

BUNGA RAMPAI



KEAMANAN DAN PRIVASI DATA KESEHATAN

Editor:
Leni Halimatusyadiah

BUNGA RAMPAI KEAMANAN DAN PRIVASI DATA KESEHATAN

Penulis:

**Ali Impron; Jenita Frisilia; R.A. Granita R. Layungasri;
Andra Dwitama Hidayat; Indah Susilowati;
Anggia Dini M. Panggabean;
Novian Adhipurna**

Editor:

Leni Halimatusyadiah



PT. Mustika Sri Rosadi

Bunga Rampai Keamanan Dan Privasi Data Kesehatan

Penulis:

Ali Impron; Jenita Frisilia; R.A. Granita R. Layungasri;
Andra Dwitama Hidayat; Indah Susilowati; Anggia Dini M.
Panggabean; Novian Adhipurna

Editor: Leni Halimatusyadiah

Layout: Tim PT. Mustika Sri Rosadi

Desain Sampul: Febriansyah

ISBN: 978-634-7535-38-2 (PDF)

Cetakan Pertama: 1 Desember 2025

Hak Cipta 2025

Hak Cipta Dilindungi Oleh Undang-Undang

Dilarang memperbanyak karya tulis ini dalam bentuk dan
dengan cara apapun tanpa izin tertulis dari penerbit.

Diterbitkan oleh Penerbit PT Mustika Sri Rosadi

Alamat Penerbit: Citra Indah City, Bukit Heliconia AG
23/32, Kecamatan Jonggol, Kab. Bogor.

Email: mars.mustikasrirosadi@gmail.com

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa atas terselesaikannya buku *Bunga Rampai Keamanan dan Privasi Data Kesehatan* ini. Buku ini hadir sebagai respon terhadap pesatnya perkembangan digitalisasi layanan kesehatan yang membawa manfaat besar sekaligus tantangan serius dalam perlindungan data kesehatan. Di era ketika rekam medis elektronik, telemedisin, big data, dan teknologi berbasis IoT semakin luas digunakan, pemahaman mengenai keamanan dan privasi data menjadi kebutuhan mendesak bagi seluruh pemangku kepentingan.

Setiap bab dalam buku ini disusun untuk memberikan wawasan komprehensif mengenai konsep, ancaman, regulasi, teknologi, serta strategi mitigasi dalam menjaga keamanan informasi kesehatan. Para penulis menyajikan kajian ilmiah yang relevan, mulai dari dasar-dasar keamanan data, enkripsi, serangan siber, hingga kebijakan dan tata kelola yang diperlukan untuk membangun sistem kesehatan digital yang aman dan terpercaya.

Penyusunan buku ini tidak terlepas dari kontribusi para akademisi, praktisi kesehatan, dan peneliti yang telah menyumbangkan ilmu, pengalaman, dan pemikiran. Semoga kehadiran bunga rampai ini dapat

menjadi rujukan yang bermanfaat bagi mahasiswa, tenaga kesehatan, pengelola fasilitas kesehatan, peneliti, serta pembuat kebijakan dalam memperkuat perlindungan data kesehatan di Indonesia.

Akhir kata, semoga buku ini dapat memberikan manfaat, memperluas wawasan, dan mendorong terwujudnya ekosistem kesehatan digital yang lebih aman, berkualitas, dan berorientasi pada perlindungan hak privasi pasien.

Bogor, 1 Desember 2025

Penulis

DAFTAR ISI

KATA PENGANTAR.....	2
DAFTAR ISI.....	4
DAFTAR TABEL.....	8
DAFTAR GAMBAR.....	9
PENDAHULUAN - Leni Halimatusyadiah	10
A. Pendahuluan.....	10
B. Metode Penulisan.....	11
C. Outline Bunga Rampai.....	12
BAB 1. KONSEP KEAMANAN DAN PRIVASI DALAM DATA KESEHATAN - Ali Impron	14
A. Pengertian Keamanan dan Privasi dalam Data Kesehatan	14
B. Prinsip Dasar Keamanan dan Privasi Data Kesehatan	21
C. Dampak dan Tantangan Keamanan dan Privasi Data Kesehatan	28
D. Strategi Pengelolaan Keamanan dan Privasi Data Kesehatan	36
E. Daftar Pustaka.....	44
BAB 2. JENIS ANCAMAN TERHADAP DATA KESEHATAN - Jenita Frisilia	48
A. Pendahuluan.....	48
B. Karakteristik Data Kesehatan	49
C. Jenis Ancaman Terhadap Data Kesehatan	50
D. Dampak Ancaman terhadap Sistem Kesehatan	57
E. Strategi Mitigasi Ancaman.....	59
F. Studi Kasus di Indonesia.....	63
G. Penutup	64

H. Daftar Pustaka.....	65
BAB 3. REGULASI DAN STANDARDISASI KEAMANAN DATA KESEHATAN - R.A. Granita Ramadhani Layungasri	68
A. Pendahuluan.....	68
B. Pengertian Keamanan Data Kesehatan	71
C. Regulasi Keamanan Data Kesehatan: Analisis Mendalam.....	85
D. Standardisasi Keamanan Data Kesehatan: Analisis Mendalam.....	98
E. Analisis Komparatif Dan Tantangan Implementasi	108
F. Kesimpulan dan Rekomendasi	117
G. Daftar Pustaka.....	118
BAB 4. TEKNOLOGI ENKRIPSI DALAM MELINDUNGI DATA KESEHATAN - Andra Dwitama Hidayat	122
A. Pendahuluan.....	122
B. Konsep Dasar Enkripsi	123
C. Enkripsi Simetris (<i>Symmetric Encryption</i>)	125
D. Enkripsi Asimetris (<i>Asymmetric Encryption</i>).....	129
E. Penerapan Enkripsi dalam Sistem Informasi Kesehatan	134
F. Penerapan Enkripsi pada Sistem Kesehatan Digital	136
G. Penutup	138
H. Daftar Pustaka.....	138
BAB 5. KEAMANAN DATA DALAM REKAM MEDIS ELEKTRONIK - Indah Susilowati	142
A. Pendahuluan.....	142
B. Pengertian Rekam Medis Elektronik.....	144

C. Pentingnya Keamanan Data dalam Rekam Medis Elektronik	144
D. Landasan Hukum	145
E. Tujuan dan Fungsi Rekam Medis Elektronik Dalam Pelayanan Kesehatan Modern.....	148
F. Prinsip-Prinsip Keamanan Data Rekam Medis Elektronik	151
G. Tantangan Tata Kelola Keamanan dan Pengembangan Data Rekam Medis Elektronik..	152
H. Prospek Pengembangan Rekam Medis Elektronik	154
I. Penutup	155
J. Daftar Pustaka.....	156
BAB 6. SISTEM AUTENTIKASI DAN KONTROL AKSES DALAM DATA KESEHATAN - Anggia Dini Marsaroha	
Panggabeaen	160
A. Pendahuluan.....	160
B. Autentikasi dalam Sistem Informasi Kesehatan .	162
C. Kontrol Akses dalam Data Kesehatan	165
D. Peran Autentikasi dan Kontrol Akses dalam Keamanan Data Kesehatan.....	167
E. Daftar Pustaka.....	168
BAB 7. TANGGUNG JAWAB ETIS DALAM PENGELOLAAN DATA KESEHATAN - R.A. Granita Ramadhani Layungasri	
.....	170
A. Pendahuluan.....	170
B. Konsep Dasar: Etika, Kepatuhan, dan Pengelolaan Data Kesehatan.....	171
C. Penerapan Etika dan Kepatuhan dalam Pengelolaan Data Kesehatan.....	189

D. Analisis Mendalam Tanggung Jawab Etis Berdasarkan Kerangka Regulasi dan Standar	206
E. Kesimpulan.....	223
F. Daftar Pustaka.....	226
BAB 8. PENGARUH KEBOCORAN DATA TERHADAP KEPERCAYAAN PUBLIK - Novian Adhipurna	229
A. Pendahuluan.....	229
B. Konsep Dasar dan Landasan Teoritis.....	234
C. Kebocoran Data Kesehatan di Era Digital.....	242
D. Pengaruh Kebocoran Data terhadap Kepercayaan Publik.....	251
E. Strategi Pemulihan dan Penguatan Kepercayaan Publik Pasca-Kebocoran Data	255
F. Kesimpulan dan Rekomendasi	257
G. Penutup	261
H. Daftar Pustaka.....	262
PENUTUP - Leni Halimatusyadiah	265
GLOSARIUM.....	269
BIOGRAFI EDITOR.....	274
BIOGRAFI PENULIS	276
SINOPSIS	290

DAFTAR TABEL

Tabel 1. Jenis Data Kesehatan	72
Tabel 2. Prinsip Perlindungan Data	89
Tabel 3. Perbandingan Metode Enkripsi AES dan DES	129
Tabel 4. Perbandingan Metode Enkripsi RSA dan ECC	133

DAFTAR GAMBAR

Gambar 1. Persyaratan dan Kepatuhan Peraturan.....	16
Gambar 2. HIPAA dan GDPR.....	27
Gambar 3. Pasien khawatir terhadap keamanan data	30
Gambar 4. Autentikasi Multi-faktor (MFA)	40
Gambar 5. <i>CIA Triad Triangle</i>	73
Gambar 6. <i>Cyberattacks</i>	77
Gambar 7. <i>HIPAA</i>	86
Gambar 8. <i>Data Protection Officer</i>	95
Gambar 9. <i>Cybersecurity in Healthcare</i>	107
Gambar 10. <i>Virtual Discussion on Patient's Medical Condition</i>	172
Gambar 11. <i>Pillars of Medical Ethics</i>	175
Gambar 12. <i>GDPR</i>	183
Gambar 13. <i>Digital Data Audit</i>	185
Gambar 14. <i>Informed Consent</i>	190
Gambar 15. <i>Simulation of Data Transfer</i>	195
Gambar 16. <i>Doctor in Hospital</i>	201
Gambar 17. <i>Telemedicine</i>	220

PENDAHULUAN

Oleh: Leni Halimatusyadiah

A. Pendahuluan

Perkembangan digitalisasi layanan kesehatan dalam satu dekade terakhir telah mengubah secara signifikan cara data medis dikumpulkan, disimpan, dan diolah. Pemanfaatan rekam medis elektronik, sistem informasi rumah sakit, telemedisin, aplikasi kesehatan, hingga perangkat Internet of Things (IoT) meningkatkan efisiensi pelayanan sekaligus membuka akses data yang jauh lebih luas. Namun, perubahan ini turut menghadirkan tantangan serius terkait keamanan dan privasi data kesehatan.

Data kesehatan merupakan jenis data pribadi yang sangat sensitif karena mengandung informasi mengenai kondisi fisik, mental, riwayat pengobatan, hasil pemeriksaan, hingga data biometrik. Kebocoran atau penyalahgunaan data kesehatan dapat berdampak luas, tidak hanya pada aspek medis maupun keselamatan pasien, tetapi juga menyebabkan kerugian sosial, psikologis, dan ekonomi. Di Indonesia, beberapa insiden kebocoran data berskala besar dalam beberapa tahun terakhir menunjukkan bahwa sistem keamanan informasi kesehatan masih menghadapi risiko yang signifikan.

Ancaman terhadap data kesehatan bersifat multidimensi. Selain serangan teknis seperti malware,

ransomware, phishing, dan peretasan, terdapat pula ancaman dari faktor manusia, lemahnya tata kelola internal, ketidakpatuhan terhadap regulasi, serta kerentanan perangkat dan infrastruktur digital. Kondisi ini menegaskan perlunya penguatan sistem keamanan informasi yang mencakup aspek teknis, organisasi, perilaku pengguna, serta kerangka hukum yang jelas.

Bunga rampai ini disusun untuk memberikan pemahaman menyeluruh mengenai konsep keamanan dan privasi data kesehatan, jenis ancaman yang dihadapi, teknologi yang digunakan untuk perlindungan data, regulasi yang berlaku, serta strategi mitigasi yang dapat diterapkan oleh institusi kesehatan. Dengan pendekatan multidisipliner, buku ini bertujuan memperkuat literasi keamanan siber di sektor kesehatan dan mendukung pengembangan ekosistem digital yang aman, terpercaya, dan berorientasi pada keselamatan serta hak privasi pasien.

B. Metode Penulisan

Penyusunan bunga rampai ini dilakukan melalui metode studi literatur (library research) dengan pendekatan kualitatif. Sumber data diperoleh dari buku teks, artikel ilmiah terindeks nasional dan internasional, laporan teknis terkait keamanan

informasi, pedoman resmi dari lembaga pemerintah seperti Kementerian Kesehatan dan Kementerian Komunikasi dan Informatika, serta dokumen regulasi dan standar keamanan informasi seperti UU PDP, HIPAA, GDPR, dan ISO/IEC 27001.

Pemilihan literatur mengutamakan publikasi paling relevan dalam kurun waktu sepuluh tahun terakhir untuk memastikan akurasi dan aktualitas informasi. Analisis dilakukan melalui identifikasi isu utama, kategorisasi topik, serta sintesis naratif untuk menghasilkan alur pembahasan yang sistematis dan terstruktur. Pendekatan penulisan bersifat deskriptif-analitis, menghubungkan konsep teoritis dengan tantangan implementatif yang terjadi di fasilitas pelayanan kesehatan.

C. Outline Bunga Rampai

BAB 1. Pendahuluan

Terdiri dari tiga subbagian utama yang menjelaskan latar belakang ilmiah, pendekatan penulisan, dan gambaran isi buku secara menyeluruh

BAB 2. Konsep Keamanan dan Privasi Data Kesehatan

Membahas definisi, prinsip dasar keamanan informasi, perbedaan keamanan dan privasi, serta urgensi perlindungan data kesehatan.

BAB 3. Jenis Ancaman terhadap Data Kesehatan

Menguraikan ancaman teknis, ancaman internal, ancaman fisik, ancaman regulasi, serta ancaman dari pihak ketiga, lengkap dengan studi kasus.

BAB 4. Regulasi dan Standardisasi Keamanan Data Kesehatan

Menganalisis kerangka hukum nasional dan internasional, seperti HIPAA, GDPR, UU PDP, Permenkes, serta standar ISO.

BAB 5. Teknologi Enkripsi dalam Perlindungan Data Kesehatan

Membahas enkripsi simetris dan asimetris, penerapannya pada sistem informasi kesehatan, serta peran teknologi dalam menjaga kerahasiaan data.

BAB 6–9. Kajian Ancaman dan Mitigasi Lanjutan

Meliputi berbagai pembahasan terkait ancaman berulang, dampak sistemik, dan strategi mitigasi multilapis pada sektor kesehatan digital.

BAB 10. Penutup

Merangkum keseluruhan pembahasan serta menegaskan kembali pentingnya sinergi aspek teknis, organisasi, regulasi, dan perilaku manusia dalam melindungi data kesehatan.

BAB 1. KONSEP KEAMANAN DAN PRIVASI DALAM DATA KESEHATAN

Oleh: Ali Impron

A. Pengertian Keamanan dan Privasi dalam Data Kesehatan

Keamanan dan privasi dalam data kesehatan adalah dua aspek fundamental yang harus dijaga dengan sangat hati-hati oleh berbagai lembaga kesehatan, baik rumah sakit, klinik, maupun penyedia layanan medis lainnya. Kedua konsep ini, meskipun saling terkait, memiliki peran yang berbeda dalam melindungi informasi medis yang sensitif.

1. Keamanan Data Kesehatan

Keamanan data kesehatan merujuk pada langkah-langkah yang diambil untuk melindungi data dari ancaman yang dapat merusak integritas, kerahasiaan, dan ketersediaannya (Shah, 2015; Pandey et al., 2021). Dalam konteks ini, ancaman bisa berupa upaya akses tidak sah, pengubahan informasi yang tidak diinginkan, atau penghancuran data yang dapat mengakibatkan kerugian serius, baik bagi pasien maupun institusi yang menangani data tersebut. Keamanan data ini melibatkan penggunaan teknologi seperti enkripsi, proteksi jaringan, dan autentikasi yang kuat untuk

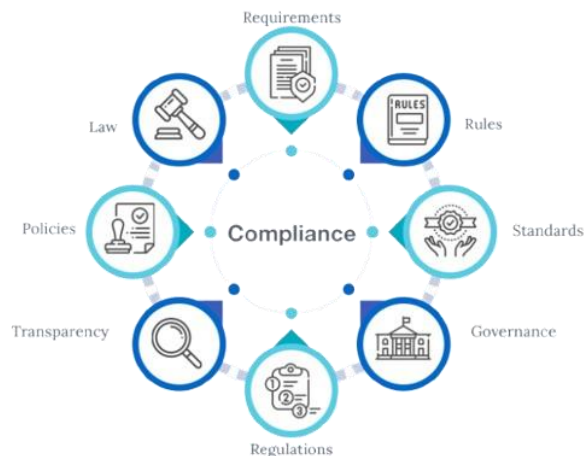
memastikan data tetap terlindungi dari potensi kerusakan.

Pada level teknis, keamanan data kesehatan mencakup beberapa elemen penting, antara lain:

- a. Keamanan Jaringan: Perlindungan terhadap data yang dipindahkan melalui jaringan komputer, baik lokal maupun internet, dari potensi penyadapan atau perusakan. Hal ini bisa dilakukan dengan penggunaan protokol enkripsi dan firewall yang kuat (Kailar and Muralidhar, 2007; Mohammed and Alheeti, 2022).
- b. Autentikasi dan Akses: Mekanisme untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses data sensitif. Ini bisa mencakup penggunaan kata sandi yang kuat, sistem autentikasi multi-faktor, dan kontrol akses berbasis peran (role-based access control) (Asija and Nallusamy, 2018; Singh and Chatterjee, 2019).
- c. Penyimpanan yang Aman: Data kesehatan harus disimpan dengan cara yang aman, baik itu dalam bentuk fisik (misalnya, di hard disk yang terenkripsi) maupun digital (melalui cloud storage yang memiliki sistem perlindungan tinggi) (Heurix, Karlinger and Neubauer, 2012; Ashok and Gopikrishnan, 2024).

d. Pemulihan Data: Implementasi kebijakan pemulihan data untuk memastikan data dapat dipulihkan dalam keadaan darurat seperti kegagalan sistem atau serangan siber, yang juga merupakan aspek dari manajemen risiko dalam keamanan data kesehatan (Brack, 2010; Goldberg, 2010, 2013).

Keamanan data kesehatan juga berkaitan erat dengan upaya untuk menghindari kebocoran informasi pribadi yang dapat merugikan pasien, baik secara finansial, sosial, atau emosional. Menurut studi (Al Kinoon et al., 2021), data kesehatan yang terkompromikan dapat menyebabkan kerusakan jangka panjang pada reputasi dan keberlanjutan institusi medis.



Gambar 1. Persyaratan dan Kepatuhan Peraturan

2. Privasi Data Kesehatan

Privasi data kesehatan berfokus pada hak individu untuk mengontrol siapa yang dapat mengakses dan mengungkapkan informasi medis mereka. Privasi mengatur tentang seberapa jauh data kesehatan pribadi boleh digunakan atau dibagikan kepada pihak ketiga dan di bawah kondisi apa informasi tersebut dapat diungkapkan. Tidak seperti keamanan, yang lebih fokus pada upaya teknis untuk melindungi data, privasi lebih menekankan pada aspek hukum dan etis dari pengelolaan informasi pribadi.

Terdapat beberapa prinsip dasar dalam privasi data kesehatan, antara lain:

1. Hak untuk Mengetahui dan Setuju: Pasien harus diberi informasi yang jelas mengenai siapa saja yang dapat mengakses data mereka, untuk tujuan apa data tersebut digunakan, dan bagaimana data mereka dilindungi. Ini mencakup hak untuk memberikan persetujuan eksplisit (informed consent) sebelum data medis mereka digunakan atau dibagikan.
2. Penggunaan Data untuk Tujuan Terbatas: Data kesehatan harus hanya digunakan untuk tujuan yang telah disetujui oleh pasien. Sebagai contoh, jika data pasien digunakan untuk penelitian medis, maka penggunaan tersebut harus sesuai

dengan persetujuan awal yang diberikan oleh pasien.

3. Hak untuk Menghapus Data: Pasien harus memiliki hak untuk meminta penghapusan data pribadi mereka setelah tidak lagi diperlukan, sesuai dengan prinsip yang diatur dalam regulasi seperti GDPR di Uni Eropa. Ini memberi pasien kendali penuh atas informasi mereka dan melindungi mereka dari penyalahgunaan data di masa depan.
4. Pengungkapan yang Minimal: Konsep privasi mengharuskan bahwa hanya informasi yang benar-benar diperlukan yang boleh diungkapkan. Sebagai contoh, jika seseorang mengakses data kesehatan untuk tujuan tertentu, mereka hanya boleh melihat informasi yang relevan dengan tujuan tersebut dan bukan seluruh riwayat medis pasien.

Penegakan privasi data kesehatan sering kali membutuhkan kepatuhan terhadap regulasi yang ketat, seperti HIPAA di Amerika Serikat dan GDPR di Eropa, yang mengatur secara rinci bagaimana data medis harus dikelola dan dibagikan. Pelanggaran terhadap privasi data kesehatan dapat mengarah pada sanksi hukum yang serius, serta hilangnya kepercayaan dari pasien.

3. Hubungan Keamanan dan Privasi dalam Data Kesehatan

Keamanan dan privasi dalam data kesehatan saling melengkapi namun memiliki fokus yang berbeda. Keamanan lebih berfokus pada perlindungan fisik dan teknis terhadap data, sedangkan privasi lebih menekankan pada hak pasien untuk mengontrol dan mengetahui bagaimana data mereka digunakan. Meskipun keduanya memiliki peran yang sangat penting, tanpa privasi yang memadai, upaya untuk mengamankan data bisa menjadi sia-sia. Sebaliknya, tanpa keamanan yang cukup, perlindungan terhadap privasi data tidak akan maksimal.

Dalam praktiknya, banyak lembaga kesehatan yang mengadopsi pendekatan berbasis kebijakan untuk memastikan kedua aspek ini dapat dijaga dengan baik. Misalnya, pengelolaan akses data secara ketat untuk memastikan bahwa hanya staf medis yang membutuhkan informasi tertentu yang dapat mengaksesnya, sekaligus memberikan transparansi penuh kepada pasien mengenai siapa saja yang memiliki akses tersebut.

4. Studi Kasus dan Tren Terkini

Salah satu contoh nyata yang menunjukkan pentingnya keamanan dan privasi data kesehatan adalah peristiwa kebocoran data yang terjadi pada beberapa rumah sakit besar di seluruh dunia, di mana serangan siber seperti ransomware menyebabkan kebocoran informasi pribadi pasien yang sangat sensitif. Sebagai respons terhadap hal ini, banyak organisasi kesehatan kini mulai menerapkan enkripsi end-to-end dan sistem deteksi intrusi berbasis AI untuk memperkuat pertahanan mereka terhadap ancaman luar.

Menurut laporan (Thenmozhi et al., 2024), penerapan teknologi seperti enkripsi dan autentikasi multi-faktor secara signifikan dapat mengurangi risiko kebocoran data, sekaligus meningkatkan kepercayaan pasien terhadap sistem yang mengelola informasi medis mereka.

Dengan demikian, pemahaman yang mendalam tentang pengertian dasar dari keamanan dan privasi dalam data kesehatan menjadi langkah awal yang penting dalam upaya melindungi data yang sangat berharga ini. Bab selanjutnya akan membahas lebih jauh mengenai berbagai jenis ancaman yang dapat mengancam keamanan data kesehatan serta cara-cara untuk menghadapinya.

B. Prinsip Dasar Keamanan dan Privasi Data Kesehatan

Keamanan dan privasi data kesehatan tidak hanya bergantung pada teknologi dan kebijakan teknis, tetapi juga pada prinsip-prinsip dasar yang membentuk kerangka kerja untuk menjaga dan mengelola data medis dengan cara yang aman dan etis. Dalam konteks ini, ada beberapa prinsip utama yang harus dipahami dan diterapkan oleh lembaga kesehatan dan profesional medis dalam melindungi data pasien. Prinsip-prinsip ini sering kali tercermin dalam regulasi dan standar yang mengatur penggunaan data kesehatan, serta dalam praktik sehari-hari untuk menjaga integritas dan kerahasiaan data.

1. Prinsip Kerahasiaan (*Confidentiality*)

Prinsip kerahasiaan adalah dasar dari privasi data kesehatan. Data medis yang dimiliki oleh pasien merupakan informasi pribadi yang sangat sensitif dan harus dilindungi dari pengungkapan yang tidak sah. Prinsip kerahasiaan menegaskan bahwa hanya individu atau pihak yang memiliki izin atau hak yang sah yang boleh mengakses informasi medis pasien. Ini termasuk profesional medis yang terlibat dalam pengobatan, serta pihak lain yang diberikan izin secara eksplisit oleh pasien.

Di dalam sistem digital, prinsip kerahasiaan dapat ditegakkan melalui berbagai mekanisme, antara lain:

- a. Enkripsi: Menggunakan algoritma enkripsi yang kuat untuk melindungi data selama transmisi dan penyimpanan.
- b. Kontrol Akses: Menggunakan kebijakan kontrol akses berbasis peran (role-based access control/RBAC) untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses data sensitif.
- c. Pengawasan Akses: Memantau dan merekam akses ke data medis untuk mendeteksi upaya penyalahgunaan atau akses yang tidak sah.

2. Prinsip Integritas (*Integrity*)

Prinsip integritas mengacu pada perlindungan terhadap data agar tidak dimodifikasi secara tidak sah atau tanpa otorisasi. Dalam konteks data kesehatan, integritas sangat penting, karena setiap perubahan atau modifikasi yang tidak sah terhadap rekam medis pasien bisa berisiko pada kesalahan diagnosis, pengobatan yang tidak tepat, atau bahkan bencana medis.

Untuk memastikan integritas data, beberapa langkah yang dapat diambil meliputi:

- a. Pencatatan Jejak (Audit Trails): Sistem yang mencatat setiap perubahan yang terjadi pada

data, termasuk siapa yang membuat perubahan dan kapan perubahan tersebut dilakukan.

- b. Checksum dan Hashing: Penggunaan teknik enkripsi seperti checksum dan hashing untuk memverifikasi bahwa data yang diterima tidak mengalami perubahan sejak terakhir kali disimpan atau dikirimkan.
- c. Pencegahan Malware: Menerapkan proteksi terhadap perangkat dari serangan malware yang dapat mengubah atau merusak data yang ada.

Kegagalan untuk menjaga integritas data bisa mengarah pada dampak yang sangat besar, baik bagi pasien maupun bagi institusi medis. Sebagai contoh, rekam medis yang dimanipulasi atau hilang dapat menyebabkan kesalahan dalam penanganan medis, yang mungkin berakibat fatal.

3. Prinsip Ketersediaan (*Availability*)

Ketersediaan data adalah prinsip yang memastikan bahwa data kesehatan dapat diakses dengan cepat dan mudah oleh pihak yang berwenang, terutama dalam keadaan darurat medis. Ketersediaan data penting untuk memastikan bahwa layanan kesehatan dapat diberikan secara efektif dan efisien, terutama ketika keputusan medis yang cepat dan akurat sangat diperlukan.

Untuk menjaga ketersediaan data, beberapa langkah teknis yang diterapkan di antaranya:

- a. Cadangan Data (Backup): Mengimplementasikan kebijakan pencadangan data secara teratur, sehingga data tetap dapat dipulihkan jika terjadi kerusakan sistem atau serangan ransomware.
- b. Redundansi: Menyediakan sistem redundansi, seperti server cadangan, untuk memastikan bahwa data tetap tersedia meskipun terjadi kegagalan pada sistem utama.
- c. Proteksi Terhadap Serangan *Denial of Service* (DoS): Melakukan perlindungan terhadap potensi serangan DDoS (*Distributed Denial of Service*) yang dapat mengganggu ketersediaan data atau layanan sistem kesehatan.

Penting untuk dicatat bahwa meskipun ketersediaan data sangat krusial, itu harus dijaga seiring dengan kerahasiaan dan integritas. Data yang mudah diakses tetapi tidak aman akan meningkatkan potensi risiko kebocoran informasi atau penyalahgunaan data.

4. Prinsip Minimasi Penggunaan (*Data Minimization*)

Prinsip ini berfokus pada penggunaan data yang paling sedikit dan relevan yang diperlukan untuk tujuan tertentu. Dalam banyak kasus, informasi medis pasien dapat sangat terperinci, tetapi hanya

sebagian dari informasi tersebut yang benar-benar diperlukan untuk tujuan diagnosis atau perawatan.

Beberapa langkah yang dapat diambil untuk menerapkan prinsip minimasi penggunaan termasuk:

- a. Penggunaan Data Secara Tertarget: Membatasi akses ke data hanya pada bagian-bagian yang relevan dengan kebutuhan medis pasien, sehingga tidak ada informasi yang tidak perlu yang dibagikan.
- b. Penghapusan Data yang Tidak Diperlukan: Menghapus atau mengarsipkan data yang tidak lagi diperlukan untuk tujuan medis tertentu sesuai dengan ketentuan yang berlaku.

Penerapan prinsip ini tidak hanya mengurangi potensi risiko terkait dengan penyalahgunaan data, tetapi juga mendukung prinsip privasi pasien dengan membatasi penggunaan informasi medis hanya pada kebutuhan yang sah dan terdefinisi dengan jelas.

5. Prinsip Akuntabilitas dan Transparansi (*Accountability and Transparency*)

Prinsip akuntabilitas dan transparansi mengharuskan lembaga kesehatan untuk bertanggung jawab dalam pengelolaan data medis dan memberi tahu pasien mengenai bagaimana data mereka akan digunakan dan dilindungi. Hal ini

penting untuk membangun kepercayaan antara pasien dan penyedia layanan kesehatan. Lembaga kesehatan harus:

- a. Memberikan Informasi yang Jelas: Menyediakan kebijakan privasi yang jelas dan mudah dipahami yang menjelaskan bagaimana data pasien akan digunakan, siapa yang memiliki akses, dan bagaimana data akan dilindungi.
- b. Mendokumentasikan Keputusan dan Tindakan: Semua keputusan terkait dengan pengelolaan data kesehatan harus terdokumentasi dengan jelas, dan institusi harus dapat menunjukkan bagaimana kebijakan dan prosedur diikuti jika diperlukan.

Keberadaan kebijakan yang transparan dan akuntabel ini tidak hanya melindungi pasien, tetapi juga melindungi organisasi dari risiko hukum dan reputasi yang mungkin timbul akibat pelanggaran privasi atau keamanan data.

6. Prinsip Kepatuhan terhadap Regulasi (*Compliance with Regulations*)

Di tingkat global, terdapat berbagai regulasi yang mengatur pengelolaan data kesehatan. Beberapa yang paling terkenal adalah HIPAA (Health Insurance Portability and Accountability Act) di Amerika Serikat dan GDPR (General Data Protection Regulation) di Uni Eropa. Kepatuhan terhadap regulasi-regulasi ini

sangat penting dalam memastikan bahwa data pasien dikelola dengan cara yang sah dan sesuai dengan standar hukum yang berlaku.

Kepatuhan melibatkan penerapan langkah-langkah keamanan yang sesuai, memberikan pelatihan kepada staf mengenai pentingnya privasi dan keamanan data, serta mengadakan audit berkala untuk memastikan bahwa kebijakan dan prosedur yang ditetapkan diikuti dengan benar.

	 HIPAA (current)	 GDPR
Health data in scope	Individually identifiable health information (IIHI), relating to individual health (physical or mental), provision of care or payment for provision of care, <u>when that IIHI is held or transmitted by a covered entity or its business associate</u>	"Personal data" which includes direct or indirect identifiers and "expresses the physical, physiological, genetic, mental, commercial, cultural or social identity" individuals. Health data is a special category with heightened protection.
Regulated entities	<i>Covered entities (CEs)</i> – Health plans, health care providers and health care clearinghouses <i>Business associates</i> – person or organization performing functions on behalf of (or providing services to) a CE	<i>Controller</i> – Any person or organization which determines the purposes or means of processing personal data <i>Processor</i> – person or organization processing data on behalf of controller
Permitted uses of personal health data	Health care treatment, payment and operations	Treatment, public health, research, judicial proceedings, substantial public interest, by informed consent, or when processing is in the "vital interests" of person unable to consent
Security standards	✓	✓
Breach notification requirements	✓	✓
Individual right to: Access Amend Delete	✓ ✓ ✗	✓ ✓ ✓

Gambar 2. HIPAA dan GDPR (sumber: itirra.com)

Prinsip dasar dari keamanan dan privasi data kesehatan adalah fondasi yang harus dijaga dan ditegakkan oleh semua pihak yang terlibat dalam pengelolaan data medis. Penerapan prinsip-prinsip ini

tidak hanya memastikan bahwa data pasien tetap terlindungi, tetapi juga membangun kepercayaan antara pasien dan penyedia layanan kesehatan, yang pada gilirannya mendukung efektivitas dan kualitas layanan medis secara keseluruhan. Dalam bab selanjutnya, kita akan mengeksplorasi jenis-jenis ancaman yang dapat mengancam keamanan data kesehatan dan bagaimana cara untuk menghadapinya.

C. Dampak dan Tantangan Keamanan dan Privasi Data Kesehatan

Keamanan dan privasi data kesehatan menjadi semakin penting di era digital saat ini. Dengan semakin banyaknya data yang dihasilkan melalui penggunaan teknologi informasi dalam sektor kesehatan, ancaman terhadap data tersebut juga semakin berkembang. Dari serangan siber yang mengancam sistem kesehatan hingga tantangan hukum dan etika yang harus dihadapi oleh penyedia layanan kesehatan, dampak dari pelanggaran terhadap keamanan dan privasi data kesehatan sangatlah besar. Dalam sub bab ini, kita akan membahas beberapa dampak utama yang ditimbulkan dari ancaman terhadap keamanan dan privasi data kesehatan, serta tantangan-tantangan

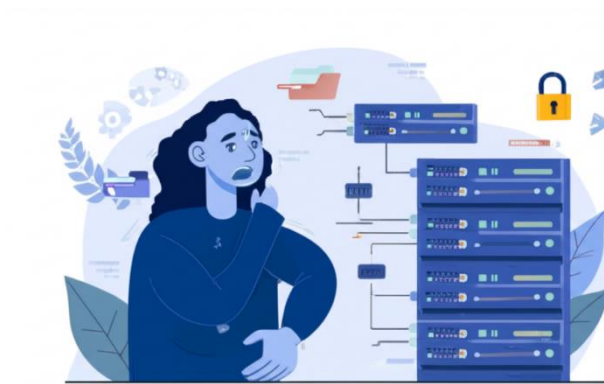
yang dihadapi oleh institusi kesehatan dalam melindungi data sensitif ini.

1. Dampak Terhadap Pasien

Salah satu dampak yang paling merugikan dari pelanggaran keamanan dan privasi data kesehatan adalah terhadap pasien itu sendiri. Data medis yang bocor atau disalahgunakan bisa mempengaruhi kehidupan pribadi, emosional, dan profesional pasien dalam berbagai cara. Beberapa dampak yang dapat timbul antara lain:

- a. Kehilangan Kepercayaan: Jika data kesehatan pasien bocor atau disalahgunakan, pasien dapat kehilangan kepercayaan pada penyedia layanan kesehatan. Ini dapat mengarah pada penurunan jumlah pasien yang bersedia berbagi informasi medis mereka secara jujur dan terbuka, yang tentunya dapat memengaruhi kualitas layanan kesehatan yang diberikan.
- b. Penyalahgunaan Identitas dan Penipuan: Informasi medis yang bocor, seperti nomor jaminan sosial, tanggal lahir, atau data kesehatan lainnya, bisa digunakan oleh pihak yang tidak bertanggung jawab untuk melakukan pencurian identitas atau penipuan. Hal ini dapat berakibat fatal bagi pasien, baik secara finansial maupun psikologis.

- c. Stigma Sosial: Dalam beberapa kasus, data kesehatan pasien yang bocor, seperti diagnosis penyakit tertentu, bisa menyebabkan stigma sosial atau diskriminasi. Pasien yang mengalami kebocoran data kesehatan berisiko untuk mendapat perlakuan tidak adil dari masyarakat atau bahkan dari institusi tempat mereka bekerja.
- d. Kesalahan Medis: Data medis yang dimodifikasi atau diakses oleh pihak yang tidak berwenang bisa mengarah pada kesalahan medis yang fatal. Jika diagnosis atau resep obat salah karena manipulasi data, konsekuensinya bisa sangat serius, bahkan mematikan.



Gambar 3. Pasien khawatir terhadap keamanan data

2. Dampak Terhadap Institusi Kesehatan

Selain berdampak pada pasien, pelanggaran terhadap keamanan dan privasi data kesehatan juga bisa berisiko besar bagi institusi kesehatan itu sendiri. Dalam hal ini, dampak yang dihadapi dapat mencakup aspek hukum, finansial, serta reputasi institusi tersebut. Beberapa dampak yang dihadapi oleh institusi kesehatan adalah:

- a. Kehilangan Reputasi: Jika terjadi kebocoran data atau pelanggaran privasi, reputasi institusi kesehatan dapat terganggu secara signifikan. Reputasi yang buruk bisa berakibat pada berkurangnya jumlah pasien yang datang, kerugian finansial, dan penurunan kepercayaan dari mitra bisnis serta regulator.
- b. Sanksi Hukum: Banyak negara memiliki regulasi yang mengatur pengelolaan data kesehatan, seperti HIPAA di Amerika Serikat atau GDPR di Uni Eropa. Jika institusi kesehatan melanggar ketentuan-ketentuan ini, mereka bisa dikenakan sanksi hukum yang berat, yang bisa mencakup denda yang sangat besar. Selain itu, institusi tersebut bisa terlibat dalam proses hukum yang memakan waktu dan sumber daya yang banyak.
- c. Kerugian Finansial: Selain denda yang mungkin dikenakan oleh regulator, institusi kesehatan juga dapat menghadapi kerugian finansial akibat

serangan siber, misalnya, akibat ransomware yang mengenkripsi data dan meminta tebusan. Dalam beberapa kasus, biaya untuk pemulihan data dan perbaikan sistem keamanan juga bisa sangat besar.

- d. Gangguan Layanan: Pelanggaran terhadap keamanan data atau serangan siber dapat mengganggu operasi sehari-hari dari sistem kesehatan. Sistem informasi yang terhenti atau rusak akibat serangan dapat menyebabkan keterlambatan atau bahkan penghentian layanan medis yang krusial bagi pasien. Gangguan semacam ini bisa merusak layanan yang diberikan kepada pasien dan membahayakan nyawa mereka dalam kasus-kasus yang membutuhkan penanganan cepat.

3. Tantangan Teknologi

Seiring berkembangnya teknologi di dunia kesehatan, institusi kesehatan juga menghadapi tantangan besar dalam menjaga keamanan dan privasi data pasien. Beberapa tantangan utama dalam hal ini meliputi:

- a. Integrasi Sistem yang Kompleks: Banyak lembaga kesehatan menggunakan berbagai sistem IT yang terpisah, mulai dari sistem manajemen rumah sakit hingga perangkat medis yang terkoneksi dengan internet (IoT). Integrasi

antara sistem-sistem ini bisa membuka celah bagi ancaman keamanan, karena masing-masing sistem memiliki tingkat keamanan yang berbeda. Hal ini memerlukan upaya yang lebih besar untuk memastikan bahwa semua sistem ini terjaga keamanannya dan dapat berfungsi dengan baik secara bersamaan.

- b. Keterbatasan Sumber Daya: Tidak semua institusi kesehatan memiliki sumber daya yang cukup untuk mengimplementasikan teknologi keamanan terbaru dan melatih staf mereka dalam penggunaan sistem yang aman. Lembaga kesehatan kecil atau yang terletak di daerah-daerah terpencil sering kali kesulitan untuk mengakses teknologi dan pelatihan yang diperlukan untuk menjaga data mereka tetap aman.
- c. Keamanan Data dalam Cloud Computing: Semakin banyak lembaga kesehatan yang memindahkan data mereka ke cloud computing untuk efisiensi dan kemudahan akses. Meskipun cloud computing menawarkan banyak manfaat, hal ini juga membawa tantangan dalam hal kontrol akses dan pemeliharaan kerahasiaan data. Data yang tersimpan di server pihak ketiga menambah potensi risiko kebocoran atau penyalahgunaan data jika penyedia layanan

cloud tidak cukup kuat dalam menjaga aspek keamanan.

- d. Perangkat IoT dalam Kesehatan: Banyak perangkat medis saat ini, seperti alat pemantauan jantung atau perangkat yang digunakan untuk diagnosis medis, terhubung langsung ke internet (IoT). Meskipun hal ini meningkatkan efisiensi perawatan, juga membuka celah bagi ancaman siber, di mana peretas bisa mengakses perangkat ini untuk merusak atau mencuri data medis pasien.

4. Tantangan Etika dan Hukum

Selain tantangan teknis, aspek etika dan hukum juga memainkan peranan penting dalam pengelolaan keamanan dan privasi data kesehatan. Beberapa tantangan utama dalam bidang ini antara lain:

- a. Persetujuan Pasien (Informed Consent): Untuk melindungi privasi data pasien, institusi kesehatan harus memastikan bahwa mereka mendapatkan persetujuan yang jelas dan terinformasi dari pasien sebelum mengumpulkan atau memproses data mereka. Namun, banyak pasien yang tidak sepenuhnya memahami implikasi dari memberikan persetujuan untuk penggunaan data medis mereka. Ini menciptakan tantangan etis dalam

memastikan bahwa pasien benar-benar memahami risiko yang terkait dengan pengumpulan dan penggunaan data medis mereka.

- b. Hak atas Privasi dan Akses Data: Pasien harus memiliki kendali atas data pribadi mereka, termasuk hak untuk meminta penghapusan data atau mengontrol siapa yang dapat mengaksesnya. Namun, tidak semua sistem kesehatan memberikan akses penuh kepada pasien untuk mengelola data mereka sendiri, yang menimbulkan pertanyaan tentang hak atas privasi dan kendali terhadap data medis.
- c. Kepatuhan terhadap Regulasi yang Berbeda: Setiap negara memiliki regulasi yang berbeda mengenai pengelolaan data kesehatan, seperti HIPAA di AS, GDPR di Eropa, dan lainnya. Bagi institusi kesehatan yang beroperasi di lebih dari satu negara, kepatuhan terhadap berbagai regulasi ini bisa sangat rumit dan memerlukan

Dampak dan tantangan yang muncul akibat pelanggaran terhadap keamanan dan privasi data kesehatan sangat besar, baik bagi pasien maupun institusi kesehatan. Menjaga keamanan dan privasi data kesehatan memerlukan upaya yang tidak hanya melibatkan teknologi canggih, tetapi juga penerapan kebijakan yang sesuai, serta kepatuhan terhadap

regulasi dan standar yang berlaku. Tantangan ini terus berkembang seiring dengan pesatnya inovasi teknologi dalam sektor kesehatan, yang memerlukan perhatian terus-menerus dari semua pihak yang terlibat dalam pengelolaan data kesehatan untuk melindungi informasi yang sangat sensitif ini. Pada bab selanjutnya, kita akan menggali lebih dalam mengenai jenis ancaman yang dihadapi oleh sistem keamanan data kesehatan dan bagaimana institusi kesehatan dapat melindungi diri mereka dari ancaman-ancaman ini.

D. Strategi Pengelolaan Keamanan dan Privasi Data Kesehatan

Dalam upaya melindungi data kesehatan yang sensitif, strategi pengelolaan yang efektif sangat diperlukan. Keamanan dan privasi data bukanlah masalah yang dapat diselesaikan dengan satu solusi tunggal, melainkan memerlukan pendekatan yang komprehensif dan berkelanjutan. Untuk itu, institusi kesehatan perlu mengembangkan kebijakan yang holistik, mencakup berbagai lapisan perlindungan serta melibatkan seluruh elemen dalam organisasi.

1. Penetapan Kebijakan Keamanan yang Jelas

Langkah pertama dalam pengelolaan keamanan data kesehatan adalah penetapan kebijakan yang jelas mengenai keamanan informasi. Kebijakan ini

harus mencakup berbagai hal, seperti prosedur pengumpulan, penyimpanan, penggunaan, dan penghapusan data kesehatan. Selain itu, kebijakan ini juga harus mencakup pedoman tentang siapa yang berwenang mengakses data tersebut, serta bagaimana data tersebut dapat dipindahkan atau dibagikan kepada pihak ketiga (misalnya, mitra kerja atau perusahaan asuransi).

Beberapa langkah yang dapat diambil dalam penyusunan kebijakan ini meliputi:

- a. Pengelompokan Data Sensitif: Data pasien harus dikelompokkan berdasarkan tingkat sensitivitasnya. Misalnya, data medis yang berhubungan langsung dengan diagnosis atau riwayat penyakit harus dilindungi dengan tingkat keamanan yang lebih tinggi dibandingkan dengan data administratif yang tidak terlalu sensitif. Hal ini memungkinkan institusi untuk menentukan langkah-langkah perlindungan yang sesuai untuk setiap kategori data.
- b. Penyusunan Protokol Pengelolaan Data: Kebijakan harus mencakup protokol yang jelas mengenai bagaimana data dikumpulkan, disimpan, diakses, dan dihapus. Protokol ini juga harus menyarankan penggunaan metode enkripsi dan kontrol akses yang ketat untuk melindungi data pasien.

- c. Pemantauan dan Penegakan Kebijakan: Selain menyusun kebijakan, penting juga untuk memastikan kebijakan tersebut dipatuhi. Institusi kesehatan harus memiliki mekanisme pemantauan yang efektif untuk mengevaluasi kepatuhan terhadap kebijakan, serta mengambil tindakan yang diperlukan jika ditemukan pelanggaran.

2. Penerapan Teknologi Keamanan Canggih

Seiring dengan meningkatnya ancaman terhadap data kesehatan, teknologi yang digunakan untuk melindungi data juga harus semakin canggih. Penerapan teknologi yang tepat sangat krusial dalam melindungi data kesehatan. Beberapa teknologi yang sering digunakan untuk meningkatkan keamanan dan privasi data kesehatan antara lain:

- a. Enkripsi Data: Enkripsi adalah salah satu langkah paling dasar dan efektif dalam melindungi data. Dengan mengenkripsi data, informasi yang dikirimkan atau disimpan hanya bisa diakses oleh pihak yang memiliki kunci dekripsi yang sah. Proses enkripsi ini sangat penting, terutama ketika data dipindahkan melalui jaringan yang tidak sepenuhnya aman (misalnya, internet).
- b. Firewall dan Sistem Deteksi Intrusi: Sistem firewall yang kuat serta sistem deteksi intrusi