang tanggung jawab atas produk cacat yang mulai berlaku pada 9 Desember 2024 dan wajib diimplementasikan pada 9 Desember 2026 secara eksplisit memasukkan perangkat lunak yang termasuk sistem operasi, *firmware*, dan sistem kecerdasan buatan sebagai produk yang tunduk pada tanggung jawab tanpa kesalahan (*no-fault liability*).[24] Hal ini krusial bagi ketahanan kesehatan nasional sebab arahan tersebut mengatur bahwa kelalaian produsen dalam menyediakan pembaruan keamanan siber yang diperlukan untuk menjaga keamanan produk sepanjang siklus hidupnya dapat dikualifikasikan sebagai cacat produk.

Arahan ini juga memberlakukan *presumption of defectiveness* dan *presumption of causation* ketika pembuktian menjadi terlalu sulit bagi pihak yang dirugikan karena kompleksitas teknis atau ilmiah produk dimana hal ini merupakan sebuah ketentuan yang sangat relevan untuk IoMT yang menggunakan algoritma *machine learning* dengan efek *black box*.[24] Indonesia tidak memiliki mekanisme hukum yang setara. Dalam terminologi pertahanan negara, ketiadaan ini merupakan kesenjangan kapabilitas proyeksi kedaulatan hukum ke dalam tata kelola rantai pasok global. Padahal, fungsi penangkalan terhadap produsen asing tidak akan optimal tanpa adanya instrumen hukum yang mampu menjangkau pelaku ancaman di luar yurisdiksi teritorial.

Secara normatif, Indonesia sebenarnya telah memiliki landasan untuk menjerat korporasi yang lalai. Pasal 70 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menentukan bahwa apabila tindak pidana dilakukan oleh korporasi, pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau korporasi itu sendiri, dengan pidana denda yang dapat mencapai sepuluh kali lipat dari maksimal pidana denda yang diancamkan (hingga Rp50.000.000.000,00).[11] Ketentuan ini diperkuat oleh Pasal 118 Kitab Undang-Undang Hukum Pidana (KUHP) yang secara tegas mengakui korporasi sebagai subjek pidana.[27]

Investigasi kebocoran data BPJS Kesehatan yang melibatkan 279 juta catatan kependudukan tidak pernah sampai pada identifikasi pelaku utama karena keterbatasan kemampuan digital forensik dan karena pelaku menggunakan *Virtual Private Network* (VPN) serta server proksi untuk menyembunyikan lokasi.[28] Indonesia yang belum meratifikasi Konvensi Budapest tentang Kejahatan Siber juga mengalami keterbatasan dalam mekanisme pertukaran bukti digital dan permintaan bantuan hukum timbal balik (*Mutual Legal Assistance*) dengan negara lain.[28]

Selama kapasitas teknis ini tidak ditingkatkan, maka fungsi penindakan dalam sistem pertahanan nirmiliter tidak akan pernah efektif. Produsen IoMT yang lalai mengetahui bahwa kemungkinan mereka dituntut secara pidana di Indonesia sangat kecil karena aparat tidak memiliki kemampuan untuk mengumpulkan dan membuktikan rantai kausalitas yang memenuhi standar pembuktian pidana. Kondisi ini menjadikan rezim pertanggungjawaban pidana korporasi di Indonesia tidak berfungsi secara optimal dalam memberikan efek jera.

Untuk menutup kesenjangan antara norma hukum dan kapasitas penegakan, diperlukan intervensi kebijakan strategis. Dalam jangka pendek, BSSN dan Kementerian Kesehatan seyogianya harus mengeluarkan Peraturan Bersama yang mengadopsi standar internasional seperti ISO 81001-1:2021 tentang *Health software and health IT systems safety, effectiveness and security* sebagai acuan teknis wajib bagi setiap perangkat IoMT yang beredar di Indonesia.[29]

Pemerintah juga harus mempercepat ratifikasi Konvensi Budapest tentang Kejahatan Siber untuk membuka akses terhadap mekanisme *Mutual Legal Assistance* dengan negara-negara anggota, yang sangat diperlukan untuk menelusuri pelaku kejahatan siber lintas batas.[28]

Kemudian, Rancangan Undang-Undang Keamanan dan Ketahanan Siber yang sedang dalam proses pembahasan harus secara eksplisit mencantumkan IoMT sebagai bagian dari *Critical Information Infrastructure* (CII) dan mewajibkan setiap operator CII di sektor kesehatan untuk menerapkan standar keamanan siber yang mengikat, dengan sanksi administratif dan pidana yang tegas bagi yang melanggar. Tanpa langkah ini, status ketahanan nasional Indonesia pada gatra pertahanan dan keamanan yang menurut pengukuran Lemhannas tahun 2016 masih berada pada level "kurang tangguh" dengan indeks 2,60 dari skala 1 sampai 5 tidak akan pernah mengalami peningkatan yang signifikan.[2]

Transformasi dari Regulasi Reaktif menuju Kerangka Proaktif

Kerangka regulasi Indonesia yang bersifat reaktif dan data-centric, serta belum adanya kewajiban sertifikasi pra-pasar sebagaimana telah diuraikan secara panjang lebar pada sub-bab sebelumnya, menunjukkan perlunya transformasi paradigma menuju pendekatan device-centric yang proaktif. Amerika Serikat, melalui kerangka regulasi yang dibangun oleh Food and Drug Administration (FDA), menawarkan sebuah model solusi yang telah teruji secara empiris dan terus disempurnakan berdasarkan dinamika ancaman. Namun, solusi bagi Indonesia tidak dapat dihasilkan melalui peniruan mentah-mentah atas teks regulasi asing, melainkan melalui kontekstualisasi terhadap elemen-elemen kunci dari model FDA ke dalam realitas hukum, kelembagaan, dan kapasitas teknis industri kesehatan Indonesia, dengan tetap berpegang pada kerangka geostrategi ketahanan nasional.

Keunggulan utama kerangka FDA terletak pada sifatnya yang holistik dan terintegrasi, mengakui bahwa keamanan siber perangkat medis harus dijamin sepanjang siklus hidup produk (*total product lifecycle*), dimulai dari konseptualisasi desain hingga penghentian operasional perangkat. Landasan hukumnya kokoh di bawah *Federal Food, Drug, and Cosmetic Act* (FD&C Act) yang diperkuat oleh Section 524B melalui *Food and Drug Omnibus Reform Act* (FDORA) tahun 2022, yang secara sah mendefinisikan *cyber device* sebagai setiap perangkat yang mencakup perangkat lunak, memiliki kemampuan untuk terhubung ke internet (baik disengaja maupun tidak), dan rentan terhadap ancaman siber.[30]

Definisi yang luas dan jelas ini memberikan FDA yurisdiksi tegas tanpa ruang tawar bagi produsen yang ingin menghindari tanggung jawab. Selanjutnya, persyaratan pra-pasar FDA bersifat preventif dan sangat terperinci. Panduan final "*Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions*" yang direvisi terakhir kali pada bulan Februari 2026 mewajibkan produsen untuk mengadopsi dan mendokumentasikan *Secure Product Development Framework* (SPDF), termasuk

penyusunan *security risk management plan*, *threat modeling*, dan *cybersecurity risk assessment* yang komprehensif. Selain itu, kewajiban penyediaan *Software Bill of Materials* (SBOM) memungkinkan pemantauan kerentanan secara proaktif ketika celah keamanan ditemukan pada komponen pihak ketiga di masa depan. Panduan ini juga mewajibkan serangkaian pengujian yang ketat, seperti uji ketahanan (*fuzz testing*) dan uji penetrasi oleh pihak independen, serta persyaratan *labeling* yang transparan, termasuk informasi tentang prosedur pembaruan perangkat lunak (*patchability view*) agar pengguna akhir dapat mengelola risiko residual. Semua persyaratan ini bersifat mengikat dan menjadi prasyarat untuk mendapatkan izin edar.

Di sisi lain, FDA juga melengkapi kerangka proaktifnya dengan kewajiban pasca-pasar yang mengikat melalui panduan "*Postmarket Management of Cybersecurity in Medical Devices*" (2016), yang mengharuskan produsen untuk terus memantau, mengidentifikasi, dan merespons kerentanan siber setelah perangkat beredar. Jika suatu kerentanan dinilai menimbulkan *uncontrolled risk* (risiko tidak terkendali) terhadap keselamatan pasien, produsen wajib melakukan tindakan remediasi (seperti pembaruan perangkat lunak darurat) dalam waktu 60 hari dan melaporkannya kepada FDA, dengan kegagalan mematuhi dapat dikenai sanksi administratif serta tuntutan perdata di bawah *False Claims Act* yang potensi dendanya telah mencapai jutaan dolar AS, seperti yang terjadi pada kasus Illumina tahun 2025. Perbandingan kerangka regulasi keamanan siber IoMT antara Indonesia dan Amerika Serikat tersebut disajikan pada Tabel 1.

Tabel 1. Komparasi Kerangka Regulasi Keamanan Siber IoMT: Indonesia vs. Amerika Serikat

Aspek Perbandingan	Indonesia	Amerika Serikat
Orientasi Regulasi	Reaktif dan *data-centric*; berfokus pada perlindungan data pribadi dan penanganan insiden pasca-kejadian.	Proaktif dan *device-centric*; berfokus pada keamanan siklus hidup produk (*total product lifecycle*).
Pengawasan Pra-Pasar	Tidak ada mekanisme sertifikasi atau verifikasi keamanan siber sebagai prasyarat perizinan alat kesehatan.	Wajib dan ketat; produsen harus mendokumentasikan *Secure Product Development Framework* (SPDF) dan pengujian penetrasi.
Pengawasan Pasca-	Pemantauan	Berkelanjutan; produsen

Pasar	dibebankan pada fasilitas kesehatan (pengelola data), tidak menyentuh kerentanan perangkat yang menempel pada pasien.	wajib memantau kerentanan dan melakukan remediasi/pembaruan perangkat lunak maksimal dalam 60 hari.
Kewajiban Produsen	Belum diatur secara spesifik	Mengikat; wajib menyediakan *Software Bill of Materials* (SBOM) dan rencana manajemen risiko keamanan.
Standar Teknis	Masih bersifat umum (seperti ISO 27001) dan tidak dirancang khusus untuk keterbatasan komputasi IoMT.	Spesifik dan terukur; diatur secara mutlak melalui *Final Guidance FDA* tentang *Cybersecurity in Medical Devices*.
Sanksi dan Kewenangan Lembaga	Sanksi denda mengacu pada UU PDP; tidak ada otoritas teknis spesifik untuk menguji atau menarik alat medis yang rentan.	FDA berwenang menolak izin edar (*Section 524B*) dan menarik produk (*recall*); sanksi denda korporasi yang sangat besar.

Bagi Indonesia, momentum yang paling strategis adalah memanfaatkan Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) yang saat ini telah masuk dalam Program Legislasi Nasional (Prolegnas) Prioritas 2026 dan menjadi harapan utama BSSN untuk mengatasi kelemahan struktural regulasi siber nasional.

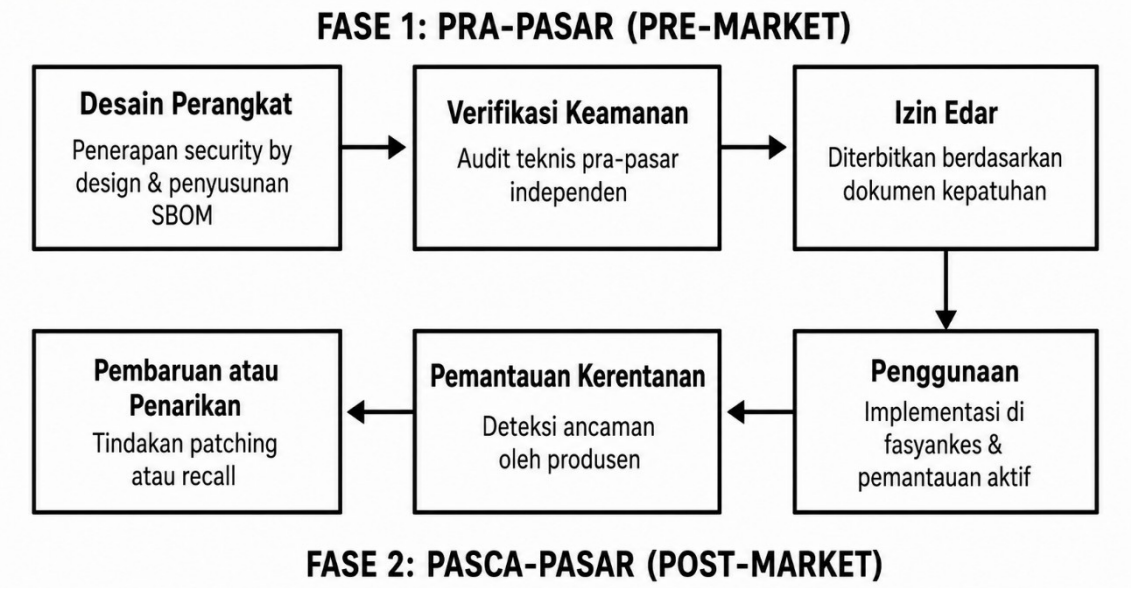
Namun, dalam draf RUU yang ada sejauh ini, cakupan IoMT masih sangat umum dan belum menyentuh tingkat perangkat individual. Oleh karena itu, revisi terhadap RUU KKS mutlak diperlukan sebelum disahkan. Pertama, RUU KKS harus mengadopsi definisi "perangkat siber" yang selaras dengan FDA, yaitu setiap alat kesehatan yang mencakup perangkat lunak, memiliki kemampuan terhubung ke jaringan atau internet, dan rentan terhadap ancaman siber, sehingga tidak ada perangkat yang lolos dari kewajiban ini. Kedua, undang-undang ini harus secara tegas menyatakan bahwa kepatuhan terhadap keamanan siber merupakan prasyarat wajib untuk mendapatkan izin edar dari Kementerian Kesehatan (Kemenkes), sebuah ketentuan yang saat ini sama sekali tidak ada dalam regulasi Indonesia. Ketiga, RUU KKS harus mewajibkan

Kemenkes dan BSSN untuk bersama-sama menyusun peraturan pelaksana yang mewajibkan produsen perangkat IoMT mengadopsi standar teknis yang setara dengan SPDF FDA, seperti yang diatur dalam IEC 81001-5-1 tentang keamanan perangkat lunak kesehatan.[15] Tidak cukup hanya rekomendasi; bagi Indonesia, kewajiban ini harus bersifat mengikat (*mandatory*) dan diverifikasi melalui dokumen yang diaudit oleh unit teknis khusus, sebuah langkah yang membutuhkan transformasi kapasitas kelembagaan secara signifikan.

Paralel dengan penguatan regulasi, kapasitas kelembagaan teknis harus segera ditingkatkan. Saat ini, tidak ada satu pun unit di Kemenkes atau BSSN yang memiliki keahlian teknis untuk mengevaluasi dokumen keamanan siber dari produsen perangkat medis asing. Untuk itu, langkah pertama yang paling mendesak adalah pembentukan Unit Verifikasi Keamanan Siber Medis di bawah Kemenkes, yang dikelola oleh personel dengan latar belakang ganda: teknologi informasi, keamanan siber, dan teknik biomedis. Unit ini akan bertanggung jawab untuk menilai kelengkapan dokumentasi pra-pasar (seperti SBOM, laporan uji penetrasi, dan rencana manajemen risiko) sebelum merekomendasikan penerbitan izin edar. Tanpa unit ini, semua klausul kewajiban dalam RUU KKS akan menjadi mandul karena tidak ada yang mampu memverifikasi kepatuhan produsen.

Selanjutnya, pemerintah harus berinvestasi dalam membangun atau mengakreditasi laboratorium uji keamanan siber perangkat medis nasional yang independen. Laboratorium ini akan melakukan uji penetrasi dan analisis kerentanan secara objektif terhadap sampel perangkat yang diimpor, untuk memverifikasi klaim keamanan produsen. Kapasitas pengujian ini juga akan sangat berharga untuk melakukan investigasi post-market ketika terjadi insiden, sebagaimana FDA memiliki kemampuan untuk memerintahkan *recall* berdasarkan bukti teknis.

Integrasi kewajiban hukum antara fase pra-pasar dan pasca-pasar tersebut dapat dikonstruksikan ke dalam sebuah tata kelola perizinan terpadu, sebagaimana diilustrasikan pada alur regulasi berikut: Skema alur regulasi dimaksud disajikan pada Gambar 1.



Gambar 1. Usulan alur regulasi IoMT

Kelemahan struktural lainnya yang tidak kalah penting adalah lemahnya pilar sarana prasarana forensik digital nasional. Investigasi kebocoran data BPJS Kesehatan (279 juta data warga) dan KPU (2,3 juta data pemilih) tidak pernah sampai pada identifikasi dan penuntasan pelaku utama karena aparat tidak memiliki kemampuan teknis untuk melakukan penelusuran digital (*cyber traceability*) lintas batas.[28] Ketiadaan kapasitas ini secara langsung mematikan fungsi penindakan dalam sistem pertahanan nirmiliter.

Untuk mengatasi ini, Indonesia harus segera meratifikasi Konvensi Budapest tentang Kejahatan Siber. Tanpa akses terhadap mekanisme *Mutual Legal Assistance* (MLA) untuk pertukaran bukti digital dengan negara maju, Indonesia akan terus menjadi surga bagi pelaku kejahatan siber lintas batas dan bagi perangkat medis yang tidak aman.[28]

Terakhir, instrumen hukum yang sudah ada harus diperkuat. Pasal 70 Undang-Undang Pelindungan Data Pribadi yang memungkinkan pidana denda korporasi hingga lima puluh miliar rupiah harus diartikulasikan dengan jelas dalam RUU KKS bahwa kelalaian produsen dalam memenuhi standar keamanan siber yang ditetapkan dapat dikenai sanksi tersebut.[11] Bersamaan dengan itu, Kementerian Kesehatan melalui Direktorat Jenderal Kefarmasian dan Alat Kesehatan harus diberikan mandat atribusi untuk menarik izin edar (recall) setiap perangkat yang terbukti mengandung uncontrolled risk yang tidak diremediasi tepat waktu oleh produsen, sebagaimana FDA secara rutin melakukan tindakan penarikan perangkat medis yang tidak aman.

KESIMPULAN

Berdasarkan analisis yang telah diuraikan, penelitian ini menyimpulkan dua hal utama:

1. Konstruksi hukum perlindungan *Internet of Medical Things* (IoMT) di Indonesia saat ini masih bersifat fragmentaris dan reaktif. Pengaturan yang ada bersandar pada pendekatan *data-centric* melalui UU PDP dan Perpres IIV, yang hanya berfokus pada pelindungan data dan pengelolaan sistem pasca-insiden, sehingga menyisakan kekosongan norma mengenai jaminan keamanan teknis perangkat medis itu sendiri.

2. Terdapat disparitas kerangka regulasi antara Indonesia dan Amerika Serikat. Tidak seperti Indonesia, Amerika Serikat menerapkan rezim proaktif dan *device-centric* di mana *Food and Drug Administration* (FDA) menetapkan kewajiban sertifikasi keamanan siber sejak tahap perancangan (pra-pasar) hingga pengawasan kerentanan (pasca-pasar) sebagai prasyarat mutlak penerbitan izin edar perangkat medis.

Guna menutup celah kerentanan yang mengancam ketahanan kesehatan nasional, penelitian ini merekomendasikan:

1. Pengadopsian standar keamanan pra-pasar (*security by design*) yang bersifat mengikat (mandatory) bagi produsen IoMT sebelum memperoleh izin edar.

2. Pelembagaan mekanisme pengawasan pasca-pasar yang mewajibkan penyediaan pembaruan perangkat lunak (*patching*) secara berkala.

3. Pembentukan Unit Verifikasi Keamanan Siber Medis secara lintas sektoral antara Kementerian Kesehatan dan Badan Siber dan Sandi Negara (BSSN) guna mengaudit kepatuhan teknis produsen.

DAFTAR PUSTAKA

[1] R. Ryacudu, "Wira: Edisi Ketahanan Nasional dan Bela Negara," *Puskom Publik Kemhan*, pp. 1–62, 2018, [Online]. Available: https://www.kemhan.go.id/wp-content/uploads/2018/11/wiraedisikhusus1.pdf

[2] Hari Mulyono, "Geostrategi Indonesia dalam Dinamika Politik Global dan Regional," *J. Kaji. Lemhannas RI*, vol. 29, pp. 19–30, 2017, [Online]. Available: https://jurnal.lemhannas.go.id/index.php/jkl/article/download/131/52

[3] A. Al Kuwaiti *et al.*, "A Review of the Role of Artificial Intelligence in Healthcare," *J. Pers. Med.*, vol. 3188, no. 1, pp. 1–22, 2023, doi: 10.1063/5.0240194.
[4] Pristiya Maulaningrum, Siti Mujanah, and Achmad Yanu Alif Fianto, "Transformasi Digital di Sektor Kesehatan Tinjauan Literatur tentang Penerapan Teknologi Informasi dalam Manajemen Pelayanan," *J. Ilmu Manajemen, Ekon. dan Kewirausahaan*, vol. 5, no. 1, pp. 494–503, 2025, doi: 10.55606/jimek.v5i1.6399.
[5] ANTARA, "BSSN ungkap uu ketahanan siber penting disahkan tahun 2025," 2025. [Online]. Available: https://www.antaranews.com/berita/5110493/bssn-ungkap-uu-ketahanan-siber-penting-disahkan-tahun-2025
[6] Kompas.com, "BSSN: serangan siber naik 7 kali lipat pada 2025 dan berlanjut di awal 2026," 2026. [Online]. Available: https://lestari.kompas.com/read/2026/04/23/192503686/bssn-serangan-siber-naik-7-kali-lipat-pada-2025-dan-berlanjut-di-awal-2026?page=all
[7] AwanPintar.id, "Laporan Ancaman Digital di Indonesi Semester 1 Tahun 2025," 2025. [Online]. Available: https://www.awanpintar.id/wp-content/uploads/2025/08/2025_AwanPintar.id_Laporan_Ancaman_Digital_sem1_2025_Green.pdf
[8] G. Shahrour, A. Junejo, and A. Al-Said Ahmad, "Security and privacy challenges in healthcare IoT systems with cloud, edge, and fog computing: A systematic literature review," *Comput. Sci. Rev.*, vol. 62, no. May, p. 101005, 2026, doi: 10.1016/j.cosrev.2026.101005.
[9] F. Syafar, "Cybersecurity Attacks in Indonesian Healthcare Institutions: Incidence, Operational Impact and a Socio-Technical Defense Framework," *World J. Adv. Eng. Technol. Sci.*, vol. 17, no. 2, pp. 470–474, 2025, doi: 10.30574/wjaets.2025.17.2.1507.
[10] Muthia Salsabila, Zaenul Slam, Mutiara Nur Alamsyah, and Hifzah Dwi Hilmi, "National Resilience in Historical and Geostrategic Perspectives: Essence and Conception," *J. Lemhannas RI*, vol. 12, no. 4, pp. 435–450, 2024, doi: 10.55960/jlri.v12i4.956.
[11] Pemerintah Pusat, *Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*, no. 016999. 2022, p. 1. [Online]. Available: https://peraturan.bpk.go.id/Download/224884/UU Nomor 27 Tahun 2022.pdf
[12] Kemenkes RI, "Sandbox kesehatan 2025 resmi dibuka." [Online]. Available: https://www.kemkes.go.id/id/sandbox-kesehatan-2025-resmi-dibuka
[13] ANTARA, "BSSN ungkap uu ketahanan siber penting disahkan tahun 2025," 2025. [Online]. Available:

https://www.antaranews.com/berita/5110493/bssn-ungkap-uu-ketahanan-siber-penting-disahkan-tahun-2025
[14] K. Raihan and S. D. Rosadi, "Have AI-Enhanced Telemedicines in Indonesia Adopted the Principles of Personal Data Protection?," *Yust. J. Huk.*, vol. 13, no. 2, pp. 151–167, 2024, doi: 10.20961/yustisia.v13i2.85996.
[15] FDA, "cybersecurity medical devices quality management system considerations and content premarket." [Online]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-management-system-considerations-and-content-premarket
[16] FDA, "for the Premarket Cybersecurity Guidance : Section 524B of the FD & C Act," 2024. [Online]. Available: https://www.fda.gov/media/178134/download
[17] A. H. Tran, "The Internet of Things and Potential Remedies in Privacy Tort Law," *Columbia J. Law Soc. Probl.*, pp. 2016–2017, 2017, [Online]. Available: http://www.columbia.edu/cu/jlsp/pdf/Winter2017/Tran.pdf
[18] Pemerintah Republik Indonesia, *Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 Tentang Pelindungan Infrastruktur Informasi Vital*. 2022, pp. 1–19. [Online]. Available: https://peraturan.bpk.go.id/Download/205174/Perpres Nomor 82 Tahun 2022.pdf
[19] Permenkes RI No 24, *Permenkes RI No 24 Tahun 2022 Tentang Rekam Medis*, vol. 151, no. 2. 2022, pp. 10–17. [Online]. Available: https://peraturan.bpk.go.id/Download/301563/Permenkes Nomor 24 Tahun 2022.pdf
[20] Pemerintah Republik Indonesia, *PERATURAN BADAN SIBER DAN SANDI NEGARA REPUBLIK INDONESIA NOMOR 10 TAHUN 2023 TENTANG PENGUKURAN TINGKAT KEMATANGAN KEAMANAN SIBER*, vol. 2. 2024, pp. 306–312. [Online]. Available: https://peraturan.bpk.go.id/Download/350568/%5BSALINAN%5D-Peraturan-BSSN-Nomor-10-Tahun-2023_signed.pdf
[21] Pemerintah Republik Indonesia, *PERATURAN BADAN SIBER DAN SANDI NEGARA NOMOR 9 TAHUN 2021 TENTANG PERUBAHAN ATAS PERATURAN BADAN SIBER DAN SANDI NEGARA NOMOR 8 TAHUN 2021 TENTANG PENYELENGGARAAN PENILAIAN KESIAPAN PENERAPAN SNI ISO/IEC 27001 MENGGUNAKAN INDEKS KEAMANAN INFORMASI*, vol. Nomor 65, no. 879. 2015, pp. 2004–2006. [Online]. Available: https://peraturan.bpk.go.id/Download/220749/Peraturan BSSN No. 9 Tahun 2021.pdf
[22] J. R. Fichtner and T. J. Strader, "Will Products Liability Litigation Help

Protect IoT Users from Cyber-Physical Attacks?," *J. Int. Technol. Inf. Manag.*, vol. 31, no. 1, pp. 79–96, 2022, doi: 10.58729/1941-6679.1515.
[23] U.S. District Court — Northern District of California, "cahen v toyota motor." [Online]. Available: https://case-law.vlex.com/vid/cahen-v-toyota-motor-890868705
[24] Official Journal of the European Union, "DIRECTIVE (EU) 2024/2853 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC (Text with EEA relevance)," 2024.
[25] Beckerlaw, "FDA Recalls 465 , 000 Pacemakers Over Cyber Security Threat," 2017.
[26] R. z. Arndt, "Abbott recall signals new era in medical-device cybersecurity," 2017, *Health Tech*.
[27] Pemerintah Republik Indonesia, *Undang-undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana*, no. 16100. 2023, pp. 1–345.
[28] S. Y. Simanjuntak and B. Waluyo, "Criminal Liability for Hacking Personal Data through Ransomware Attacks on Digital Service Providers in Indonesia," *J. Daulat Huk.*, vol. 8, no. 4, pp. 851–861, 2025.
[29] "ISO 81001-1:2021: Health software and health IT systems safety, effectiveness and security," 2021.
[30] FDA, "cybersecurity." [Online]. Available: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity