Indonesian Journal of Health Information Management Service (IJHIMS)
p-ISSN 2909-0462 (print) | e-ISSN 2809-0241 (online) Vol. 5, No. 1, Bulan Mei 2025

Optimalisasi Keamanan dan Kesadaran Perilaku Cyber Pengguna Sistem RME di RSUD Limpung Kabupaten Batang

Fitria Wulandari[1], Oki Setiono[2*], Arif Kurniadi[3]
[1,2,3] Program Studi D3 RMIK, Fakultas Kesehatan, Universitas Dian Nuswantoro Semarang, Indonesia
*Corresponding author: okisetiono@dsn.dinus.ac.id

ABSTRAK. RSUD Limpung Kabupaten Batang telah melaksanakan Rekam Medis Elektronik (RME), berdasarkan hasil survey masih di temukan kendala dalam implementasi RME di RSUD Limpung yaitu keterbatasan infrastruktur IT dan dukungan serta ketrampilan SDM dalam menggunakan RME. Tujuan kegiatan ini untuk meningkatkan pemahaman petugas tentang keamanan *system* RME dan meningkatkan kesadaran perilaku *cyber* di kalangan pengguna sistem, yang terdiri dari tenaga kesehatan dan staf administrasi. Kegiatan ini mencakup audit keamanan melalui wawancara, penilaian risiko, pelatihan keamanan informasi, serta sosialisasi dengan media edukatif. Hasil evaluasi menunjukkan bahwa kerentanan utama berasal dari perilaku pengguna, seperti penggunaan kata sandi yang lemah dan kurangnya pembaruan sistem. Pelatihan yang diberikan berhasil meningkatkan pemahaman peserta terhadap praktik keamanan data, yang terlihat dari peningkatan skor hasil *post-test*. Sosialisasi juga memberikan dampak positif terhadap kesadaran kolektif dalam menjaga kerahasiaan informasi pasien. Namun, observasi menunjukkan masih adanya kesenjangan antara pemahaman dan praktik di lapangan. Oleh karena itu, diperlukan tindak lanjut berupa pelatihan berkelanjutan dan penguatan kebijakan internal rumah sakit. Pengabdian ini memberikan kontribusi nyata dalam membangun budaya keamanan informasi yang lebih baik di lingkungan RSUD Limpung serta mendukung kualitas pelayanan kesehatan yang berbasis sistem informasi yang aman dan terpercaya.

Kata kunci: Keamanan data; Rekam Medis Elektronik; Perilaku *Cyber*; RSUD Limpung, Sosialisasi Digital

ABSTRACT. *The Electronic Medical Records (EMR) system has been implemented at RSUD Limpung, Batang Regency. Based on survey results, challenges in EMR implementation were identified, such as limitations in IT infrastructure and insufficient human resources support and skills in using the system. The aim of this activity was to enhance officers' understanding of EMR system security and increase cyber behavior awareness among system users, including healthcare personnel and administrative staff. The activities included a security audit through interviews, risk assessment, information security training, and socialization using educational media. The evaluation showed that the main vulnerabilities stemmed from user behavior, such as weak password usage and lack of system updates. The training successfully improved participants' understanding of data security practices, reflected in the increased survey scores. Socialization positively impacted collective awareness in maintaining patient information confidentiality. However, observations revealed gaps between understanding and field practices. Therefore, continuous training and the strengthening of internal hospital policies are needed. This community service has contributed to building a better information security culture at RSUD Limpung, supporting the quality of healthcare services based on a secure and reliable information system.*

Keywords*: Information Security; Electronic Medical Records; Cyber Behavior; RSUD Limpung; Digital Socialization*

PENDAHULUAN

Perkembangan era industri 4.0 mendorong pemanfaatan perangkat dan informasi digital dalam berbagai aspek, termasuk hiburan, pengetahuan, dan pendidikan. Di sektor kesehatan, informasi digital berkembang pesat, memperluas akses dan sumber informasi melalui internet (Rachmani et al., 2023).

Keamanan informasi merupakan salah satu aspek penting dalam pengelolaan sistem informasi rumah sakit di sektor Kesehatan. Rumah sakit yang mengimplementasikan sistem elektronik seperti RME (Rekam Medis Elektronik) harus memastikan bahwa data yang dikelola, terutama data pasien, terlindungi dengan baik dari potensi ancaman *cyber* yang semakin kompleks (Navisa Putri et al., 2024). Keamanan informasi di rumah sakit tidak hanya bergantung pada teknologi, tetapi juga pada perilaku dan kesadaran pengguna sistem tersebut dalam menghadapi risiko *cyber* (Budi et al., 2025).

RSUD Limpung Kabupaten Batang, sebagai salah satu rumah sakit di Indonesia, selain sebagai salah satu rumah sakit daerah, rumah sakit tersebut dituntut untuk memenuhi harapan masyarakat dengan menyediakan pelayanan kesehatan yang aman, ramah, dan berkualitas, disertai fasilitas yang memadai

untuk mendukung proses penyembuhan pasien. Oleh karena itu, penting bagi RSUD Limpung untuk terus mengoptimalkan kualitas pelayanan dan fasilitas demi kepuasan pasien, serta untuk menjaga kepercayaan masyarakat terhadap layanan kesehatan yang diberikan (Sigit & Syaqiq, 2021).

RSUD Limpung Kabupaten Batang mengadopsi sistem RME dalam operasionalnya. Meskipun sistem RME membawa banyak manfaat dalam meningkatkan efisiensi pengelolaan data medis dan administrasi rumah sakit, tantangan besar muncul terkait dengan ancaman terhadap integritas dan kerahasiaan data yang dikelola. Ancaman ini bisa berupa serangan siber seperti peretasan atau kebocoran data, yang tidak hanya dapat merugikan pasien tetapi juga dapat menurunkan kepercayaan masyarakat terhadap rumah sakit (Fatmala Putri & Ratna Sari, 2023)berdasarkan hasil survey awal peneliti melihat, pentingnya bagi RSUD Limpung untuk mengidentifikasi dan mengurangi potensi risiko dengan melakukan evaluasi teknis terhadap sistem RME dan meningkatkan kesadaran perilaku *cyber* di kalangan pengguna sistem.

Menurut penelitian yang dilakukan oleh (Algiffary et al., 2023), kesadaran pengguna dalam mengelola data dan informasi sangat berpengaruh terhadap tingkat keamanan sistem informasi rumah sakit. Pengguna sistem, baik tenaga medis maupun administrasi, perlu memahami pentingnya praktik keamanan dasar seperti penggunaan kata sandi yang kuat, pengamanan perangkat, dan pengelolaan informasi sensitif pasien. Tanpa adanya kesadaran yang cukup, risiko kebocoran data atau penyalahgunaan informasi akan semakin tinggi.

Tujuan dari pengabdian ini adalah untuk melakukan evaluasi teknis terhadap keamanan sistem RME yang digunakan di RSUD Limpung Kabupaten Batang serta meningkatkan kesadaran perilaku *cyber* di kalangan penggunanya. Dengan pendekatan yang terstruktur, diharapkan dapat ditemukan solusi yang efektif untuk meningkatkan keamanan informasi dan perilaku pengguna dalam menghadapi ancaman *cyber* yang ada. RSUD limpung telah melakukan kegiatan sosialisasi kepada petugas terkait dengan palaksanaan RME, begitu pula dengan upaya kemanan data, salah satunya dengan pembagian user dan password untuk masing-masing petugas. Kesadaran pengguna untuk melakukan penggantian password secara berkala masih kurang, sehingga memungkinkan terjadinya ketidak amanan data baik sengaja maupun tidak, sehingga peneliti melihat perlunya dilakukan kegiatan ini.

METODE

Kegiatan ini di awali dengan pengurusan izin ke RSUD limpung, kemudian dilanjutkan dengan mengurus surat ijin kegiatan pengabdian dari LPPM Udinus. Setelah itu menyepakati hari dan tempat pelaksanaan kegiatan. Di awali dengan pembukaan oleh pimpinan Rumah sakit dan dilanjutkan dengan pemaparan materi. Kegiatan diawali dengan cara memberikan materi dalam bentuk edukasi yang berisi materi yang disampaikan meliputi keamanan data, dan informasi untuk meningkatkan kepedulian pengguna terhadap kemungkinan kejahatan *cyber* atau ancaman terhadap sistem yang di jalankan. Sebelum kegiatan di mulai dilakukan *Pre Test* dan setelah pemberian materi dilakukan Post Test, untuk mengetahui efektifitas materi yang diberikan.

1. Lokasi dan Sasaran

Pengabdian ini dilaksanakan di RSUD Limpung Kabupaten Batang, yang merupakan rumah sakit daerah yang mulai mengadopsi sistem RME dalam pengelolaan data medis dan administrasi rumah sakit. Sasaran utama dalam pengabdian ini adalah pengguna sistem RME yang terdiri dari tenaga kesehatan beserta staf administrasi yang terlibat langsung dalam penggunaan sistem.

2. Tahapan Pelaksanaan

A. Evaluasi Keamanan Sistem RME

Langkah pertama dalam pengabdian ini adalah melakukan observasi terhadap sistem RME yang digunakan di RSUD Limpung. observasi ini bertujuan untuk mengidentifikasi potensi kerentanannya dan memberikan rekomendasi untuk perbaikan (Ariyadi Tamsir, Fadli Hidayatul, Akbar Taufik, 2025). Proses observasi meliputi langkah-langkah berikut:

1) Audit Keamanan Sistem

Audit dilakukan dengan tanya jawab kepada tenaga kesehatan dan staf administrasi untuk memeriksa

infrastruktur teknologi, perangkat keras, dan perangkat lunak yang digunakan dalam sistem RME. Audit ini juga mencakup penilaian terhadap perlindungan data pasien dan pengelolaan hak akses pengguna.

2) **Identifikasi Risiko dan Kerentanan**
Penilaian risiko dilakukan dengan memberikan saran dan masukan terkait potensi ancaman yang dapat mempengaruhi sistem RME, baik dari segi perangkat lunak (seperti celah keamanan aplikasi) maupun perilaku pengguna (misalnya penggunaan kata sandi yang lemah) (Neng Sari Rubiyanti, 2023). Analisis risiko dilakukan untuk mengetahui celah dan potensi kerentanannya.

B. Pelatihan Perilaku *Cyber* untuk Pengguna

Setelah evaluasi keamanan dilakukan, langkah selanjutnya adalah memberikan pelatihan kepada pengguna sistem RME di RSUD Limpung. Pelatihan ini bertujuan untuk meningkatkan kesadaran pengguna mengenai pentingnya praktik keamanan *cyber* yang baik dalam mengelola data medis dan informasi sensitif (Manurung et al., 2023). Program pelatihan mencakup:

1) **Penggunaan Kata Sandi yang Aman**
Pelatihan mengenai pentingnya penggunaan kata sandi yang kuat dan cara-cara untuk menjaga kerahasiaan kata sandi. Pengguna juga dilatih untuk menghindari kebiasaan seperti menggunakan kata sandi yang mudah ditebak atau berbagi kata sandi.
2) **Keamanan Perangkat**
Edukasi tentang pengamanan perangkat yang digunakan dalam sistem RME, seperti komputer, tablet, dan smartphone, yang terhubung dengan jaringan rumah sakit. Hal ini mencakup penggunaan perangkat lunak antivirus, pengaturan firewall, dan pembaruan sistem secara rutin.
3) **Pengenalan Ancaman *Cyber***
Pelatihan mengenai berbagai jenis ancaman *cyber* yang dapat menyerang rumah sakit, seperti *phishing*, *malware*, dan *ransomware*. Pengguna diberi pemahaman mengenai cara-cara untuk mengidentifikasi dan menghindari potensi serangan tersebut.
4) **Praktik Keamanan Data**
Pelatihan tentang cara menjaga kerahasiaan data pasien dan informasi medis yang sensitif. Pengguna dilatih untuk tidak mengakses atau membagikan informasi yang tidak relevan dengan pekerjaan mereka dan bagaimana cara menyimpan data dengan aman.
5) **Simulasi dan Evaluasi**
Menyediakan simulasi situasi serangan *cyber*, seperti percakapan phishing atau percakapan dengan malware, untuk mengukur reaksi pengguna dalam menghadapi ancaman tersebut. Hasil dari simulasi ini digunakan untuk memberikan umpan balik dan memperkuat pembelajaran.

C. Penyuluhan dan Sosialisasi

Sebagai bagian dari upaya untuk meningkatkan kesadaran, dilakukan juga sosialisasi tentang pentingnya keamanan data kepada seluruh staf rumah sakit. Sosialisasi ini menggunakan berbagai media, seperti poster, brosur, dan video yang menjelaskan langkah-langkah keamanan dasar yang harus diterapkan di setiap bagian rumah sakit.

3. Teknik Pengumpulan Data

Metode dalam kegiatan ini adalah Pendidikan masyarakat dalam hal ini adalah tenaga kesehatan di RSUD Limpung, pada kegiatan ini dilakukan edukasi untuk meningkatkan pemahaman tentang keamanan data dan perilaku yang memungkinkan munculnya kejahatan (*cyber crime*).

4. Teknik Analisis Data

Data yang terkumpul dari wawancara, *post-test*, dan observasi akan dianalisis secara kualitatif. Analisis kualitatif digunakan untuk mengidentifikasi pola, tema, dan masalah yang muncul selama pelaksanaan evaluasi dan pelatihan, serta untuk menggali pemahaman dan persepsi pengguna terkait keamanan *cyber*.

HASIL DAN PEMBAHASAN

Pada bagian ini, akan dibahas hasil yang diperoleh dari pelaksanaan metode pengabdian yang telah dijelaskan sebelumnya. Pembahasan ini mencakup evaluasi keamanan sistem RME, pelatihan perilaku cyber, serta pengumpulan data yang dilakukan melalui wawancara, *post-test*, dan observasi langsung.

Untuk memberikan gambaran yang lebih nyata terhadap proses pelaksanaan kegiatan, pada subbab ini juga disertakan dokumentasi berupa gambar-gambar kegiatan pengabdian yang dilakukan di RSUD Limpung Kabupaten Batang. Gambar tersebut mencakup proses audit dan wawancara dengan tenaga Kesehatan dan staf administrasi, sesi pelatihan dan penyuluhan, serta kegiatan observasi di lingkungan rumah sakit. Dokumentasi visual ini bertujuan untuk memperkuat penjelasan data dan mendukung pemahaman pembaca terhadap proses serta dampak nyata dari kegiatan yang telah dilaksanakan.

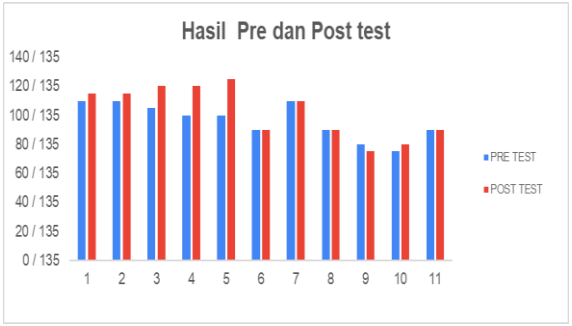
Gambar 1. Kegiatan sosialisasi keamanan dan kesadaran perilaku *cyber*

Gambar 1 tersebut menunjukkan kegiatan pelatihan sosialisasi keamanan dan kesadaran *cyber* yang diberikan kepada tenaga kesehatan dan staf administrasi RSUD Limpung, selanjutnya proses pelaksanaan *post-test* terkait pemahaman dan kesadaran mereka terhadap keamanan data. Dokumentasi ini merepresentasikan keterlibatan aktif peserta dalam memahami praktik perlindungan data yang baik dan pentingnya menjaga kerahasiaan informasi pasien dalam penggunaan sistem RME.

Gambar 2. Kegiatan pelatihan dan *post-test* keamanan dan kesadaran perilaku *cyber*

Gambar 2 tersebut menunjukkan kegiatan pelatihan keamanan data serta keseriusan mereka saat mengisi *post-test*. Kegiatan berlangsung interaktif, dengan diskusi yang aktif terkait ancaman siber dan praktik perlindungan data pasien. Dokumentasi ini mencerminkan komitmen RSUD Limpung dalam meningkatkan kesadaran dan kapasitas staf terhadap keamanan informasi.

Hasil *post-test* yang diperoleh dari 12 peserta menunjukkan bahwa kegiatan pelatihan dan sosialisasi memberikan dampak positif terhadap peningkatan pemahaman peserta terkait keamanan informasi dan perilaku *cyber* dalam penggunaan sistem Rekam Medis Elektronik (RME). Berikut adalah grafik perolehan skor pre dan post test



Grafik 1. Hasil Pre dan Post Test

Skor rata-rata peserta mencapai 102,7 dengan skor tertinggi 125 dan skor terendah 75. Sebagian besar peserta memperoleh skor di atas rata-rata, yang menunjukkan bahwa sebagian besar peserta mampu memahami materi yang diberikan dengan baik.

1. Hasil Evaluasi Keamanan Sistem RME

Temuan dari evaluasi sistem menunjukkan bahwa masih terdapat kerentanan, terutama pada aspek perilaku pengguna, seperti penggunaan kata sandi yang lemah dan kurangnya pembaruan perangkat lunak. Hasil *post-test* memperkuat temuan ini, di mana beberapa peserta masih belum memahami secara menyeluruh konsep-konsep seperti *two-factor authentication*, tindakan saat menghadapi serangan siber, dan praktik aman dalam penggunaan RME. Hal ini menjadi catatan penting bahwa meskipun teknologi sudah tersedia, pemahaman dan kedisiplinan pengguna sangat menentukan keamanan sistem.

2. Hasil Pelatihan Perilaku Cyber untuk Pengguna

Peningkatan skor pasca pelatihan menunjukkan bahwa materi pelatihan berhasil meningkatkan kesadaran dan pengetahuan peserta, terutama pada aspek penggunaan kata sandi yang kuat, pengenalan jenis-jenis ancaman siber (seperti *phishing*), serta pentingnya melakukan pembaruan sistem secara berkala. Peserta juga mulai memahami pentingnya pelaporan insiden keamanan kepada pihak terkait sebagai bagian dari tanggung jawab bersama menjaga integritas sistem informasi rumah sakit.

3. **Hasil Sosialisasi dan Penyuluhan**

Sosialisasi yang dilakukan melalui media visual dan diskusi interaktif terbukti meningkatkan kesadaran peserta. Hal ini tercermin dari skor yang cenderung tinggi pada pertanyaan yang berkaitan dengan konsep dasar keamanan data dan peran pengguna dalam pengelolaan informasi RME. Penyuluhan juga membuka ruang diskusi tentang kondisi nyata di lapangan, seperti hambatan pengguna dalam menjalankan prosedur keamanan yang ideal.

4. Hasil Pengumpulan Data

Data yang diperoleh dari wawancara dan observasi mendukung temuan dalam *post-test*. Peserta mengungkapkan bahwa pelatihan sangat membantu, namun beberapa di antaranya masih merasa perlu pendampingan lanjutan dalam penerapan praktik terbaik sehari-hari. Observasi menunjukkan adanya perubahan positif dalam kebiasaan penggunaan sistem, namun konsistensi penerapan perlu terus didorong melalui kebijakan internal dan pengawasan.

Gambar 2 foto bersama setelah kegiatan berakhir

Hasil *post-test* menunjukkan bahwa pelatihan yang diberikan selama kegiatan pengabdian telah memberikan dampak positif terhadap peningkatan pemahaman peserta mengenai keamanan informasi dan praktik perilaku *cyber* yang baik. Sebagian besar peserta menunjukkan peningkatan skor yang mencerminkan pemahaman yang lebih baik tentang penggunaan sistem RME secara aman, termasuk dalam hal penggunaan kata sandi yang kuat, pengenalan terhadap ancaman siber seperti phishing, serta pentingnya pembaruan sistem secara berkala. Hal ini menunjukkan bahwa pendekatan pelatihan yang diberikan berhasil menumbuhkan kesadaran dan literasi digital di kalangan tenaga kesehatan dan staf administrasi RSUD Limpung.

Selain itu, hasil evaluasi keamanan yang dilakukan melalui wawancara dan audit ringan juga menunjukkan bahwa tantangan utama terletak pada aspek perilaku pengguna, bukan pada infrastruktur teknologi itu sendiri. Beberapa pengguna masih belum sepenuhnya memahami pentingnya pengelolaan hak akses yang benar dan prosedur penanganan jika terjadi insiden siber. Hal ini diperkuat dengan hasil *post-test*, di mana masih ada beberapa pertanyaan yang tidak dijawab dengan benar oleh sebagian peserta, terutama yang berkaitan dengan langkah respons terhadap serangan dan penerapan autentikasi ganda. Dengan demikian, pelatihan dan edukasi yang berkelanjutan sangat dibutuhkan untuk memastikan bahwa pemahaman tersebut dapat diterapkan secara konsisten dalam kegiatan operasional sehari-hari.

Sosialisasi yang dilakukan melalui media visual seperti penyajian *slide* tentang studi kasus dan contoh nyata yang edukatif juga memberikan pengaruh positif terhadap

peningkatan kesadaran (Manurung et al., 2023). Para peserta mengaku lebih memahami pentingnya menjaga kerahasiaan data pasien serta langkah-langkah preventif untuk menghindari kebocoran data. Namun, dari hasil observasi langsung, masih ditemukan beberapa kebiasaan lama yang belum berubah secara signifikan, seperti penggunaan perangkat tanpa proteksi yang memadai. Hal ini menunjukkan adanya kesenjangan antara pemahaman dan penerapan, yang perlu ditindaklanjuti dengan penguatan kebijakan internal serta pengawasan yang lebih intensif dari manajemen rumah sakit.

SIMPULAN

Kegiatan pengabdian ini telah berhasil meningkatkan kesadaran dan pemahaman pengguna terhadap pentingnya keamanan sistem RME dan perilaku cyber yang baik. Untuk mendukung keberlanjutan hasil ini, RSUD Limpung diharapkan dapat melanjutkan program pelatihan secara berkala, membentuk kebijakan keamanan informasi yang lebih terstruktur, serta mendorong budaya keamanan digital di lingkungan kerja. Dengan upaya yang konsisten dan komprehensif, keamanan informasi di rumah sakit dapat terjaga dengan lebih baik demi perlindungan data pasien dan peningkatan mutu pelayanan kesehatan.

UCAPAN TERIMAKASIH

Ucapan terima kasih kami sampaikan atas kesempatan yang diberikan untuk berkontribusi dalam peningkatan pemahaman terkait keamanan informasi dan perilaku *cyber* di lingkungan RSUD Limpung.

DAFTAR PUSTAKA

Algiffary, A., M. Izman Herdiansyah, & Yesi Novaria Kunang. (2023). Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI. *Journal of Applied Computer Science and Technology*, *4*(1), 19–26. https://doi.org/10.52158/jacost.v4i1.505

Ariyadi Tamsir, Fadli Hidayatul, Akbar Taufik, P. M. B. (2025). *Implementasi OWASP untuk Analisis Kerentanan dan Keamanan pada Sistem Informasi Akademik Terintegrasi Universitas Bina Darma*. *4*(1), 1–7.

Budi, A. P., Wulandari, S., & Budi, G. N. (2025). Analisis Model Hot-Fit Terhadap Kinerja Keamanan Siber Dengan Mediasi Kesiapan Keamanan Siber Di Rsud Ajibarang. *Infokes: Jurnal Ilmiah Rekam Medis Dan Informatika Kesehatan*, *15*(1), 42–49. https://doi.org/10.47701/infokes.v15i1.4392

Fatmala Putri, D., & Ratna Sari, W. (2023). Analisis Perlindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking. *Jurnal Ilmiah Ekonomi Dan Manajemen*, *1*(4), 173–181. https://doi.org/10.61722/jiem.v1i4.331

Manurung, J., Sihombing, A. P. E., & Pandiangan, B. (2023). Sosialisasi Dan Edukasi Tentang Keamanan Data Dan Privasi Di Era Digital Untuk Meningkatkan Kesadaran Dan Perlindungan Masyarakat. *Jurnal Pengabdian Masyarakat Nauli*, *2*(1), 1–7. https://ejournal.marqchainstitute.or.id/index.php/Nauli/article/view/103

Navisa Putri, M., Setiono, O., Astuti S., R., & Widianawati, E. (2024). Analysis Of The Readiness Of Medical Record Officers In The Outpatient Unit To The Use Of RME By TRI Methods At RSUD Dr. M. Ashari Pemalang. *International Journal of Health Literacy and Science*, *2*(2), 50–59. https://doi.org/10.60074/ihelis.v2i2.62

Neng Sari Rubiyanti. (2023). Penerapan Rekam Medis Elektronik di Rumah Sakit di Indonesia: Kajian Yuridis. *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora*, *1*(1), 179–187. https://doi.org/10.59246/aladalah.v1i1.163

Rachmani, E., Dewi, F., Haikal, H., & Setiono, O. (2023). Pengukuran Literasi Kesehatan Digital Kader Kesehatan Desa Penadaran Menggunakan SI-Cerdik. *Indonesian Journal of Health*

Information Management Services, *3*(1), 7–10. https://doi.org/10.33560/ijhims.v3i1.57

Sigit, K. N., & Syaqiq, M. (2021). Pengaruh Pelayanan Dan Fasilitas Terhadap Kepuasan Pasien Di RSUD Limpung Batang. *JURNAL LITBANG KOTA PEKALONGAN*, *21*, 4. https://doi.org/10.54911/litbang.v21i1.148