

Analisis Tematik Hambatan dan Kebutuhan Kebijakan Keamanan Data Pribadi Sistem Informasi Laboratorium

Nurul Huda^{1*}, Feby Artwodini Muqtadiroh², Reny Nadlifatin³, Rr. Sri Isjworowati⁴

Institut Teknologi Sepuluh Nopember, Indonesia^{1,2,3}

Akademi Kesehatan 17 Agustus 1945 Semarang, Indonesia⁴

Email: 6032241094@student.its.ac.id*

Keywords:

Data Security; Laboratory Information System; Personal Data Protection; Thematic Analysis; Medical Laboratory Technologist

Abstract

Laboratory Information Systems (LIS) manage specific personal health data under Indonesia's Personal Data Protection Law No. 27/2022 and Ministry of Health Regulation No. 24/2022, yet the practical barriers and policy needs perceived by LIS users remain unmapped. This research aims to map regulatory awareness, implementation barriers, and data-security policy needs among Medical Laboratory Technologists (MLT). As the qualitative component of a concurrent embedded mixed-methods study, three mandatory open-ended questions were administered to 310 MLT of the Semarang branch of PATELKI, producing 773 quotations analyzed through two-cycle thematic analysis in ATLAS.ti 23 (41 active codes, 18 code groups). Regulatory awareness was relatively high (58.4%). The largest single barrier category was the absence of perceived barriers (23.2%); human and organizational barriers outnumbered technical ones, while complaints that procedures slow services were nearly absent (0.6%) against 60 quotations demanding stricter enforcement. The leading policy needs were periodic training, enforced standard operating procedures, role-based access control, and two-factor authentication. The findings support a three-pillar intervention framework spanning technology, process, and governance, and indicate that security socialization should emphasize efficacy and institutional commitment rather than threat. Health facilities, professional organizations, and LIS developers can use this user-grounded map to prioritize security interventions aligned with regulatory mandates.

Kata Kunci:

Keamanan Data; Sistem Informasi Laboratorium; Pelindungan Data Pribadi; Analisis Tematik; Ahli Teknologi Laboratorium Medik

Abstrak

Sistem Informasi Laboratorium (SIL) mengelola data kesehatan pribadi spesifik yang diatur Undang-Undang Pelindungan Data Pribadi No. 27/2022 dan Peraturan Menteri Kesehatan No. 24/2022, namun hambatan praktis dan kebutuhan kebijakan dari perspektif pengguna SIL belum terpetakan. Penelitian ini bertujuan memetakan kesadaran regulasi, hambatan implementasi, dan kebutuhan kebijakan keamanan data pada Ahli Teknologi Laboratorium Medik (ATLM). Sebagai komponen kualitatif dari studi mixed-methods concurrent embedded, tiga pertanyaan terbuka wajib diberikan kepada 310 ATLM DPC PATELKI Kota Semarang, menghasilkan 773 kutipan yang dianalisis dengan analisis tematik dua siklus pada ATLAS.ti 23 (41 kode aktif, 18 kelompok kode). Kesadaran regulasi relatif tinggi (58,4%). Kategori hambatan tunggal terbesar justru ketiadaan hambatan yang dirasakan (23,2%); hambatan manusia dan organisasi melampaui hambatan teknis, sementara keluhan bahwa prosedur memperlambat layanan nyaris nihil (0,6%) berbanding 60 kutipan yang menuntut penegakan lebih tegas. Kebutuhan kebijakan utama adalah pelatihan berkala, penegakan prosedur operasional standar,

kontrol akses berbasis peran, dan autentikasi dua faktor. Temuan mendukung kerangka intervensi tiga pilar yang mencakup teknologi, proses, dan tata kelola, serta menunjukkan bahwa sosialisasi keamanan sebaiknya menekankan efikasi dan komitmen institusional, bukan ancaman. Fasilitas kesehatan, organisasi profesi, dan pengembang SIL dapat menggunakan peta berbasis pengguna ini untuk memprioritaskan intervensi keamanan yang selaras dengan mandat regulasi.

PENDAHULUAN

Sistem Informasi Laboratorium (SIL) merupakan tulang punggung pelayanan laboratorium klinik yang mengelola hasil pemeriksaan, data demografi pasien, dan alur kerja diagnostik, serta berperan penting dalam meningkatkan mutu pelayanan (Tangdililing & Pramarta, 2023). Platform SIL kini kian terintegrasi dengan sistem informasi rumah sakit dan instrumen diagnostik melalui protokol standar (Edayan et al., 2024). Di Indonesia, lebih dari 2.800 laboratorium klinik memproses jutaan rekam pasien setiap tahun, dan adopsi sistem informasi kesehatan terus meluas di berbagai fasilitas (Aisyah et al., 2025). Data yang dikelola SIL tergolong data pribadi yang bersifat spesifik menurut Undang-Undang Pelindungan Data Pribadi Nomor 27 Tahun 2022 (Republik Indonesia, 2022), dengan kewajiban pengamanan yang dipertegas Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis (Kementerian Kesehatan RI, 2022). Pelanggaran membawa ancaman sanksi administratif hingga Rp 2 miliar dan pidana hingga enam tahun penjara, sehingga pelindungan data pasien dalam digitalisasi layanan kesehatan menjadi isu yang semakin mengemuka (Syahrial & Sara, 2024).

Meskipun mandat regulasi telah berlaku, kesenjangan kepatuhan masih ditemukan dalam praktik, antara lain pengiriman hasil laboratorium secara informal melalui aplikasi pesan, berbagi kredensial akses antar-shift, dan implementasi kontrol akses yang belum memadai (Posey et al., 2015; Sari et al., 2022). Penelitian manajemen informasi kesehatan di Indonesia selama ini banyak menyoroti kelengkapan dan mutu data untuk mendukung pengambilan keputusan (Etylusfina, 2024), serta faktor adopsi sistem laboratorium elektronik (Riana et al., 2021), sementara dimensi keamanan dan pelindungan data dari perspektif pengguna garis depan masih jarang dikaji. Studi keamanan informasi kesehatan pun lebih banyak menggunakan pendekatan kuantitatif terhadap intensi kepatuhan (Alanazi & Soh, 2019), sehingga suara pengguna mengenai hambatan riil dan kebutuhan kebijakan yang mereka prioritaskan belum terpetakan, khususnya pada profesi Ahli Teknologi Laboratorium Medik (ATLM) pasca-pemberlakuan UU Pelindungan Data Pribadi.

Dua kerangka teori mendominasi kajian perilaku keamanan informasi. Protection Motivation Theory menyatakan perilaku protektif didorong oleh penilaian ancaman dan penilaian koping (Rogers, 1975), yang kemudian disempurnakan dengan menekankan peran efikasi diri (Maddux & Rogers, 1983). Privacy Calculus Theory memandang keputusan privasi sebagai penimbangan manfaat dan risiko (Dinev & Hart, 2006), dan kepedulian privasi menjadi konstruk sentral dalam riset privasi sistem informasi (Malhotra et al., 2004; Smith et al., 2011). Fenomena privacy paradox menunjukkan kesenjangan antara sikap dan perilaku privasi yang lazim ditemukan pada konteks sukarela (Kokolakis, 2017).

Urgensi penelitian ini didorong oleh sanksi hukum berat yang menuntut kepatuhan, namun kesenjangan praktik seperti berbagi kredensial dan kontrol akses belum memadai masih

ditemukan (Posey et al., 2015; Sari et al., 2022). Dengan lebih dari 2.800 laboratorium memproses jutaan data sensitif harian, potensi dampak pelanggaran sangat masif. Belum adanya peta kebutuhan berbasis pengguna membuat intervensi yang ada cenderung umum dan tidak menjawab hambatan operasional, sementara digitalisasi layanan kesehatan yang cepat (Aisyah et al., 2025) menuntut keseimbangan antara akselerasi dan keamanan data, menjadikan pemahaman perspektif pengguna sangat mendesak untuk mencegah insiden yang mengguncang kepercayaan publik.

Penelitian ini bertujuan memetakan tiga hal dari perspektif ATLM sebagai pengguna SIL: tingkat kesadaran terhadap regulasi perlindungan data, hambatan implementasi prosedur keamanan, serta kebutuhan dan rekomendasi kebijakan untuk meningkatkan kepatuhan. Artikel ini merupakan komponen kualitatif dari penelitian berdesain mixed-methods concurrent embedded; komponen kuantitatif berupa pemodelan determinan intensi kepatuhan dianalisis dan dilaporkan secara terpisah.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif yang tertanam dalam desain mixed-methods concurrent embedded (Creswell & Plano Clark, 2018). Partisipan adalah 310 ATLM anggota DPC PATELKI Kota Semarang, diperoleh melalui probability sampling dengan PATELKI sebagai gatekeeper institusional dari populasi 1.233 anggota, melampaui target formula Slovin sebesar 302 responden pada margin kesalahan 5%. Mayoritas responden perempuan (81,6%), berpendidikan D3 Teknologi Laboratorium Medik (73,6%), berpengalaman lebih dari sepuluh tahun sebagai ATLM (61,9%), dan telah menggunakan SIL lebih dari lima tahun (66,5%). Profil lengkap karakteristik responden disajikan pada Tabel 1.

Tabel 1. Profil Responden (N = 310)

Karakteristik	Kategori	n	%
Jenis kelamin	Perempuan	253	81,6
	Laki-laki	57	18,4
Usia	25–35 tahun	153	49,4
	36–45 tahun	93	30,0
	> 45 tahun	51	16,5
	< 25 tahun	13	4,2
Pendidikan	D3 Analis Kesehatan/TLM	228	73,5
	D4 / Sarjana Terapan TLM	68	21,9
	S1 Biologi/Kimia/Kesehatan	10	3,2
	S2 / Magister	4	1,3
Jabatan	Pelaksana / Analis	249	80,3
	Koordinator / PJ Unit	40	12,9
	Kepala Instalasi / Lab.	11	3,5
	Lainnya	10	3,2
Lama sebagai ATLM	> 10 tahun	192	61,9
	1–5 tahun	60	19,4
	6–10 tahun	53	17,1
	< 1 tahun	5	1,6
Lama menggunakan LIS	> 5 tahun	206	66,5
	3–5 tahun	50	16,1
	1–3 tahun	40	12,9
	< 1 tahun	14	4,5
Jenis fasyankes	RS Swasta	117	37,7

RS Pemerintah	77	24,8
Puskesmas	42	13,5
Laboratorium Kesehatan	29	9,4
Laboratorium Klinik Mandiri	17	5,5
Klinik Pratama / Utama	16	5,2
Lainnya (PMI/UDD, dll.)	12	3,9

Sumber: ATLAS.ti (Document Groups), data demografis responden (2026).

Komposisi sampel ini menjadi dasar pertimbangan keteralihan (transferability) temuan. Dominasi responden berpengalaman lebih dari sepuluh tahun (61,9%) serta pengguna SIL lebih dari lima tahun (66,5%) merupakan konteks penting bagi interpretasi pada bagian pembahasan, sementara keragaman jenis fasilitas layanan—rumah sakit pemerintah dan swasta, puskesmas, hingga laboratorium mandiri—memperluas keteralihan temuan ke beragam latar layanan laboratorium, meskipun cakupannya tetap terbatas pada satu kota.

Data dikumpulkan melalui tiga pertanyaan terbuka wajib pada kuesioner daring: pengalaman dan kesadaran terhadap regulasi perlindungan data, hambatan terbesar dalam menerapkan prosedur keamanan dan perlindungan data pasien, serta kebutuhan dan saran perbaikan kebijakan. Terkait pertimbangan etik, partisipasi bersifat sukarela dengan informed consent yang disampaikan pada bagian awal kuesioner; seluruh respons dikumpulkan secara anonim tanpa meminta pengenalan langsung (nama, kontak, atau identitas lain) sebagai penerapan prinsip minimisasi data; setiap responden hanya diberi kode urut (RESP001–RESP310) untuk keperluan analisis, dan kerahasiaan data dijaga sepanjang penelitian. Analisis tematik mengikuti tahapan Braun dan Clarke (2006) dengan bantuan perangkat lunak ATLAS.ti versi 23 terhadap 773 kutipan dari 310 dokumen responden. Koding dilakukan dua siklus: inductive coding pada putaran pertama untuk membiarkan tema muncul dari data, dilanjutkan deductive recoding pada putaran kedua untuk menyelaraskan tema dengan kerangka Protection Motivation Theory dan Privacy Calculus Theory. Hasil akhir berupa 41 kode aktif dalam 18 kelompok kode, terbagi tiga keluarga: hambatan, kebutuhan, dan kesadaran regulasi. Frekuensi dilaporkan sebagai grounded count, yaitu jumlah kutipan per kode; angka tersebut bersifat deskriptif (quasi-statistics) untuk menopang interpretasi, bukan statistik inferensial (Maxwell, 2010). Kredibilitas temuan diperkuat melalui triangulasi internal—konvergensi antara grounded count, jaringan ko-okurensi kode, dan kutipan verbatim—sehingga pola yang dilaporkan, termasuk kedua temuan paradoksal, diposisikan sebagai proposisi analitis yang bersifat transferable, bukan generalisasi statistik.

Artikel ini melaporkan komponen kualitatif dari penelitian tesis magister penulis pertama pada Program Magister Manajemen Teknologi, Institut Teknologi Sepuluh Nopember (2026), yang menggunakan desain concurrent embedded mixed-methods dengan analisis PLS-SEM dan analisis tematik atas sampel yang sama; komponen kuantitatif berupa model intensi kepatuhan dilaporkan secara terpisah.

HASIL DAN PEMBAHASAN

Kesadaran terhadap Regulasi

Distribusi tema kesadaran regulasi disajikan pada Tabel 2. Sebanyak 181 responden (58,4%) telah mengetahui UU Pelindungan Data Pribadi dan/atau PMK 24/2022, sementara 41 responden (13,2%) belum mengetahuinya. Sebanyak 18 responden (5,8%) menyatakan sudah mengetahui namun tetap membutuhkan sosialisasi tambahan, dan 17 responden (5,5%) secara

proaktif mengusulkan topik sosialisasi spesifik, suatu bentuk keterlibatan yang mencerminkan internalisasi kepedulian privasi.

Tabel 2. Distribusi Kode Kesadaran Regulasi (N = 310)

Kode	Tema	f	%
C3.1	Sudah tahu UU PDP/PMK 24	181	58,4
C3.2	Belum mengetahui regulasi	41	13,2
C3.3	Sudah tahu, butuh sosialisasi	18	5,8
C3.4	Memberi saran topik sosialisasi	17	5,5
C9.x	Non-respons / umum	53	17,1

Sumber: Codebook ATLAS.ti, hasil analisis tematik (2026).

Baseline kesadaran yang relatif tinggi sejalan dengan masifnya pemberitaan UU Pelindungan Data Pribadi pasca-2022. Namun, 13,2% responden yang belum mengetahui regulasi, ditambah 11,3% yang meminta sosialisasi lanjutan atau mengusulkan topiknya, menunjukkan distribusi kesadaran yang belum merata dan memberi sasaran konkret bagi program edukasi dinas kesehatan dan organisasi profesi.

Pola berlapis ini tampak langsung pada suara partisipan. Mayoritas menyatakan telah memahami kewajiban dasar, namun menuntut sosialisasi yang lebih operasional dan spesifik:

“Ya, saya sudah memahami kewajiban dasar tersebut, terutama terkait pengelolaan kerahasiaan rekam medis elektronik. Namun, sosialisasi yang lebih mendalam dan spesifik mengenai langkah-langkah praktis mitigasi atau SOP jika terjadi insiden kebocoran data di level operasional laboratorium masih sangat diperlukan.”
(RESP192)

Sebaliknya, partisipan yang mengaku belum sepenuhnya paham justru mampu menyebutkan kebutuhan yang sangat spesifik, menandakan kepedulian privasi yang laten dan siap diaktifkan:

“Belum sepenuhnya. Informasi yang paling perlu disosialisasikan: kewajiban pelaporan insiden kebocoran data dalam waktu 3×24 jam, pengaturan hak akses data pasien, serta sanksi terhadap pelanggaran perlindungan data.” (RESP029)

Hambatan Implementasi Keamanan Data

Tabel 3 menyajikan sepuluh tema hambatan teratas. Temuan paling mencolok justru kategori tidak ada hambatan atau sudah baik (H7.1) yang mendominasi dengan 72 kutipan (23,2%). Hambatan substantif terkonsentrasi pada empat kategori: sumber daya manusia (kelompok H1, 76 kutipan), teknologi (kelompok H2, 60 kutipan), sumber daya (kelompok H4, 33 kutipan), dan organisasi (kelompok H3, 32 kutipan).

Tabel 3. Sepuluh Tema Hambatan Teratas (N = 310)

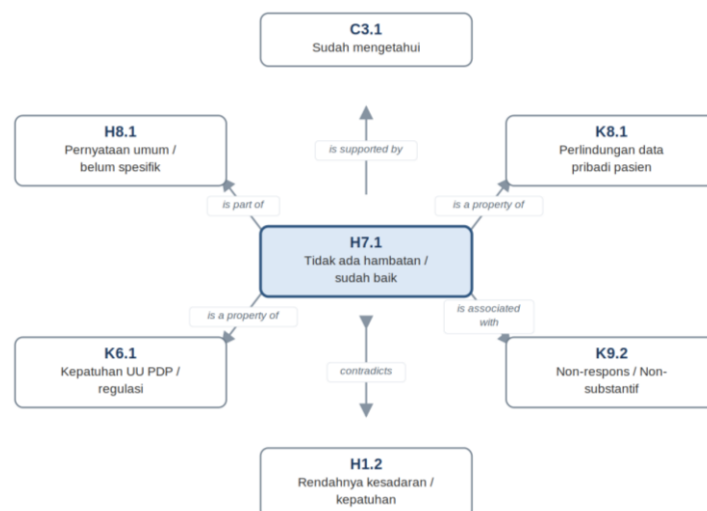
Kode	Tema	f	%
H7.1	Tidak ada hambatan/sudah baik	72	23,2
H1.2	Rendah kesadaran/kepatuhan staf	33	10,6
H2.2	Sistem error/bug/lambat	24	7,7
H4.1	Biaya/anggaran terbatas	18	5,8
H2.3	Sistem belum terintegrasi	18	5,8
H3.1	SOP/regulasi belum jelas	16	5,2
H1.3	Kurang pelatihan/kompetensi IT	16	5,2
H1.1	Berbagi password/akun	15	4,8
H4.2	SDM IT terbatas	15	4,8
H2.1	Jaringan tidak stabil	13	4,2

Sumber: Codebook ATLAS.ti, hasil analisis tematik (2026). *f* = grounded count.

Dominasi kategori “tidak ada hambatan” (23,2%) pada profesi yang menangani data sensitif setiap hari membentuk apa yang penelitian ini namai sebagai Reverse Privacy Paradox: alih-alih cemas berlebihan, pengguna cenderung meremehkan risiko karena rutinitas kerja yang selama ini berjalan tanpa insiden. Satu respons merangkum paradoks ini sekaligus paradoks berikutnya dalam satu tarikan napas:

“Tidak ada [hambatan]. Karena sudah berjalan. Menggunakan kode OTP. Yang ada malah bikin lama. Tapi memang keamanan data pasien terjamin.” (RESP042)

Gambar 1 memetakan jaringan kode di sekitar persepsi “tidak ada hambatan” (H7.1): persepsi ini didukung oleh kesadaran regulasi (C3.1) dan klaim perlindungan data pasien (K8.1), namun secara langsung bertentangan dengan pengakuan rendahnya kesadaran dan kepatuhan (H1.2).



Gambar 1. Jaringan Reverse Privacy Paradox di sekitar kode H7.1 “Tidak ada hambatan / sudah baik”

Sumber: Data primer (diolah dengan ATLAS.ti 23, 2026)

Pola tidak ada hambatan tampak pada respons seperti “*Sejauh ini belum ada hambatan yang besar*” dan “*tidak ada hambatan, asal semua pelaksanaan pelayanan dilakukan sesuai SOP yang ada*”. Sebaliknya, hambatan faktor manusia diungkap melalui pernyataan “*masih banyak yang kurang sadar diri atas penggunaan sistem lama yang riskan untuk*

disalahgunakan” serta praktik “masih sering berbagi akses/password, alur pelaporan belum jelas”.

Hambatan akses yang konkret berulang kali muncul. Seorang partisipan menggambarkan kerentanan prosedural yang lugas:

“Orang lain dapat meminta hasil pemeriksaan laboratorium hanya dengan menyebutkan nama pasien dan tanggal lahir pasien ke petugas lab.” (RESP304)

sementara partisipan lain menautkan kerentanan itu pada struktur organisasi tempatnya bekerja:

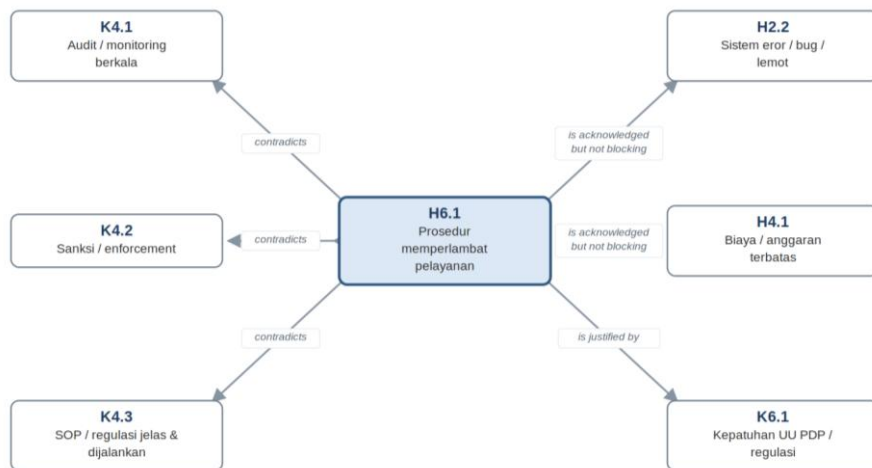
“(1) Sistem rolling tempat kerja membuat perubahan role akses bagi petugas sangat cepat; (2) sebagai RS pendidikan, peserta didik bisa mengakses data pasien; (3) banyak perangkat yang harus diakses oleh satu petugas membuat petugas harus sering log in–log out.” (RESP087)

Dominasi pengakuan tidak ada hambatan pada profesi dengan paparan risiko data harian mengindikasikan kombinasi etika profesi yang kuat dengan potensi bias optimisme (Weinstein, 1980): rutinitas kerja bertahun-tahun tanpa insiden membentuk ilusi kekebalan, terlebih 61,9% responden berpengalaman lebih dari sepuluh tahun. Dalam kerangka Extended Parallel Process Model (Witte, 1992), kampanye yang menonjolkan ancaman tanpa efikasi berisiko memicu fear control berupa penyangkalan alih-alih danger control berupa tindakan protektif. Penelitian kepatuhan keamanan informasi kesehatan berbasis Protection Motivation Theory menegaskan bahwa keyakinan akan efikasi merupakan pendorong perilaku protektif yang lebih kuat daripada rasa takut (Lee & Seomun, 2021). Hambatan yang teridentifikasi juga dominan bersifat manusiawi-organisasional (108 kutipan) dibandingkan teknis murni, konsisten dengan literatur yang menempatkan perilaku pengguna sebagai kerentanan utama yang tidak terselesaikan oleh kontrol teknis semata (Herath & Rao, 2009; Sari et al., 2022). Perbedaan budaya keamanan informasi antar-fasilitas kesehatan di Indonesia turut memengaruhi konsistensi penerapan praktik tersebut (Sari et al., 2021). Temuan signifikan lainnya adalah kelangkaan keluhan prosedur memperlambat pelayanan yang hanya muncul pada 2 kutipan (0,6%), kontras dengan 60 kutipan yang menuntut penegakan lebih ketat. Asimetri ini menunjukkan bahwa dalam konteks kepatuhan yang diwajibkan, prosedur keamanan dimaknai sebagai sinyal keseriusan institusi, bukan beban, sejalan dengan teori keadilan prosedural (Tyler, 1990).

Asimetri tersebut hanya 0,6% mengeluh prosedur memperlambat layanan berbanding 60 kutipan yang menuntut penegakan lebih tegas, membentuk paradoks kedua yang penelitian ini namai Mandatoriness Paradox: ketika kepatuhan bersifat wajib (mandatory), prosedur keamanan dimaknai sebagai sinyal keseriusan institusi, bukan beban yang menghambat. Hanya dua partisipan yang menyuarakan keluhan ini, salah satunya:

“Waktu tunggu pelayanan menjadi lebih lama karena banyak langkah yang harus dilewati. Dan adanya batasan akses membuat waktu tunggu konfirmasi hasil kritis menjadi lebih lama.” (RESP009)

Gambar 2 menunjukkan bahwa keluhan “prosedur memperlambat” (H6.1) justru bertentangan dengan tuntutan akan SOP, audit, dan sanksi (kelompok K4); diakui namun tidak dianggap menghambat bersama kendala sistem dan biaya (H2.2, H4.1); serta dijustifikasi oleh kepatuhan terhadap regulasi (K6.1).



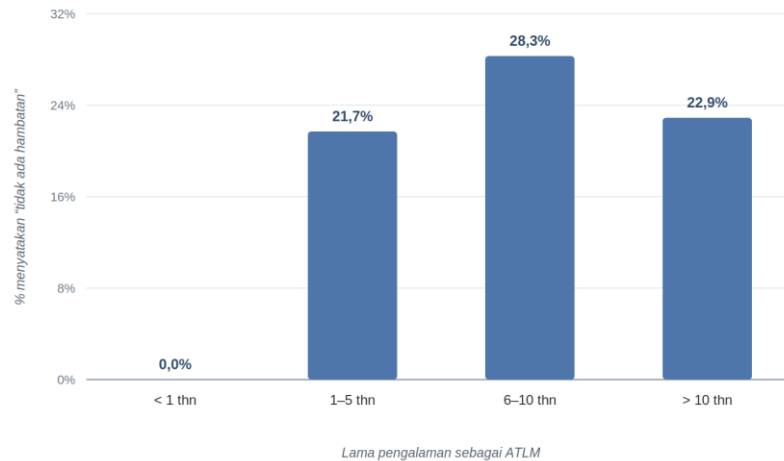
Gambar 2. Jaringan Mandatoriness Paradox di sekitar kode H6.1 “Prosedur memperlambat pelayanan”

Sumber: Data primer (diolah dengan ATLAS.ti 23, 2026)

Konfirmasi Lintas-Karakteristik Subkelompok

Analisis lintas-subkelompok memperkuat kedua paradoks di atas dan menunjukkan bahwa keduanya bukan artefak data. Pertama, kesadaran terhadap regulasi tidak menjamin implementasi yang mulus. Dari 176 responden yang menyatakan telah mengetahui regulasi (C3.1), sebanyak 59,1% tetap melaporkan hambatan konkret dan hanya 23,3% yang menyatakan tidak ada hambatan. Kesenjangan kesadaran–tindakan ini merupakan manifestasi kualitatif dari privacy paradox, yakni lemahnya keterkaitan antara pengetahuan dan perilaku protektif (Kokolakis, 2017), sekaligus menegaskan bahwa persepsi “sudah aman” pada Reverse Privacy Paradox tidak bersumber dari kompetensi aktual.

Kedua, persepsi “tidak ada hambatan” (H7.1) menunjukkan gradien yang khas menurut pengalaman sebagaimana disajikan pada Gambar 3. Seluruh responden dengan pengalaman kurang dari satu tahun (0%) justru mampu mengidentifikasi hambatan, sementara proporsi yang merasa tidak ada hambatan melonjak ke kisaran 21,7–28,3% setelah melewati tahun pertama; pola serupa muncul pada lama penggunaan SIL. Gradien ini konsisten dengan habituasi dan bias optimisme (Weinstein, 1980): kewaspadaan pendatang baru terkikis oleh rutinitas kerja yang berlangsung tanpa insiden, bukan oleh meningkatnya keamanan objektif.



Gambar 3. Gradien persepsi “tidak ada hambatan” (H7.1) menurut lama pengalaman sebagai ATLM

Sumber: Data primer (diolah dengan ATLAS.ti 23, 2026)

Konvergensi kedua pola tersebut—kesenjangan kesadaran—tindakan dan gradien habituasi—menunjukkan bahwa Reverse Privacy Paradox merupakan pola yang konsisten lintas-subkelompok, bukan sekadar temuan agregat. Implikasinya, intervensi keamanan tidak cukup berhenti pada penyampaian pengetahuan, melainkan perlu menekankan penyegaran efikasi secara berkala, terutama untuk mengantisipasi erosi kewaspadaan pada pengguna yang telah berpengalaman.

Kebutuhan dan Rekomendasi Kebijakan

Tabel 4 menyajikan sepuluh tema kebutuhan teratas. Prioritas responden bersifat operasional: pelatihan penyegaran berkala (32 kutipan) menjadi kebutuhan tunggal tertinggi, diikuti SOP yang jelas dan dijalankan (26), role-based access control (25), autentikasi dua faktor (22), dan peningkatan sistem keamanan (21).

Tabel 4. Sepuluh Tema Kebutuhan Teratas (N = 310)

Kode	Tema	f	%
K1.1	Pelatihan/penyegaran berkala	32	10,3
K4.3	SOP jelas dan dijalankan	26	8,4
K2.2	Role-based access control	25	8,1
K2.1	Autentikasi ganda/OTP/2FA	22	7,1
K3.3	Upgrade sistem keamanan	21	6,8
K1.2	Sosialisasi internal staf	20	6,5
K2.3	Password management	18	5,8
K4.1	Audit/monitoring berkala	18	5,8
K4.2	Sanksi/enforcement konsisten	16	5,2
K8.1	Perlindungan data pasien	13	4,2

Sumber: Codebook ATLAS.ti, hasil analisis tematik (2026).

Kebutuhan pelatihan diungkap melalui pernyataan seperti “*perlunya refresh berkala tentang pentingnya patuh terhadap privasi pengguna LIS*”, sedangkan kebutuhan tata kelola tampak pada usulan “*penyusunan dan penegakan SOP perlindungan data pasien yang jelas*”

dan sesuai regulasi” yang disertai “pelatihan rutin, reward bagi yang patuh, dan punishment bagi yang melanggar”. Satu respons representatif menggambarkan kematangan pertimbangan: “tingkat keamanan sebaiknya disesuaikan dengan kemampuan mitigasi risiko masing-masing institusi”.

Kebutuhan tata kelola yang komprehensif terungkap dalam respons yang merinci langkah berlapis dari hulu ke hilir:

“Langkah yang paling perlu dilakukan antara lain: penyusunan dan penegakan SOP perlindungan data pasien yang jelas dan sesuai regulasi; pelatihan rutin dan sosialisasi kepada seluruh petugas laboratorium; penerapan kontrol akses berbasis peran (role-based access control); audit dan monitoring berkala; serta penerapan sanksi tegas terhadap pelanggaran privasi data.” (RESP057)

Namun sejumlah partisipan menegaskan bahwa akar persoalan bukan semata teknologi, melainkan komitmen dan pemahaman individual:

“Minimnya komitmen pribadi petugas untuk melindungi data pasien karena kurang paham sebab/akibat bila terjadi kebocoran data.” (RESP073)

Peta kebutuhan ini membentuk kerangka intervensi tiga pilar yang dapat dioperasionalkan fasilitas kesehatan. Pilar teknologi mencakup role-based access control, autentikasi dua faktor, kebijakan manajemen password, dan peningkatan sistem (95 tuntutan) yang sekaligus menjawab praktik berbagi akun. Pilar proses mencakup pelatihan penyegaran berkala dan sosialisasi internal yang dijadwalkan rutin dengan konten berbasis efikasi, sejalan dengan prinsip bahwa penguatan keyakinan diri mendorong perilaku protektif (Maddux & Rogers, 1983). Pilar tata kelola mencakup SOP yang dijalankan, audit berkala, serta sanksi yang konsisten. Urutan implementasinya penting: membangun kapabilitas teknologi dan pelatihan sebaiknya mendahului penegakan, agar tuntutan kepatuhan disertai sarana untuk mematuhi. Keterbatasan penelitian ini mencakup cakupan satu kota dan respons tertulis singkat yang tidak memungkinkan pendalaman sebagaimana wawancara; studi lanjutan dengan wawancara mendalam lintas wilayah serta evaluasi eksperimental kerangka tiga pilar akan memperkuat dasar bukti kebijakan.

KESIMPULAN

Pasca-pemberlakuan UU Pelindungan Data Pribadi, ATLM menunjukkan baseline kesadaran regulasi yang relatif tinggi (58,4%) namun belum merata. Hambatan implementasi keamanan data didominasi faktor manusia dan organisasi, yaitu rendahnya kesadaran staf, praktik berbagi kredensial, dan SOP yang belum jelas, melebihi hambatan teknis, sementara hampir seperempat responden tidak merasakan hambatan sama sekali. Beban prosedural nyaris tidak dikeluhkan; sebaliknya responden menuntut penegakan yang lebih ketat. Kebutuhan kebijakan terkonsentrasi pada pelatihan berkala, SOP yang dijalankan, kontrol akses berbasis peran, dan autentikasi dua faktor. Fasilitas kesehatan direkomendasikan mengadopsi kerangka tiga pilar (teknologi, proses, tata kelola) dengan pesan sosialisasi berbasis efikasi dan komitmen institusional, bukan berbasis ancaman. Penelitian lanjutan disarankan menggunakan wawancara mendalam lintas wilayah dan tipe fasilitas serta menguji kerangka tiga pilar secara eksperimental. Secara konseptual, penelitian ini mengidentifikasi dua paradoks dalam konteks kepatuhan privasi yang diwajibkan, yaitu *Reverse Privacy Paradox* dan *Mandatoriness*

Paradox, yang menjelaskan mengapa intervensi keamanan sebaiknya menekankan efikasi dan komitmen institusional alih-alih ancaman.

REFERENSI

- Aisyah, D. N., Setiawan, A. H., Mayadewi, C. A., Lokopessy, A. F., Kozlakidis, Z., & Manikam, L. (2025). Understanding health information systems utilization across public health centers in Indonesia: cross-sectional study. *JMIR Medical Informatics*, 13(1), e68613.
- Alanazi, M. H., & Soh, B. (2019). Behavioral intention to use IoT technology in healthcare settings. *Engineering, Technology & Applied Science Research*, 9(5), 4769-4774.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101.
- Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). Sage Publications.
- Crossler, R., & Belanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices instrument. *The Data Base for Advances in Information Systems*, 45(4), 51-71.
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.
- Edayan, J. M., Gallemmit, A. J., Sacala, N. E., Palmer, X. L., Potter, L., & Rarugal, J. (2024). Integration technologies in laboratory information systems: A systematic review. *Informatics*, 11(3), 54.
- Etylusfina, E. (2024). Tinjauan kelengkapan data dan informasi rekam medis untuk mendukung pengambilan keputusan kesehatan. *Jurnal Rekam Medis dan Informasi Kesehatan*, 7(1), 32-39.
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.
- Kementerian Kesehatan Republik Indonesia. (2022). *Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis*. Kementerian Kesehatan RI.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122-134.
- Lee, E., & Seomun, G. (2021). Structural model of the healthcare information security behavior of nurses applying protection motivation theory. *International Journal of Environmental Research and Public Health*, 18(4), 2084.
- Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469-479.
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355.
- Maxwell, J. A. (2010). Using numbers in qualitative research. *Qualitative Inquiry*, 16(6), 475-482. <https://doi.org/10.1177/1077800410364740>
- Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, 32(4), 179-214.
- Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Sekretariat Negara.
- Riana, D., Hidayanto, A. N., Hadianti, S., & Napitupulu, D. (2021). Integrative factors of e-health laboratory adoption: A case of Indonesia. *Future Internet*, 13(2), 27.

- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93-114.
- Sari, P. K., Candiwan, C., & Trianasari, N. (2022). Information security behavior in health information systems: A review of research trends and antecedent factors. *Healthcare*, 10(12), 2531.
- Sari, P. K., Handayani, P. W., Hidayanto, A. N., & Sandhyaduhita, P. I. (2021). Information security cultural differences among health care facilities in Indonesia. *Heliyon*, 7(6), e07272.
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989-1015.
- Syahrial, S., & Sara, R. (2024). Health data protection and patient privacy in the context of digitalization of public health services in Indonesia. *EAI Endorsed Transactions*.
- Tangdililing, M. L., & Pramarta, V. (2023). Peran sistem informasi laboratorium dalam meningkatkan mutu pelayanan laboratorium. *Jurnal Manajemen dan Administrasi Rumah Sakit Indonesia*, 7(2), 112-120.
- Tyler, T. R. (1990). *Why people obey the law*. Princeton University Press.
- Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, 39(5), 806-820.
- Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, 59(4), 329-349.