RSUD Sayangi Diriku	PROSEDUR PERLINDUNGAN KERAHASIAAN, KEAMANAN, DAN INTEGRITAS DATA		
	No. Dokumen 34	**No. Revisi** 00	**Halaman** -
STANDAR PROSEDUR OPERASIONAL	**Tanggal Terbit :** **26 Juli 2026**	Ditetapkan Oleh : Kepala Rumah Sakit **dr. Herlina, Sp.THT.KL. M.Kes** PNS IV B / NIP 1232313131	

PENGERTIAN	Prosedur ini mengatur tata cara perlindungan kerahasiaan, keamanan, dan integritas data pasien serta data operasional Rumah Sakit Umum Daerah (RSUD) Sayangi Diriku dari akses tidak sah, modifikasi, kerusakan, atau kehilangan. Perlindungan data mencakup data elektronik dalam Sistem Informasi Manajemen Rumah Sakit (SIMRS) dan Rekam Medis Elektronik (RME), serta data fisik.
TUJUAN	• Memastikan kerahasiaan data pasien dan data operasional RSUD Sayangi Diriku terjaga dari pihak yang tidak berwenang. • Menjamin keamanan data dari ancaman siber, kerusakan, atau kehilangan. • Memastikan integritas data, yaitu data akurat, lengkap, dan tidak dimodifikasi tanpa otorisasi. • Memenuhi kepatuhan terhadap regulasi perlindungan data pribadi dan rekam medis elektronik yang berlaku.
KEBIJAKAN	• Setiap staf RSUD Sayangi Diriku wajib mematuhi kebijakan perlindungan data pribadi pasien dan data rumah sakit. • RSUD Sayangi Diriku wajib menyelenggarakan SIMRS yang terintegrasi dengan RME sesuai PMK No. 82 Tahun 2013 dan PMK No. 24 Tahun 2022. • Perlindungan data pribadi pasien wajib dilaksanakan sesuai UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. • Setiap akses terhadap data pasien harus berdasarkan prinsip kebutuhan untuk mengetahui (need-to-know basis) dan otorisasi yang jelas. • Manajemen RS bertanggung jawab penuh atas keamanan dan kerahasiaan data yang dikelola. • Sistem Informasi Manajemen Rumah Sakit (SIMRS) wajib memiliki fitur keamanan yang memadai untuk mencegah akses tidak sah dan menjaga integritas data. • Audit log sistem informasi wajib dilakukan secara berkala untuk memantau aktivitas akses dan perubahan data. • SE Menkes No. HK.02.01/MENKES/1030/2023 tentang Kewajiban Integrasi RME ke Platform SatuSehat
REFERENSI	
PROSEDUR	1. **1. Identifikasi dan Klasifikasi Data:** a. Identifikasi seluruh jenis data yang dikelola oleh RSUD Sayangi Diriku, termasuk data pasien (identitas, rekam medis, hasil pemeriksaan), data keuangan, data SDM, dan data operasional lainnya. b. Klasifikasikan data berdasarkan tingkat sensitivitas dan kepentingannya (misalnya: Sangat Rahasia, Rahasia, Terbatas, Publik) untuk menentukan tingkat perlindungan yang diperlukan. *Sumber: UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi Pasal 4; PMK No. 24 Tahun 2022 tentang Rekam Medis Pasal 3*

2. **2. Pengelolaan Akses Data (Access Control):** a. Tentukan peran dan hak akses pengguna SIMRS dan RME secara spesifik berdasarkan jabatan dan kebutuhan kerja (role-based access control). b. Berikan setiap pengguna kredensial unik (username dan password) yang kuat dan wajib diganti secara berkala (minimal 3 bulan sekali). c. Lakukan verifikasi identitas pengguna sebelum memberikan atau mengubah hak akses. d. Nonaktifkan akun pengguna yang sudah tidak bertugas atau berganti peran yang tidak memerlukan akses data tertentu.

   Sumber: PMK No. 82 Tahun 2013 tentang SIMRS Pasal 10; PMK No. 24 Tahun 2022 tentang Rekam Medis Pasal 30; UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi Pasal 27

3. **3. Perlindungan Data Elektronik (SIMRS & RME):** a. Terapkan enkripsi data sensitif, baik saat data disimpan (data at rest) maupun saat data ditransmisikan (data in transit) antar sistem atau ke platform SatuSehat. b. Gunakan firewall, antivirus, dan sistem deteksi intrusi (IDS) yang mutakhir untuk melindungi jaringan dan server SIMRS dari serangan siber. c. Lakukan pembaruan perangkat lunak (patching) dan sistem operasi secara rutin untuk menutup celah keamanan. d. Pastikan SIMRS memiliki fitur audit log yang mencatat setiap aktivitas akses, modifikasi, dan penghapusan data, termasuk identitas pengguna, waktu, dan jenis tindakan.

   Sumber: PMK No. 82 Tahun 2013 tentang SIMRS Pasal 10; PMK No. 24 Tahun 2022 tentang Rekam Medis Pasal 30; UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi Pasal 27; SE Menkes No. HK.02.01/MENKES/1030/2023

4. **4. Perlindungan Data Fisik:** a. Simpan rekam medis fisik dan dokumen sensitif lainnya di area yang terkunci, terbatas aksesnya, dan terlindungi dari bencana (kebakaran, banjir). b. Terapkan prosedur pemusnahan dokumen fisik yang tidak terpakai atau telah melewati masa retensi sesuai regulasi, dengan metode yang tidak dapat dipulihkan (misalnya shredding). c. Batasi akses fisik ke ruang server dan fasilitas penyimpanan data lainnya hanya untuk personel yang berwenang.

   Sumber: PMK No. 24 Tahun 2022 tentang Rekam Medis Pasal 31; PMK No. 40 Tahun 2022 tentang Persyaratan Teknis Bangunan, Prasarana, dan Peralatan Kesehatan RS

5. **5. Pencadangan dan Pemulihan Data (Backup & Recovery):** a. Lakukan pencadangan data SIMRS dan RME secara berkala (harian/mingguan) ke lokasi penyimpanan yang terpisah dan aman. b. Uji coba prosedur pemulihan data (data recovery) secara rutin untuk memastikan data dapat dikembalikan dengan cepat dan utuh jika terjadi insiden kehilangan data. c. Simpan salinan cadangan data di lokasi off-site yang aman untuk perlindungan terhadap bencana lokal.

   Sumber: PMK No. 82 Tahun 2013 tentang SIMRS Pasal 10; PMK No. 24 Tahun 2022 tentang Rekam Medis Pasal 30

6. **6. Penanganan Insiden Keamanan Data:** a. Bentuk tim respons insiden keamanan data yang bertugas untuk menanggapi, menyelidiki, dan memulihkan dari insiden keamanan data. b. Laporkan setiap insiden keamanan data (misalnya: kebocoran data, akses tidak sah, serangan siber) kepada tim IT/SIMRS dan manajemen RS segera setelah terdeteksi. c. Lakukan investigasi menyeluruh terhadap insiden untuk mengidentifikasi akar masalah dan mencegah terulangnya insiden serupa. d. Berikan informasi kepada pihak yang terdampak (pasien) jika terjadi kebocoran data pribadi yang berisiko tinggi, sesuai ketentuan UU PDP.

   Sumber: UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi Pasal 46; PMK No. 11 Tahun 2017 tentang Keselamatan Pasien

7. **7. Edukasi dan Pelatihan Staf:** a. Selenggarakan pelatihan rutin bagi seluruh staf mengenai pentingnya perlindungan data, kebijakan keamanan informasi, dan praktik terbaik dalam menjaga kerahasiaan data. b. Sosialisasikan secara berkala mengenai ancaman keamanan data terbaru dan cara menghindarinya (misalnya: phishing, rekayasa sosial). c. Pastikan setiap staf menandatangani perjanjian kerahasiaan data sebagai bagian dari kontrak kerja.

   Sumber: UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi Pasal 58; KMK No. HK.01.07/MENKES/1596/2024 (STARKES 2024) Bab PMKP

<table>
<tr><td rowspan="2">RSUD Sayangi Diriku</td><td colspan="3">PROSEDUR PERLINDUNGAN KERAHASIAAN, KEAMANAN, DAN INTEGRITAS DATA</td></tr>
<tr><td>No. Dokumen
34</td><td>No. Revisi
00</td><td>Halaman
-</td></tr>
<tr><td></td><td colspan="3">8. **8. Audit dan Evaluasi:** a. Lakukan audit keamanan informasi secara berkala (minimal setahun sekali) oleh pihak internal atau eksternal yang independen untuk menilai efektivitas kontrol keamanan data. b. Evaluasi dan perbarui kebijakan serta prosedur perlindungan data secara rutin (minimal setiap 2-3 tahun) atau jika ada perubahan regulasi dan teknologi. c. Gunakan hasil audit dan evaluasi untuk perbaikan berkelanjutan dalam sistem perlindungan data.
Sumber: PMK No. 82 Tahun 2013 tentang SIMRS Pasal 10; KMK No. HK.01.07/MENKES/1596/2024 (STARKES 2024) Bab PMKP</td></tr>
<tr><td>UNIT TERKAIT</td><td colspan="3">• Unit Rekam Medis
• Unit Teknologi Informasi (IT) / SIMRS
• Seluruh Unit Pelayanan Klinis (Rawat Jalan, Rawat Inap, IGD, ICU, Kamar Operasi, Laboratorium, Radiologi, Farmasi)
• Manajemen Rumah Sakit
• Komite Mutu dan Keselamatan Pasien
• Komite Medik
• Komite Keperawatan</td></tr>
</table>