LEMBAR KERJA MAHASISWA

KEAMANAN DAN PERLINDUNGAN DATA

Dosen Pengampu: Yuda Syahidin, S.T.,M.Kom., MTA., CPDSA

Disusun Oleh:

Revana Khoerunnisa 24323030

RMIK-K31/24

PROGRAM STUDI D III REKAM MEDIS DAN INFORMASI KESEHATAN

POLITEKNIK PIKSI GANESHA BANDUNG

2025

MATERI 1

PENGANTAR KEAMANAN DAN PERLINDUNGAN DATA

STUDI KASUS: Analisis Kasus Kebocoran Data Pasien di Indonesia

1. **Kasus: Dugaan Kebocoran Data Pasien di Server Kementerian Kesehatan (Kemenkes RI) Tahun 2022**

   Pada Januari 2022, muncul laporan bahwa data pasien dari berbagai rumah sakit di Indonesia bocor dan dijual di forum gelap (dark web). Data tersebut diklaim berasal dari server Kementerian Kesehatan (Kemenkes) dan berukuran sekitar 720 GB. Data yang bocor mencakup:

   - Nama lengkap pasien
   - Nomor rekam medis
   - Nomor BPJS Kesehatan
   - Alamat dan tanggal lahir
   - Hasil tes COVID-19
   - Hasil laboratorium, radiologi (X-Ray, CT Scan)
   - Surat rujukan rumah sakit

   Sampel sekitar 6 juta data pasien ditampilkan oleh pelaku di forum "RaidForums" sebagai bukti kebocoran.

2. **Analisis dan Pelanggaran Regulasi**

   Kasus ini menimbulkan dugaan pelanggaran terhadap prinsip-prinsip perlindungan data pribadi dan keamanan informasi kesehatan, sebagaimana diatur dalam:

   - UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)
   - Permenkes No. 24 Tahun 2022 tentang Rekam Medis Elektronik
   - Serta prinsip yang sejalan dengan HIPAA (Health Insurance Portability and Accountability Act) di Amerika Serikat, yang mengatur kerahasiaan data kesehatan pasien.

   Menurut analisis BSSN (Badan Siber dan Sandi Negara) dan Kominfo, kebocoran ini menunjukkan:

   - Adanya kelemahan dalam sistem keamanan siber di sektor kesehatan, terutama pada enkripsi data dan kontrol akses.
   - Kurangnya audit keamanan rutin pada server yang menampung data sensitif.
   - Tata kelola data yang terpusat tanpa segmentasi keamanan yang baik, sehingga ketika satu sistem ditembus, seluruh data ikut terpapar.

3. **Dampak Kebocoran Data terhadap Pasien**

    - Privasi Pasien Data medis bersifat sangat pribadi. Bocornya hasil laboratorium atau diagnosis bisa menyebabkan rasa malu, stigma sosial, atau diskriminasi (misalnya pasien HIV atau penyakit kronis).
    - Pencurian Identitas (Identity Theft) Nomor BPJS dan NIK bisa disalahgunakan untuk klaim asuransi palsu atau transaksi ilegal.
    - Turunnya Kepercayaan Pasien Masyarakat menjadi ragu untuk memberikan data pribadi saat berobat di fasilitas kesehatan.
    - Risiko Hukum bagi Rumah Sakit dan Kemenkes Dapat dikenai sanksi administratif atau pidana menurut UU PDP jika terbukti lalai dalam menjaga keamanan data.
    - Kerugian Finansial Perbaikan sistem, investigasi forensik digital, dan pemulihan sistem memerlukan biaya besar.

4. **Langkah-langkah Perbaikan dan Pencegahan**
   Langkah yang Diambil Setelah Kebocoran
    - Investigasi Forensik Digital. Kemenkes bekerja sama dengan Kominfo dan BSSN untuk menelusuri sumber kebocoran serta menutup akses yang terbuka.
    - Audit Sistem dan Infrastruktur Seluruh rumah sakit diminta melakukan audit keamanan pada sistem rekam medis elektronik (RME).
    - Peningkatan Sistem Enkripsi dan Akses Data medis mulai diamankan dengan enkripsi end-to-end dan multi-factor authentication (MFA) bagi pengguna sistem rumah sakit.
    - Pelatihan Keamanan Siber (Cybersecurity Awareness) Seluruh tenaga kesehatan dan staf IT diberi pelatihan tentang phishing, social engineering, dan etika pengelolaan data pasien.
    - Implementasi Kebijakan Perlindungan Data Pasca insiden ini, pembahasan dan pengesahan UU Perlindungan Data Pribadi (UU PDP) pada September 2022 semakin dipercepat untuk memberikan dasar hukum yang kuat terhadap perlindungan data kesehatan.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Mengapa Enkripsi Sangat Penting dalam Pengelolaan Data Medis?**
   Enkripsi adalah proses mengubah data menjadi kode yang tidak bisa dibaca tanpa kunci tertentu. Dalam konteks data medis, enkripsi sangat penting karena:
    - Menjaga kerahasiaan data pasien, hanya petugas berwenang (dokter, rekam medis) yang bisa membuka data.
    - Mencegah kebocoran saat transmisi, misalnya ketika data dikirim antar rumah sakit atau ke server pusat.

- Melindungi dari serangan siber, jika sistem diretas, data terenkripsi tidak dapat digunakan tanpa kunci dekripsi.
- Kepatuhan hukum, UU PDP dan Permenkes 24/2022 mewajibkan penggunaan teknologi pengamanan seperti enkripsi dan autentikasi.

2. Apa yang Dapat Dilakukan Rumah Sakit untuk Melindungi Data Medis Pasien dari Ancaman Siber?

1. Aspek Teknis
    - Gunakan firewall, antivirus, dan intrusion detection system (IDS/IPS).
    - Terapkan enkripsi end-to-end untuk seluruh data pasien (baik di database maupun saat dikirim).
    - Gunakan multi-factor authentication (MFA) bagi semua pengguna sistem.
    - Lakukan backup data terenkripsi secara rutin di lokasi aman (offsite backup).
    - Gunakan sistem audit log untuk mencatat siapa mengakses data pasien dan kapan.
2. Aspek Sumber Daya Manusia
    - Adakan pelatihan rutin keamanan data untuk seluruh pegawai (termasuk dokter dan perawat).
    - Terapkan Role-Based Access Control (RBAC) setiap pegawai hanya boleh mengakses data sesuai jabatannya.
    - Buat kebijakan logout otomatis pada komputer yang tidak aktif.
3. Aspek Regulasi dan Tata Kelola
    - Bentuk Data Protection Officer (DPO) di setiap rumah sakit.
    - Terapkan kebijakan sesuai Permenkes No. 24 Tahun 2022 dan UU PDP No. 27 Tahun 2022.
    - Lakukan audit keamanan data secara berkala dan laporkan hasilnya ke Kominfo/BSSN.

3. Diskusikan Peran Setiap Individu di Rumah Sakit dalam Menjaga Keamanan Data

Peran dan tanggung jawab dalam keamanan data.

- Direktur Rumah Sakit. Menetapkan kebijakan keamanan data dan memastikan seluruh unit mematuhi UU PDP & Permenkes.
- Petugas Rekam Medis. Menyimpan, mengelola, dan membagikan data pasien secara sah, tidak membocorkan kepada pihak luar.
- Dokter dan Perawat. Menjaga kerahasiaan diagnosis, hasil laboratorium, dan tidak membicarakan informasi medis pasien di tempat umum.
- Bagian IT / SIMRS. Menjamin sistem informasi aman, mengelola enkripsi, firewall, backup, serta memantau akses tidak sah.
- Petugas Administrasi. Tidak mencetak, memfoto, atau menyebarkan dokumen pasien tanpa izin resmi.

- Pasien. Memberi data dengan benar dan memastikan izin penggunaannya (consent) sebelum data dibagikan ke pihak lain.

REFERENSI

Antara News. (2022, Januari 7). Kemenkes telusuri dugaan kebocoran jutaan data pasien. https://www.antaranews.com/berita/2628049

Katadata. (2022, Januari 7). Kominfo kaji dugaan kebocoran data jutaan pasien di server Kemenkes. https://katadata.co.id

Kementerian Kesehatan RI. (2022). Permenkes No. 24 Tahun 2022 tentang Rekam Medis Elektronik.

Republik Indonesia. (2022). UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Badan Siber dan Sandi Negara (BSSN). (2022). Laporan keamanan siber sektor kesehatan. https://bssn.go.id

MATERI 2

JENIS-JENIS DATA KESEHATAN DAN RISIKONYA

STUDI KASUS: Analisis Kasus Kebocoran Data Pasien di Indonesia

1. **Studi Kasus: Kehilangan Data Rekam Medis dan Pengaruhnya terhadap Keputusan Medis & Perawatan Pasien**
   Ada beberapa penelitian lokal yang menggambarkan bagaimana rekam medis pasien di rumah sakit di Indonesia mengalami kerusakan, hilang atau tidak lengkap — yang secara langsung ataupun tidak langsung memengaruhi pengambilan keputusan medis. Misalnya:
   - Analisis Penyebab dan Jenis Kerusakan Rekam Medis Pasien Rawat Inap di Rumah Sakit Angkatan Darat Tingkat IV Dr. R. Ismoyo Kendari (Alvirayanti, Kartiko & Wasita, 2022) melaporkan bahwa dari 427 rekam medis rawat inap di satu rumah sakit, 254 (59 %) mengalami kerusakan fisik, kimia atau biologis (misalnya sobek, hilang bagian, jamur, noda) yang mengganggu integritas data.
   - Faktor Faktor yang Mempengaruhi Ketidaklengkapan Rekam Medis Pasien pada Rumah Sakit di Indonesia (Wirajaya & Nuraini, 2021) menunjukkan bahwa banyak berkas rekam medis pasien rawat inap di rumah sakit Indonesia belum lengkap — yang dapat dimaknai sebagai "data hilang" dalam arti bahwa informasi penting tidak tercatat atau tercatat secara tidak memadai.
   - Regulasi nasional, misalnya Keputusan Menteri Kesehatan Republik Indonesia Nomor 269 Tahun 2008 tentang Rekam Medis, menegaskan bahwa fasilitas pelayanan kesehatan harus menjaga dan memantau agar data/informasi rekam medis baik cetak maupun elektronik dilindungi dari kehilangan, pencurian, kerusakan atau penghancuran yang tidak diinginkan.

   Analisis bagaimana kehilangan (atau kerusakan, ketidaklengkapan) data rekam medis dapat mempengaruhi keputusan medis & perawatan pasien:

   1. Kehilangan data historis pasien
      - Bila rekam medis seorang pasien tidak lengkap (misalnya diagnosis sebelumnya, alergi obat, hasil laboratorium lama) hilang atau kerusakannya, maka dokter yang menangani mungkin tidak mendapatkan gambaran lengkap kondisi medis pasien.
      - Akibatnya: keputusan medis (misalnya pemilihan terapi, dosis obat, prosedur tindakan) bisa menjadi kurang tepat atau lebih berisiko karena dokter bertindak dengan data yang tidak lengkap.
   2. Terhambatnya continuity of care (kelanjutan perawatan)
      - Jika transfer antar unit rawat inap/outpatient atau antar rumah sakit terjadi, dan data rekam medis hilang atau tidak lengkap, maka tim baru tidak memiliki "riwayat lengkap".

- Ini dapat mengakibatkan pengulangan pemeriksaan (menambah biaya/risiko), atau bahkan kelalaian terhadap kondisi sebelumnya.

3. Risiko kesalahan medis meningkat
    - Data yang hilang atau rusak dapat menyebabkan mis-interpretasi: misalnya obat yang sebelumnya diberikan tidak tercatat → pasien bisa mendapat obat yang seharusnya dihindari karena alergi atau interaksi obat.
    - Hasil laboratorium penting mungkin tidak tersedia → pengambilan keputusan (misalnya operasi, rawat ICU, dosis kemoterapi) bisa didasarkan pada data lama atau asumsi.
4. Berkurangnya keandalan rekam medis sebagai bukti atau dasar evaluasi
    - Untuk audit klinis, pertanggungjawaban medis, atau klaim asuransi, rekam medis yang hilang/kerusakakan berarti fasilitas kesehatan kehilangan bukti bahwa tindakan sudah dilakukan sesuai standar.
    - Ini bisa menyebabkan risiko hukum bagi rumah sakit maupun dokter.
5. Menurunnya mutu pelayanan & kepercayaan pasien
    - Ketika pasien mengetahui bahwa catatan mereka hilang atau data tidak dapat diakses, bisa muncul keraguan terhadap pelayanan.
    - Hal ini mengganggu hubungan kepercayaan antara pasien-penyedia layanan kesehatan dan dapat membuat pasien enggan berbagi data atau datang untuk tindakan lanjutan.

2. Pelajaran yang Dapat Diambil untuk Memperbaiki Pengelolaan Data di Masa Depan

Berdasarkan kasus-kasus di atas, berikut pembelajaran penting:

1. Standar operasional prosedur (SOP) pengisian dan pengarsipan rekam medis harus jelas dan diterapkan
    - Studi seperti yang di Wirajaya & Nuraini menunjukkan bahwa ketidaklengkapan rekam medis disebabkan oleh kurangnya SOP, kurangnya monitoring, dan kesibukan petugas.
2. Infrastruktur penyimpanan & sistem pengamanan data harus memadai
    - Penyimpanan baik fisik maupun digital harus dilindungi dari kerusakan fisik, kebakaran, jamur, kelembapan, maupun kehilangan elektronik. (contoh: kasus Kendari)
    - Sistem backup rutin, proteksi dari kesalahan penghapusan atau kerusakan, serta pemantauan akses sangat penting (lihat regulasi Kemenkes).
3. Digitalisasi rekam medis (EMR) dengan keamanan yang memadai
    - Transisi ke rekam medis elektronik memberi banyak keuntungan (akses cepat, integrasi antar unit), namun juga meningkatkan risiko kehilangan/manipulasi data bila keamanan lemah.
    - Oleh karena itu: enkripsi, autentikasi pengguna, kontrol akses, audit log dan backup adalah keharusan.

4. Pelatihan SDM & budaya keamanan data
    - Petugas rekam medis, dokter, perawat semua harus sadar bahwa kehilangan atau ketidaklengkapan data bukan hanya administrasi tetapi bisa berdampak klinis.
    - Monitoring dan evaluasi rutin terkait kelengkapan berkas dan integritas data harus diterapkan (contoh penelitian di RS Kalisat)
5. Retention policy dan monitoring retensi berkas
    - Arsip rekam medis yang sudah lama harus dikelola: dikategorikan, diarsipkan secara aman atau dihapus sesuai kebijakan, agar tidak menumpuk dan rusak. (contoh RSUD Waluyo Jati)
6. Keamanan informasi dan perlindungan data dari kehilangan/manipulasi
    - Harus ada strategi untuk menghindari kehilangan data seperti yang terjadi akibat gangguan teknis atau kelalaian petugas.
    - Evaluasi kerentanan (risk assessment) secara berkala agar sistem data rekam medis tahan terhadap ancaman.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Apa saja jenis data medis yang paling rentan terhadap kebocoran?**

   Beberapa jenis data medis yang sangat rentan adalah:
    - Biodata pasien (nama lengkap, NIK, alamat, tanggal lahir) karena sering dicatat dan dipindahkan antar sistem.
    - Data identitas asuransi/keanggotaan (BPJS, asuransi swasta) rentan digunakan untuk penipuan.
    - Hasil diagnosa dan riwayat penyakit kronis karena sangat sensitif secara klinis dan sosial (misalnya HIV, kanker).
    - Hasil pemeriksaan laboratorium, radiologi, gambar CT/X-Ray karena memiliki nilai medis tinggi dan bisa digunakan untuk eksploitasi.
    - Catatan tindakan atau operasi medis jika bocor, bisa jadi dasar litigasi atau klaim yang merugikan fasilitas.
    - Data medis elektronik yang dipertukarkan antar fasilitas apabila sistem interoperabilitas kurang aman maka risiko bocorannya tinggi.

   Karena data-data tersebut memiliki kombinasi faktor “sangat sensitif” + “sering diakses atau ditransfer”, maka proteksi ekstra dibutuhkan.

2. **Bagaimana cara melindungi data pasien dari risiko manipulasi atau kehilangan?**

   Langkah-langkah yang bisa dilakukan rumah sakit adalah:
    - Backup rutin dan off-site storage: Simpan salinan data di lokasi terpisah dan pastikan dapat dipulihkan bila terjadi kehilangan.
    - Enkripsi data: Pastikan data saat disimpan (at-rest) dan saat dikirim (in-transit) terenkripsi agar tidak dapat dibaca pihak tidak berwenang.

- Kontrol akses dan autentikasi kuat: Terapkan login dengan multi-factor authentication (MFA), dan hanya izinkan akses sesuai peran (role-based access).
- Audit log dan monitoring aktivitas: Catat siapa mengakses data apa dan kapan, gunakan sistem untuk mendeteksi akses abnormal atau potensi manipulasi.
- Pemeliharaan fisik maupun digital: Untuk berkas fisik, lindungi dari kerusakan fisik (kelembapan, jamur, api, hilang). Untuk sistem digital, perbarui patch keamanan, antivirus, firewall, IDS/IPS.
- Penerapan SOP dan pelatihan SDM: Petugas harus dilatih secara rutin agar sadar risiko kehilangan atau manipulasi data. Kesadaran pegawai bisa mencegah banyak risiko.
- Retensi dan penghapusan yang aman: Tentukan kebijakan berapa lama menyimpan data dan kapan harus dihapus atau diarsipkan secara aman untuk menghindari akumulasi berkas usang yang rawan kerusakan atau akses tidak sah.
- Sistem pemulihan darurat (disaster recovery plan): Jika sistem utama gagal (banjir, kebakaran, ransomware), harus ada rencana pemulihan agar data dan layanan bisa kembali sesegera mungkin.

REFERENSI

Alvirayanti, N. K. P., Kartiko, B. H., & Wasita, R. R. (2022). Analisis penyebab dan jenis kerusakan rekam medis pasien rawat inap di Rumah Sakit Angkatan Darat Tingkat IV Dr. R. Ismoyo Kendari. Bali Health Published Journal, 5(2). https://doi.org/10.47859/bhpj.v5i2.339

Wirajaya, M. K., & Nuraini, N. (2021). Faktor-faktor yang mempengaruhi ketidaklengkapan rekam medis pasien pada rumah sakit di Indonesia. Jurnal Manajemen Informasi Kesehatan Indonesia, 7(2). https://doi.org/10.33560/jmiki.v7i2.225

Kementerian Kesehatan Republik Indonesia. (2008). Keputusan Menteri Kesehatan Republik Indonesia Nomor 269 Tahun 2008 tentang Rekam Medis. Jakarta: Kemenkes RI. https://keslan.kemkes.go.id/unduhan/fileunduhan_1654499045_682777.pdf

Agustina, E. A. (2023). Evaluasi aspek keamanan dan kerahasiaan rekam medis elektronik. Jurnal Permata Indonesia, 3(1). https://jurnal.permataindonesia.ac.id/index.php/JPI/article/download/265/202/394

Rahmawati, A. Y., Putri, D. A., & Wijayanti, D. (2022). Tinjauan permasalahan instalasi rekam medis berdasarkan unsur 5M+1T di Rumah Sakit X Surabaya. Jurnal Ilmiah Keperawatan, 10(2). https://doi.org/10.33023/jikep.v10i2.1802

MATERI 3

ANCAMAN KEAMANAN DATA DI DUNIA KESEHATAN

STUDI KASUS: Analisis Kasus Kebocoran Data Pasien di Indonesia

1. Kasus Serangan Phishing di Rumah Sakit

BAnyak literatur menyebut bahwa sektor kesehatan sangat rentan phishing sebagai vektor awal. Sebagai contoh:

- Menurut laporan dari HIPAA Journal, phishing adalah pemicu utama pelanggaran data di bidang kesehatan—"phishing is a leading cause of healthcare data breaches and attacks appear to be increasing."
- Laporan dari U.S. Department of Health & Human Services (HHS) tentang social engineering di sektor kesehatan menyebut bahwa "phishing remains one of the most effective social engineering attacks used against healthcare organizations."

Narasi kasus:

Sebuah rumah sakit besar di Indonesia (sebut saja RS "Bhayangkara") yang menggunakan sistem Rekam Medis Elektronik (RME). Seorang staf admisi atau petugas rekam medis menerima email yang tampak sah dari "IT Helpdesk" dengan subjek "Verifikasi Akun RME – Tindakan cepat diperlukan". Email tersebut mengandung link ke tampilan login yang tampak identik dengan portal RME internal. Karena merasa terdesak dan tidak cukup pelatihan tentang phishing, staf tersebut memasukkan kredensial login (username + password). Hacker kemudian menggunakan kredensial tersebut untuk mengakses sistem RME, mengeksfiltrasi data pasien (nama, NIK, hasil laboratorium, rekam medis rawat inap) dan menjualnya di forum gelap.

Akibatnya:

- Data pasien jatuh ke tangan yang tidak berwenang.
- Rumah sakit kehilangan kontrol terhadap akses dan integritas data.
- Potensi pelanggaran regulasi seperti UU PDP di Indonesia (ditetapkan 2022).
- Pasien merasa privasi mereka terganggu, dan kepercayaan publik terhadap RS Bhayangkara menurun.

Analisis: Pencegahan dengan Pelatihan Staf dan Otentikasi Multi-Faktor (MFA)

Faktor kegagalan yang memungkinkan phishing berhasil

1. Kurangnya kesadaran staf: Staf tidak mendapat pelatihan rutin mengenai phishing, social engineering, identifikasi email mencurigakan.

2. Kredensial tunggal (single factor authentication): Sistem hanya menggunakan username & password, tanpa lapisan keamanan tambahan.

3. Prosedur kurang kuat: Tidak ada verifikasi ganda (misalnya konfirmasi via telepon atau token) sebelum perubahan akses atau reset password.

4. Monitoring dan deteksi lambat: Setelah login yang mencurigakan, tidak ada sistem pemantauan yang cepat untuk mendeteksi anomali akses.

Langkah-langkah pencegahan

- Pelatihan keamanan rutin untuk semua staf: Meliputi simulasi phishing (uji coba email palsu), edukasi tentang tanda-tanda phishing, prosedur pelaporan jika staf ragu. Studi di Italia menunjukkan simulasi phishing berhasil meningkatkan kesadaran staf.
- Penerapan Otentikasi Multi-Faktor (MFA): Misalnya penggunaan token (hardware atau aplikasi) atau SMS/OTP sebagai lapisan kedua di atas password. Dengan MFA, meskipun password bocor, akses tetap tertahan karena faktor kedua gagal.
- Pembatasan akses sesuai peran & hak istimewa (least-privilege access): Hanya staf yang benar-benar butuh akses ke data tertentu yang diberikan izin, dan akses diaudit secara ketat.
- Segregasi jaringan dan segmentasi sistem: Sistem RME dipisah dari sistem e-mail umum agar kompromi e-mail tidak langsung membuka RME.
- Log audit dan pemantauan aktivitas tidak biasa: Sistem memantau akses di luar jam kerja, dari lokasi/IP tidak biasa, atau volume data yang tinggi dan memicu alert.
- Prosedur respons insiden: Ada SOP jika kredensial diketahui kompromi segera reset, isolasi akun, investigasi forensik.

Untuk konteks Indonesia, rumah sakit perlu merujuk juga pada regulasi seperti UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Permenkes No. 24 Tahun 2022 tentang Rekam Medis Elektronik agar kebijakan keamanan data ditaati.

2. Kasus Serangan Ransomware di Rumah Sakit

Dalam studi oleh HHS: dokumen "Ransomware & Healthcare" menyatakan bahwa banyak jaringan rumah sakit besar mengalami ransomware, yang "large hospital network experienced a ransomware incident, and multiple sites within the network were impacted."

Sebuah studi kasus di UVM Health Network, AS: Seorang karyawan menggunakan laptop untuk keperluan pribadi di luar sistem, membuka email phishing dan memicu ransomware. Infrastruktur TI banyak rusak, namun mereka sudah memiliki backup sehingga pasien data tidak bocor.

Narasi kasus (adaptasi untuk rumah sakit Indonesia, RS “Fatmawati”):
RS Fatmawati terhubung ke sistem elektronik dan jaringan internal. Seorang karyawan IT menggunakan laptop kerja di rumah dan secara tidak sengaja membuka lampiran malware lewat email. Malware tersebut menyebar ke server utama RME, mengenkripsi database, memblokir akses ke ratusan ribu rekam medis pasien. Sistem layanan terhenti sementara: proses pendaftaran, pemeriksaan laboratorium, dan rujukan semuanya berjalan secara manual. Rumah sakit menerima permintaan tebusan (ransom) dari hacker agar mengembalikan akses, namun RS Bhayangkara memilih untuk tidak membayar dan memulihkan dari backup.

Akibatnya:

- Layanan pasien tertunda, beberapa operasi elektif dibatalkan atau dipindahkan.
- Data mungkin tidak dibocorkan tapi aksesnya hilang, membuat RS Y harus manual selama beberapa hari.
- Biaya pemulihan sangat besar: mengganti hardware, memulihkan backup, audit keamanan, dan komunikasi dengan pasien.

Analisis: Kesalahan yang Membuat Serangan Berhasil & Langkah Perbaikan Kebijakan

Faktor kelemahan yang memfasilitasi ransomware

- Endpoint yang lemah: Laptop karyawan yang digunakan untuk keperluan pribadi tanpa pengamanan yang memadai (patching, antivirus up to date).
- Akses jaringan yang kurang segmentasi: Laptop tersebut memiliki akses yang cukup luas ke server RME tanpa pembatasan.
- Tidak ada backup yang teruji atau cadangan offline: Jika backup belum diuji, atau jaringan yang sama bisa terinfeksi, maka pemulihan sulit.
- Tidak ada rencana pemulihan bencana (disaster recovery plan) yang efektif.

Langkah-langkah perbaikan

- Backup yang aman, sering, dan terpisah secara fisik / jaringan (“offline” or “air-gap”): Sistem backup yang tidak terhubung ke jaringan utama mencegah malware mengenkripsi backup juga.
- Cadangan uji rutin dan verifikasi pemulihan: Pastikan backup dapat dipulihkan dalam waktu wajar tanpa kehilangan data.
- Segmentasi jaringan dan kontrol akses kuat: Server penting harus diisolasi, akses ke server RME melalui jalur yang aman, minimal jumlah perangkat yang bisa terhubung langsung.
- Penerapan prinsip least-privilege dan autentikasi kuat (MFA): Siapa saja yang bisa menjalankan server atau memiliki hak tinggi harus melalui MFA dan harus diaudit.

- Endpoint protection dan kebijakan penggunaan perangkat: Kebijakan BYOD (Bring Your Own Device) atau penggunaan laptop kerja punya pengamanan seperti enkripsi disk, VPN aman, monitoring.
- Rencana Pemulihan Insiden teruji: Simulasi secara berkala (table-top exercise), kesiapan tim IT, prosedur manual apabila sistem offline (misalnya formulir kertas, fallback).
- Pengawasan dan pembaruan rutin sistem keamanan: Patch OS, aplikasi, firewall, IDS/IPS, serta pelatihan kepada staf tentang malware dan ransomware.

RS harus juga mengacu pada standar keamanan informasi seperti ISO/IEC 27001 dan pedoman dari Badan Siber dan Sandi Negara (BSSN) untuk sektor kesehata.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Apa yang dimaksud dengan ancaman internal dan eksternal dalam konteks keamanan data rumah sakit? Berikan contoh dari keduanya.**
    - Ancaman eksternal: Serangan berasal dari luar organisasi, misalnya hacker yang mengirim email phishing ke staf rumah sakit, atau ransomware yang dimasukkan melalui exploit jaringan. Contoh: phishing ke staf RS Bhayangkara yang memberi hacker akses ke sistem.
    - Ancaman internal: Serangan atau kebocoran yang berasal dari dalam organisasi atau karena kelemahan internal, misalnya staf yang tidak berwenang mengakses data pasien secara tidak sah, atau karyawan yang secara tidak sengaja membuka malware dari email pribadi. Contoh: laptop staf IT RS Fatmawati digunakan untuk email pribadi dan menjadi vektor ransomware.

2. **Jelaskan langkah-langkah yang dapat diambil rumah sakit untuk mengurangi risiko serangan ransomware dan phishing.**
   Untuk phishing:
    - Pelatihan dan simulasi phishing secara rutin bagi seluruh staf.
    - Implementasi MFA untuk akses ke sistem RME dan sistem vital lainnya.
    - Audit akses dan pemantauan log aktivitas, deteksi anomali.
    - Pembuatan dan pemeliharaan kebijakan penggunaan email, perangkat, dan internet.
    - Segmentasi jaringan dan pemisahan sistem vital dari sistem yang berisiko.

   Untuk ransomware:
    - Backup data rutin dan terpisah (offline atau air-gap).
    - Verifikasi pemulihan backup secara berkala.
    - Endpoint protection kuat dan patch management.
    - Segmentasi jaringan dan hak akses terbatas (least-privilege).
    - Rencana pemulihan insiden dan latihan simulasi.

- Pengawasan vendor dan pihak ketiga (third-party risk), karena sering melalui vendor remote access.

3. **Bagaimana Anda akan mendesain kebijakan keamanan untuk melindungi data pasien di rumah sakit?**

   Desain kebijakan keamanan harus mencakup elemen-elemen berikut:

   1. Kebijakan akses dan autentikasi
      - Semua pengguna sistem harus melalui MFA.
      - Role-based access: hanya personel yang memerlukan akses ke data medis yang diberi hak, dan hak tersebut harus ditinjau secara rutin.
      - Hak administrator dibatasi dan dipantau.
   2. Pelatihan dan pendidikan keamanan
      - Pelatihan rutin tentang phishing, social engineering, penggunaan perangkat dan email yang aman.
      - Simulasi serangan (phishing) setiap 3–6 bulan untuk menguji kesiapan staf.
   3. Proteksi teknis
      - Enkripsi data saat disimpan (data at-rest) dan saat dikirim (data in-transit).
      - Segmentasi jaringan: sistem RME dipisah dari sistem email/general IT.
      - Backup reguler yang diuji pemulihannya dan disimpan secara offline/terpisah.
      - Penggunaan firewall, IDS/IPS, antivirus, monitoring keamanan secara real-time.
   4. Pengelolaan perangkat dan endpoint
      - Kebijakan BYOD jika diterapkan: enkripsi perangkat, VPN, akses terbatas.
      - Laptop kerja tidak boleh digunakan untuk kegiatan pribadi yang berisiko.
   5. Manajemen insiden dan pemulihan bencana
      - SOP insiden keamanan: siapa dihubungi, langkah isolasi, pemberitahuan ke Kominfo/BSSN/pasien.
      - Rencana pemulihan bencana: skenario manual bila sistem down (formulir kertas, fallback).
   6. Audit, evaluasi dan kepatuhan regulasi
      - Audit sistem dan proses keamanan secara berkala.
      - Kepatuhan terhadap regulasi seperti UU PDP dan Permenkes 24/2022.
      - Pencatatan log akses dan analisis anomali.
   7. Vendor & pihak ketiga
      - Kebijakan keamanan untuk vendor yang memiliki akses ke sistem atau data rumah sakit.
      - Kontrak yang memuat persyaratan keamanan dan audit.

REFERENSI

HIPAA Journal. (2024, Jan 6). Healthcare Data Breaches Due to Phishing. Retrieved from https://www.hipaajournal.com/healthcare-data-breaches-due-to-phishing/

U.S. Department of Health & Human Services. (2023). Social Engineering Attacks Targeting the HPH Sector. Retrieved from https://www.hhs.gov/sites/default/files/social-engineering-targeting-the-hph-sector-tlpclear.pdf

Centripetal. (n.d.). How Ransomware and Phishing Impact the Healthcare Sector. Retrieved from https://www.centripetal.ai/blog/how-ransomware-and-phishing-impact-the-healthcare-sector/

Insurica. (2020). Cyber Case Study: UVM Health Network Ransomware Attack. Retrieved from https://insurica.com/blog/uvm-health-network-ransomware-attack/

American Hospital Association. (n.d.). Ransomware Attacks on Hospitals Are Not White-Collar Crimes. Retrieved from https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed

MATERI 4

KEAMANAN DATA DALAM INFRASTRUKTUR TEKNOLOGI INFORMASI KESEHATAN

STUDI KASUS ATAU ANALISIS DATA

1. **Analisis Kasus Serangan Ransomware di Rumah Sakit: Kasus RS Dharmais dan RS Harapan Kita (Jakarta, 2017)**

   Pada Mei 2017, dua rumah sakit besar di Indonesia RS Dharmais dan RS Harapan Kita menjadi korban serangan ransomware global bernama WannaCry. Serangan ini mengenkripsi data di komputer rumah sakit dan meminta tebusan dalam bentuk Bitcoin agar data bisa dipulihkan. Serangan tersebut menjadi salah satu insiden siber terbesar yang pernah melanda sektor kesehatan di Indonesia.

   Dampak terhadap Operasional Rumah Sakit

   - Gangguan Layanan Medis: Sistem pendaftaran pasien, antrean, dan sistem BPJS Online di RS Dharmais lumpuh total. Pelayanan menjadi manual, menyebabkan antrean panjang dan keterlambatan penanganan pasien.
   - Gangguan terhadap Staf Medis: Dokter dan perawat kehilangan akses ke sistem rekam medis elektronik (RME) sementara, sehingga pengambilan keputusan medis harus dilakukan tanpa riwayat digital pasien.
   - Dampak pada Pasien:Beberapa pasien harus menunda perawatan karena keterlambatan administratif dan identifikasi data. Risiko kesalahan medis meningkat akibat kurangnya akses cepat ke data klinis.
   - Kerugian Reputasi dan Finansial: Meskipun data akhirnya bisa dipulihkan tanpa membayar tebusan, reputasi rumah sakit sempat menurun karena dinilai tidak siap menghadapi ancaman siber.

   Pelajaran dan Perbaikan Infrastruktur TI

   - Pentingnya Backup Data Teratur: RS Dharmais mampu memulihkan data karena memiliki cadangan offline yang tidak terinfeksi ransomware.
   - Segmentasi Jaringan: Infrastruktur TI perlu dipisah antara sistem klinis, administrasi, dan publik agar malware tidak mudah menyebar.
   - Peningkatan Kesadaran Staf: Banyak serangan siber berhasil karena kesalahan manusia, seperti mengklik tautan atau lampiran berbahaya. Rumah sakit wajib melatih staf untuk mengenali tanda-tanda serangan siber.
   - Implementasi Patch Management: Serangan WannaCry memanfaatkan celah keamanan Windows yang belum diperbarui. Pembaruan sistem secara rutin harus menjadi prioritas utama.

- Koordinasi dengan Pemerintah: RS Dharmais berkoordinasi dengan Kemenkes dan Kominfo untuk pemulihan sistem, menunjukkan pentingnya sinergi lintas lembaga.

2. **Keberhasilan Pengimplementasian Sistem Keamanan di Rumah Sakit: Kasus RS Universitas Gadjah Mada (RS UGM, Yogyakarta)**
   RS Universitas Gadjah Mada (RS UGM) menjadi salah satu rumah sakit pendidikan di Indonesia yang berhasil menerapkan sistem keamanan informasi berlapis dengan standar ISO/IEC 27001:2013. Sertifikasi ini menunjukkan komitmen terhadap pengamanan data, termasuk data medis pasien, serta tata kelola sistem TI yang kuat dan berkelanjutan.

   Upaya dan Strategi Pengamanan Data
   - Penerapan Sistem Keamanan Berlapis: RS UGM menerapkan firewall, enkripsi data, deteksi intrusi, dan kontrol akses berbasis hak pengguna.
   - Penerapan Kebijakan Keamanan Informasi (Information Security Policy): Setiap staf wajib mengikuti pelatihan keamanan data, termasuk cara menangani email mencurigakan dan menjaga kerahasiaan informasi pasien.
   - Implementasi Otentikasi Multi-Faktor (MFA): Akses ke sistem RME dan server dilakukan dengan verifikasi ganda (password + token digital).
   - Audit Keamanan Berkala: Tim internal dan eksternal melakukan penilaian keamanan sistem TI secara periodik untuk memastikan kepatuhan terhadap standar ISO/IEC 27001.
   - Backup & Disaster Recovery System: RS UGM memiliki sistem cadangan data dan server pemulihan (recovery site) untuk memastikan layanan tetap berjalan jika terjadi gangguan.

   Dampak Positif Implementasi

   - Meningkatkan Kepercayaan Pasien dan Mitra: Pasien merasa lebih aman karena data medis mereka dilindungi sesuai standar internasional.
   - Efisiensi Operasional: Dengan keamanan sistem yang baik, downtime akibat gangguan teknis menurun drastis.
   - Peningkatan Citra Institusi: RS UGM menjadi contoh praktik terbaik (best practice) dalam keamanan informasi di sektor kesehatan Indonesia.

   Pelajaran yang Dapat Diambil
   - Investasi pada SDM TI: Keamanan siber bukan hanya urusan teknologi, tetapi juga kesadaran dan kompetensi manusia.
   - Standarisasi Global (ISO 27001): Sertifikasi ini membantu rumah sakit membangun sistem keamanan yang terukur dan dapat diaudit.
   - Monitoring dan Evaluasi Berkelanjutan: Ancaman siber terus berevolusi, sehingga rumah sakit harus melakukan evaluasi keamanan secara berkala.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Apa saja langkah-langkah yang dapat diambil rumah sakit untuk melindungi jaringan mereka dari serangan siber?**
    - Implementasi Firewall dan IDS (Intrusion Detection System) untuk memantau aktivitas jaringan.
    - Pembaruan sistem secara rutin (patch management) untuk menutup celah keamanan.
    - Penggunaan Enkripsi Data saat transmisi dan penyimpanan.
    - Penerapan Otentikasi Multi-Faktor (MFA) pada semua sistem sensitif.
    - Pelatihan Keamanan Siber untuk seluruh staf medis dan administrasi.
    - Rencana Kontinjensi (Disaster Recovery Plan) agar layanan tetap berjalan saat terjadi serangan.
2. **Bagaimana Anda dapat meningkatkan keamanan sistem RME di rumah sakit?**
    - Audit Sistem Berkala: Mengevaluasi hak akses pengguna dan mendeteksi aktivitas mencurigakan
    - Enkripsi Database RME: Semua data pasien harus dienkripsi agar tidak dapat dibaca jika dicuri.
    - Implementasi Role-Based Access Control (RBAC): Setiap pengguna hanya dapat mengakses data sesuai peran.
    - Backup Harian ke Server Terpisah: Menjamin data dapat dipulihkan jika terjadi serangan.
    - Simulasi Serangan (Penetration Test): Menguji kesiapan sistem terhadap ancaman dunia nyata.

REFERENSI

Kompas.com. (2023, Mei 17). Melihat kembali kehebohan serangan ransomware WannaCry di Indonesia 6 tahun lalu. https://tekno.kompas.com/read/2023/05/17/14150007/melihat-kembali-kehebohan-serangan-ransomware-wannacry-di-indonesia-6-tahun

DetikHealth. (2017, Mei 15). Ada serangan ransomware, Menkes harap layanan RS segera pulih. https://health.detik.com/berita-detikhealth/d-3501205/ada-serangan-ransomware-menkes-harap-besok-layanan-rs-sudah-pulih

Universitas Gadjah Mada. (2023, Juni 20). RS UGM raih sertifikasi ISO 27001 untuk keamanan informasi. https://ugm.ac.id/id/berita/23743-rs-ugm-raih-sertifikasi-iso-27001-keamanan-informasi/

MATERI 5

PERATURAN PERLINDUNGAN DATA KESEHATAN (HIPAA, GDPR)

STUDI KASUS ATAU ANALISIS DATA

1. **Analisis Kasus Denda GDPR di Rumah Sakit**
   Di Jerman, sebuah rumah sakit di distrik Rheinland-Pfalz dikenakan denda €105.000 oleh komisi perlindungan data setempat karena berbagai pelanggaran GDPR termasuk pencampuran pasien saat penerimaan yang menyebabkan faktur salah serta "deficits in patient and privacy management".

   Di Portugal, sebuah rumah sakit dikenakan denda sebesar €400.000 oleh otoritas nasional (CNPD) karena pelanggaran regulasi GDPR yang berkaitan dengan data pasien melalui profil palsu.

   Dampak dari Pelanggaran
   - Finansial langsung: Denda besar dapat menghabiskan dana yang bisa dialokasikan ke layanan medis ataupun investasi teknologi.
   - Reputasi rumah sakit: Rumah sakit yang terkena denda dilihat sebagai lembaga yang tidak dapat melindungi data pasien menurunkan kepercayaan masyarakat dan mungkin mengurangi jumlah pasien atau kolaborasi.
   - Operasional terganggu: Ketika audit dilakukan atau lembaga eksternal memeriksa, fokus TI dan manajemen bisa terganggu, mengalihkan sumber daya dari layanan klinis.
   - Peninjauan sistem internal: Rumah sakit harus melakukan revisi besar terhadap kebijakan, sistem keamanan, pelatihan staf yang semuanya memakan waktu dan biaya.
   - Tanggung jawab hukum dan regulasi: Pelanggaran GDPR bisa memicu investigasi lebih lanjut, kewajiban melaporkan insiden, dan tuntutan pasien yang merasa haknya dilanggar.

   Langkah Pencegahan Setelah Denda

   - Peningkatan pengamanan teknis, seperti autentikasi kuat, enkripsi data, pengendalian akses yang lebih ketat.
   - Penguatan tata kelola dan prosedur internal (SOP) untuk manajemen data pasien, termasuk penerimaan, penyimpanan, berbagi data, dan penghapusan data.
   - Pelatihan intensif bagi semua pihak, dan simulasi insiden kebocoran atau pelanggaran agar staf siap merespons.
   - Pemantauan dan audit internal secara berkala, serta kerjasama dengan otoritas perlindungan data dan konsultan keamanan agar kualitas sistem selalu ditingkatkan.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Bagaimana GDPR memengaruhi cara rumah sakit mengelola data pribadi pasien di Eropa?**
   GDPR membawa beberapa perubahan penting bagi rumah sakit:
   - Harus memiliki dasar hukum yang jelas untuk pengolahan data pribadi pasien (misalnya consent, kepentingan publik, pelayanan kesehatan) sesuai Pasal 6 & 9 GDPR.
   - Data kategori khusus (termasuk data kesehatan) mendapat perlindungan ekstra misalnya persyaratan minimalisasi data, pseudonimisasi, dan keamanan tambahan.
   - Hak pasien diperkuat: akses ke data mereka, portabilitas data, hak penghapusan (right to erasure), hak pembatasan pemrosesan.
   - Kewajiban memperhatikan "confidentiality, integrity and availability" data rumah sakit harus memastikan bahwa sistem data mereka memenuhi standar teknis dan organisasi yang memadai.
   - Pelaporan insiden kebocoran dalam waktu 72 jam kepada otoritas.
   - Dokumentasi internal dan audit: rumah sakit harus mampu menunjukkan mereka sudah menerapkan standar keamanan dan tata kelola yang memadai.
   - Fokus pada keamanan sejak desain ("privacy by design" dan "privacy by default") sistem RME dan rekam medis elektronik harus dibangun dengan pertimbangan perlindungan data sejak awal.

2. **Apa saja dampak dari pelanggaran Health Insurance Portability and Accountability Act (HIPAA) pada reputasi rumah sakit dan kepercayaan pasien?**
   Walaupun HIPAA adalah regulasi AS, implikasinya serupa bagi rumah sakit di mana pun yang menangani data sensitif:
   - Ketika terjadi pelanggaran HIPAA, rumah sakit bisa terkena denda besar, dikenai investigasi federal/negara bagian, dan harus mengambil langkah pemulihan yang signifikan.
   - Reputasi rumah sakit bisa rusak: pasien khawatir bahwa data mereka tidak aman dan bisa berpindah ke institusi lain. Partner dan asuransi bisa ragu berkolaborasi.
   - Layanan medis bisa terganggu karena fokus dialihkan ke pemulihan, audit, litigasi — sumber daya yang seharusnya untuk klinis dipakai untuk keamanan dan regulasi.
   - Kepercayaan publik hilang: pasien bisa mencurigai bahwa rumah sakit akan membagikan atau menjual data mereka tanpa izin, yang bisa mengurangi keinginan pasien untuk memberikan informasi lengkap atau datang ke rumah sakit.
   - Biaya tersembunyi: selain denda, rumah sakit harus menginvestasikan lebih banyak di TI, pelatihan, pemulihan reputasi, dan mungkin kompensasi kepada pasien yang terkena dampak.

REFERENSI

European Data Protection Board. (2019, November 4). Fine against hospital due to data protection deficits in patient management. https://www.edpb.europa.eu/news/national-news/2019/fine-against-hospital-due-data-protection-deficits-patient-management_en

GDPR.eu. (n.d.). What are the GDPR fines? https://gdpr.eu/fines/

Riou, C. (2025). Ensuring General Data Protection Regulation compliance: A study of France's CDW framework through its implementation at a major university hospital. International Journal of Medical Informatics. (Note: article online ahead of print) https://doi.org/10.1016/j.ijmedinf.2025.104593

GDPRRegister. (2018, July 17). Hospital in Portugal receives and contests €400,000 fine for GDPR infringement. https://www.insideprivacy.com/data-privacy/portuguese-hospital-receives-and-contests-400000-e-fine-for-gdpr-infringement/

Dutch DPA (Autoriteit Persoonsgegevens). (2021). Dutch DPA fines OLVG hospital for inadequate protection of medical records. https://www.edpb.europa.eu/news/national-news/dutch-dpa-fines-olvg-hospital-inadequate-protection-medical-records_en

Vukovic, J., et al. (2022). Enablers and barriers to the secondary use of health data in Europe: The role of GDPR. Archives of Public Health, 80. https://doi.org/10.1186/s13690-022-00866-7

MATERI 6

PENGELOLAAN AKSES DATA DAN KONTROL PENGGUNA

STUDI KASUS ATAU ANALISIS DATA

1. **Kasus Penyalahgunaan Akses oleh Staf Rumah Sakit**
   Kasus penyalahgunaan akses data pasien oleh staf rumah sakit pernah terjadi di berbagai negara, termasuk Indonesia. Salah satu kasus yang menjadi perhatian adalah dugaan akses tidak sah terhadap data pasien di RSUD Dr. Soetomo, Surabaya, di mana data pasien HIV bocor dan tersebar ke publik pada tahun 2021.

   Kebocoran tersebut terjadi akibat akses internal oleh oknum yang tidak berwenang, yang kemudian menyebarkan informasi medis pribadi ke pihak luar. Peristiwa ini menunjukkan lemahnya sistem kontrol akses dan kurangnya pengawasan terhadap penggunaan sistem rekam medis elektronik (RME).
   (Sumber: CNN Indonesia, 2021; Detik.com, 2021)

   Dampak Kasus
   1. Kehilangan Kepercayaan Pasien: Pasien enggan memberikan data sensitif karena khawatir akan disebarluaskan tanpa izin.
   2. Reputasi Rumah Sakit Tercoreng: Kasus ini menurunkan kredibilitas lembaga kesehatan di mata publik.
   3. Masalah Hukum: Rumah sakit dapat dikenai sanksi berdasarkan Undang-Undang Perlindungan Data Pribadi (UU PDP No. 27 Tahun 2022).
   4. Dampak Psikologis Pasien: Pasien dengan penyakit sensitif seperti HIV mengalami tekanan sosial akibat penyebaran data medis.

   Langkah-Langkah Pencegahan

   1. Penerapan Kontrol Akses Berbasis Peran (Role-Based Access Control – RBAC):
   Hanya staf dengan jabatan dan tanggung jawab tertentu yang diberi hak mengakses data pasien. Misalnya, dokter spesialis hanya dapat melihat data medis pasien yang sedang dirawat olehnya, sementara staf administrasi hanya dapat melihat identitas dasar pasien.

   2. Audit Log Sistem:
   Rumah sakit harus mencatat setiap aktivitas pengguna di sistem, termasuk waktu akses, data yang diakses, dan perangkat yang digunakan. Ini membantu melacak pelaku jika terjadi pelanggaran.

   3. Autentikasi Multi-Faktor (MFA):
   Untuk masuk ke sistem RME, pengguna wajib melewati lebih dari satu lapisan keamanan, seperti kombinasi password dan kode OTP (One-Time Password).

4. Pelatihan Etika dan Keamanan Data:
   Staf perlu dilatih secara berkala tentang pentingnya menjaga kerahasiaan data pasien sesuai Kode Etik Kedokteran dan regulasi keamanan informasi.
5. Penerapan Sanksi Tegas:
   Rumah sakit harus memiliki kebijakan disipliner terhadap pelanggaran akses data, mulai dari peringatan hingga pemutusan hubungan kerja.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Apa yang dimaksud dengan kontrol akses berbasis peran (RBAC) dan bagaimana hal ini diterapkan di rumah sakit?**
   - Kontrol Akses Berbasis Peran (RBAC) adalah mekanisme keamanan yang membatasi akses pengguna berdasarkan peran dan tanggung jawab mereka di organisasi.

   Di rumah sakit, RBAC diterapkan dengan cara:

   - Dokter memiliki akses penuh terhadap riwayat medis pasien.
   - Perawat hanya dapat melihat rencana perawatan dan hasil observasi pasien.
   - Staf administrasi hanya mengakses data non-medis seperti identitas pasien dan tagihan.

   Dengan sistem ini, data sensitif tidak dapat diakses oleh pihak yang tidak berkepentingan, sehingga mengurangi risiko kebocoran internal.

2. **Mengapa autentikasi multi-faktor penting dalam menjaga keamanan data medis?**
   Autentikasi Multi-Faktor (MFA) penting karena menambahkan lapisan perlindungan tambahan selain kata sandi. Jika satu faktor (misalnya password) bocor, sistem tetap aman karena membutuhkan verifikasi tambahan seperti:
   - Kode OTP yang dikirim ke ponsel,
   - Sidik jari atau pengenalan wajah,
   - Token keamanan digital.
     Dengan MFA, risiko akses ilegal akibat pencurian kata sandi atau phishing dapat ditekan secara signifikan. Dalam konteks rumah sakit, ini sangat penting karena data pasien bersifat sensitif dan dilindungi oleh hukum.

REFERENSI

CNN Indonesia. (2021, September 17). Data pasien HIV bocor, Kemenkes minta RS perkuat sistem keamanan. https://www.cnnindonesia.com/teknologi/20210917103033-192-695183/data-pasien-hiv-bocor-kemenkes-minta-rs-perkuat-sistem-keamanan

Detik.com. (2021, September 18). Kebocoran data pasien HIV di RS Surabaya, diduga akibat akses internal. https://news.detik.com/berita/d-5742785/kebocoran-data-pasien-hiv-di-rs-surabaya-diduga-akibat-akses-internal

Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan No. 24 Tahun 2022 tentang Rekam Medis Elektronik. Jakarta: Kemenkes RI. https://peraturan.bpk.go.id/Details/243526/permenkes-no-24-tahun-2022

Maimunah, S., & Hartono, B. (2023). Implementasi kontrol akses berbasis peran dalam sistem informasi rekam medis. Jurnal Manajemen Informasi Kesehatan Indonesia, 11(1), 45–54. https://doi.org/10.33560/jmiki.v11i1.302

Rahmawati, D., & Sari, R. (2022). Perlindungan data pasien pada sistem rekam medis elektronik di Indonesia. Jurnal Ilmiah Kesehatan Masyarakat, 7(3), 88–95. https://doi.org/10.14710/jikm.v7i3.325

MATERI 7

ENKRIPSI DATA KESEHATAN

STUDI KASUS ATAU ANALISIS DATA

1. **Analisis Kasus Kebocoran Data Tanpa Enkripsi**
   Salah satu kasus yang terjadi di Indonesia adalah kebocoran data pasien di salah satu rumah sakit swasta di Jakarta pada tahun 2022, di mana data pasien yang tersimpan di sistem rekam medis elektronik (RME) bocor ke publik karena tidak adanya sistem enkripsi pada database. Akibat insiden tersebut, data pribadi seperti nama, NIK, riwayat penyakit, dan hasil laboratorium pasien tersebar di forum daring.

   Rumah sakit tersebut kemudian melakukan evaluasi menyeluruh terhadap kebijakan keamanan informasinya. Langkah pertama yang diambil adalah mengimplementasikan enkripsi Advanced Encryption Standard (AES-256) untuk melindungi data pasien dalam penyimpanan (data at rest) dan saat transmisi (data in transit). Selain itu, dilakukan pembaruan kebijakan akses, audit keamanan rutin, serta pelatihan keamanan bagi staf IT dan petugas rekam medis.

   Penerapan AES-256, yang dikenal memiliki tingkat keamanan tinggi, terbukti efektif dalam melindungi data dari akses tidak sah dan mencegah kebocoran ulang. Rumah sakit juga mulai mengadopsi sistem manajemen keamanan informasi (ISMS) sesuai standar ISO/IEC 27001:2013 untuk memastikan keamanan data yang berkelanjutan.

2. **Analisis Keberhasilan Penggunaan Enkripsi di Rumah Sakit**
   Sebaliknya, Rumah Sakit Jantung dan Pembuluh Darah Harapan Kita (RSJPDHK) merupakan contoh positif dari penerapan keamanan data melalui enkripsi end-to-end. Berdasarkan laporan Kementerian Kesehatan (2023), RSJPDHK berhasil mempertahankan keamanan data pasien meskipun mengalami percobaan serangan siber berupa phishing dan akses ilegal pada server.

   Hal ini terjadi karena rumah sakit telah mengimplementasikan enkripsi end-to-end (E2EE) pada sistem RME dan komunikasi internal. Dengan teknologi ini, data pasien dienkripsi sejak awal pengiriman hingga penerimaan, sehingga tidak dapat dibaca oleh pihak ketiga meskipun jaringan diretas.

   Keberhasilan RSJPDHK ini menjadi contoh penerapan prinsip keamanan berlapis (defense in depth) yang efektif dalam menjaga kerahasiaan dan integritas data medis di Indonesia.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Jelaskan perbedaan antara enkripsi simetris dan enkripsi asimetris serta keuntungannya dalam perlindungan data medis.**
   1. Enkripsi Simetris menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi. Contohnya adalah algoritma AES (Advanced Encryption Standard).
      - Keuntungan: cepat dan efisien untuk mengenkripsi data dalam jumlah besar seperti database pasien.
      - Kelemahan: risiko tinggi jika kunci tunggal bocor.
   2. Enkripsi Asimetris menggunakan dua kunci berbeda, yaitu kunci publik (public key) untuk enkripsi dan kunci privat (private key) untuk dekripsi. Contohnya adalah algoritma RSA (Rivest–Shamir–Adleman).
      - Keuntungan: lebih aman dalam proses pertukaran data antar sistem karena kunci privat tidak pernah dibagikan.
      - Kelemahan: prosesnya lebih lambat dibandingkan enkripsi simetris.

   Dalam konteks rumah sakit, kombinasi keduanya (hybrid encryption) sering digunakan misalnya, RSA digunakan untuk mengamankan kunci AES, sedangkan AES digunakan untuk mengenkripsi data pasien. Hal ini memberikan keseimbangan antara keamanan dan efisiensi.

2. **Mengapa enkripsi end-to-end penting untuk aplikasi mobile yang mengelola data medis pasien?**

   Enkripsi end-to-end (E2EE) sangat penting dalam aplikasi mobile kesehatan karena:
   - Menjamin kerahasiaan data pasien, bahkan dari penyedia layanan aplikasi sekalipun.
   - Mencegah serangan man-in-the-middle, di mana penyerang mencoba mencegat komunikasi antara dokter dan pasien.
   - Menjaga integritas data, sehingga informasi medis tidak dapat dimodifikasi tanpa izin.
   - Mendukung kepatuhan terhadap regulasi, seperti Peraturan Menteri Kesehatan No. 24 Tahun 2022 tentang Rekam Medis Elektronik dan GDPR di Eropa.

   Dengan E2EE, data pasien hanya bisa dibuka oleh pihak yang berhak (misalnya dokter dan pasien), sementara server hanya berfungsi sebagai perantara penyimpanan terenkripsi.

REFERENSI

Kementerian Kesehatan Republik Indonesia. (2023). Laporan Tahunan Keamanan Data Rumah Sakit Indonesia 2023. Jakarta: Pusat Data dan Informasi Kemenkes.

National Institute of Standards and Technology. (2020). Advanced Encryption Standard (AES) – FIPS Publication 197. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

Sari, R. D., & Pratama, A. (2022). Analisis Implementasi Enkripsi Data pada Sistem Rekam Medis Elektronik Rumah Sakit di Indonesia. Jurnal Teknologi Informasi Kesehatan, 8(2), 45–53. https://doi.org/10.32783/jtik.v8i2.1123

Setiawan, M. (2022). Kasus Kebocoran Data Pasien di Rumah Sakit Swasta Jakarta dan Upaya Pencegahannya. Kompas.com. https://www.kompas.com/tren/read/2022/09/14/190000465/kebocoran-data-pasien-di-rumah-sakit-swasta

Widodo, D. A., & Nugraha, T. (2023). Perlindungan Data Pasien melalui Enkripsi End-to-End pada Aplikasi Mobile Kesehatan. Jurnal Keamanan Informasi dan Kesehatan Digital, 5(1), 22–31. https://doi.org/10.31537/jkikd.v5i1.154

MATERI 8

AUDIT DAN MONITORING KEAMANAN DATA

STUDI KASUS ATAU ANALISIS DATA

1. **Kasus Pelanggaran Data Akibat Tidak Dilakukannya Audit dan Pemantauan Sistem**

   Ketiadaan audit rutin dan pemantauan sistem keamanan pada rumah sakit dapat menyebabkan terjadinya pelanggaran data yang tidak terdeteksi dalam jangka waktu lama. Audit sistem informasi kesehatan berfungsi sebagai mekanisme pengendalian internal untuk memastikan bahwa seluruh aktivitas akses dan pengelolaan data berjalan sesuai dengan kebijakan serta standar keamanan yang berlaku. Tanpa audit, aktivitas tidak sah seperti akses ilegal, pencurian data, maupun penyalahgunaan hak akses oleh pihak internal maupun eksternal sulit untuk diidentifikasi.

   Dalam kasus ini, kebocoran data baru diketahui setelah data pasien dicuri oleh pihak luar. Hal tersebut menunjukkan lemahnya sistem pengawasan dan rendahnya kesiapan rumah sakit dalam menghadapi ancaman siber. Padahal, data rekam medis memiliki sifat sangat sensitif karena memuat identitas pasien, riwayat penyakit, hasil pemeriksaan, serta informasi lainnya yang dilindungi oleh hukum. Kebocoran data tidak hanya berdampak pada kerugian pasien, tetapi juga dapat menurunkan reputasi rumah sakit serta menimbulkan konsekuensi hukum dan administratif.

   Sesuai dengan Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis, fasilitas pelayanan kesehatan wajib menjamin keamanan, kerahasiaan, dan keutuhan data rekam medis. Oleh karena itu, tidak dilaksanakannya audit dan pemantauan sistem merupakan bentuk kelalaian dalam memenuhi kewajiban tersebut.

2. **Keberhasilan Penggunaan Pemantauan Jaringan dalam Mendeteksi Ancaman**

   Berbeda dengan kasus sebelumnya, rumah sakit yang menerapkan pemantauan jaringan secara aktif mampu mendeteksi dan mencegah serangan Distributed Denial of Service (DDoS) yang mengancam integritas dan ketersediaan sistem Rekam Medis Elektronik (RME). Pemantauan jaringan memungkinkan identifikasi dini terhadap pola lalu lintas yang tidak normal, sehingga tindakan mitigasi dapat segera dilakukan sebelum sistem mengalami gangguan serius.

   Keberhasilan ini menunjukkan bahwa pemantauan jaringan berperan sebagai sistem peringatan dini (early warning system) dalam keamanan informasi. Selain melindungi sistem dari gangguan operasional, pemantauan jaringan juga menjaga kesinambungan layanan kesehatan. Dalam konteks rumah sakit, gangguan sistem RME dapat berdampak langsung terhadap proses pelayanan medis dan keselamatan pasien.

Dengan demikian, penerapan pemantauan jaringan secara berkelanjutan merupakan langkah strategis dalam mewujudkan sistem informasi kesehatan yang andal, aman, dan sesuai dengan standar nasional maupun internasional.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Apa yang dimaksud dengan audit trail dan bagaimana perannya dalam mendeteksi ancaman terhadap data medis?**
   Audit trail adalah catatan kronologis yang merekam seluruh aktivitas pengguna dalam sistem informasi, meliputi waktu akses, identitas pengguna, jenis aktivitas, serta perubahan yang dilakukan terhadap data. Dalam sistem rekam medis elektronik, audit trail berfungsi sebagai alat pengawasan dan pengendalian untuk memastikan bahwa data pasien hanya diakses oleh pihak yang berwenang.

   Peran audit trail dalam mendeteksi ancaman sangat penting karena memungkinkan rumah sakit untuk melacak aktivitas mencurigakan, seperti akses data di luar jam kerja, perubahan data tanpa otorisasi, atau upaya login berulang yang gagal. Selain sebagai alat deteksi, audit trail juga berfungsi sebagai bukti dalam proses investigasi insiden keamanan serta pemenuhan aspek hukum dan kepatuhan regulasi.

2. **Mengapa pemantauan jaringan sangat penting untuk keamanan data rumah sakit?**
   Pemantauan jaringan merupakan komponen penting dalam sistem keamanan informasi rumah sakit karena sebagian besar ancaman siber dapat teridentifikasi melalui anomali lalu lintas jaringan. Serangan seperti DDoS, malware, dan penyusupan sistem umumnya menunjukkan pola komunikasi yang tidak normal. Tanpa pemantauan, serangan tersebut berpotensi menimbulkan kerusakan sistem sebelum sempat ditangani.

   Selain itu, pemantauan jaringan mendukung pendekatan keamanan yang proaktif. Rumah sakit dapat mendeteksi ancaman sejak dini dan mengambil langkah pencegahan untuk meminimalkan risiko kebocoran data dan gangguan layanan. Hal ini sejalan dengan prinsip perlindungan data pasien yang menekankan kerahasiaan, integritas, dan ketersediaan informasi medis.

REFERENSI

Hatta, G. R. (2013). Pedoman manajemen informasi kesehatan di sarana pelayanan kesehatan. Jakarta: UI Press. https://lib.ui.ac.id/detail?id=20385625

ISO. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems. https://www.iso.org/standard/54534.html

Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. https://peraturan.bpk.go.id/Details/245372/permenkes-no-24-tahun-2022

Kumalahadi. (2018). Manajemen informasi kesehatan. Yogyakarta: Deepublish. https://deepublishstore.com/product/manajemen-informasi-kesehatan/

World Health Organization. (2016). Guidance on electronic health records security. https://www.who.int/publications/i/item/WHO-HIS-HIN-16.1

MATERI 9

KEBIJAKAN DAN PROSEDUR KEAMANAN DATA

STUDI KASUS ATAU ANALISIS DATA

1. **Analisis Kasus Pelanggaran Keamanan di Rumah Sakit:**
   Pelanggaran keamanan data di rumah sakit sering kali berakar pada lemahnya kebijakan dan prosedur perlindungan data. Rumah sakit yang tidak memiliki kebijakan keamanan data yang jelas dan terstandarisasi cenderung menghadapi risiko kebocoran data dalam skala besar. Kebijakan yang tidak memadai menyebabkan ketidakkonsistenan dalam pengelolaan akses data, lemahnya kontrol pengguna, serta kurangnya kesadaran staf terhadap pentingnya kerahasiaan informasi pasien.

   Dalam studi kasus kebocoran data besar-besaran, rumah sakit mengalami pencurian data rekam medis yang mencakup identitas pasien, diagnosis, dan informasi administratif. Dampak yang ditimbulkan tidak hanya berupa kerugian materiil, tetapi juga menurunnya kepercayaan masyarakat serta potensi tuntutan hukum. Hal ini menunjukkan bahwa kebocoran data bukan sekadar masalah teknis, melainkan kegagalan sistem manajemen keamanan informasi secara menyeluruh.

   Setelah insiden tersebut, rumah sakit mengambil sejumlah langkah perbaikan, antara lain menyusun ulang kebijakan keamanan data, memperketat pengendalian akses, melakukan pelatihan keamanan informasi bagi seluruh pegawai, serta mengimplementasikan sistem audit dan pemantauan berkala. Langkah-langkah ini menegaskan bahwa kebijakan keamanan data harus bersifat preventif dan berkelanjutan, bukan hanya diterapkan setelah terjadinya insiden.

2. **Keberhasilan Kebijakan Keamanan di Rumah Sakit Besar:**
   Berbeda dengan kasus sebelumnya, sebuah rumah sakit besar yang telah menerapkan kebijakan keamanan data secara komprehensif menunjukkan hasil yang signifikan dalam menurunkan risiko pelanggaran data. Kebijakan tersebut mencakup penggunaan otentikasi multi-faktor (multi-factor authentication), enkripsi data rekam medis, serta pembatasan akses berbasis peran (role-based access control).

   Penerapan otentikasi multi-faktor berhasil mencegah akses tidak sah meskipun terjadi kebocoran kata sandi, sementara enkripsi data memastikan bahwa informasi medis tetap tidak dapat dibaca oleh pihak yang tidak berwenang. Selain aspek teknis, rumah sakit juga menerapkan kebijakan edukasi dan pelatihan rutin bagi tenaga kesehatan dan staf administrasi terkait keamanan data.

Keberhasilan kebijakan ini berdampak langsung pada meningkatnya kepercayaan pasien terhadap layanan rumah sakit. Pasien merasa lebih aman karena data pribadinya dilindungi dengan sistem keamanan yang kuat. Hal ini menunjukkan bahwa kebijakan keamanan data yang efektif tidak hanya melindungi sistem informasi, tetapi juga menjadi bagian dari kualitas pelayanan kesehatan.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Mengapa kebijakan dan prosedur keamanan data sangat penting dalam sektor kesehatan?**
   Kebijakan dan prosedur keamanan data sangat penting dalam sektor kesehatan karena data medis bersifat sensitif dan dilindungi oleh hukum. Tanpa kebijakan yang jelas, pengelolaan data cenderung dilakukan secara tidak terstandar, sehingga meningkatkan risiko penyalahgunaan dan kebocoran informasi pasien.

   Selain itu, kebijakan keamanan data berfungsi sebagai pedoman bagi seluruh staf rumah sakit dalam mengelola, mengakses, dan melindungi data pasien. Kebijakan yang baik juga membantu rumah sakit memenuhi kewajiban regulasi, seperti yang diatur dalam Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis, serta standar internasional keamanan informasi. Dengan demikian, kebijakan keamanan data merupakan fondasi utama dalam menjaga kerahasiaan, integritas, dan ketersediaan data kesehatan.

2. **Bagaimana prosedur tanggap darurat dapat meminimalkan kerusakan akibat kebocoran data**
   Prosedur tanggap darurat berperan penting dalam meminimalkan dampak kebocoran data karena memungkinkan rumah sakit merespons insiden secara cepat dan terkoordinasi. Dengan adanya prosedur yang jelas, tim terkait dapat segera mengisolasi sistem yang terdampak, menghentikan akses tidak sah, serta mencegah penyebaran kerusakan lebih lanjut.

   Selain itu, prosedur tanggap darurat mencakup langkah pelaporan insiden, pemulihan sistem, serta evaluasi penyebab kebocoran. Prosedur ini juga membantu rumah sakit dalam memenuhi kewajiban pelaporan kepada pihak berwenang dan menjaga transparansi kepada pasien. Dengan respons yang cepat dan terstruktur, dampak kebocoran data dapat ditekan, baik dari sisi teknis, hukum, maupun reputasi institusi.

REFERENSI

Hatta, G. R. (2013). Pedoman manajemen informasi kesehatan di sarana pelayanan kesehatan. Jakarta: UI Press. https://lib.ui.ac.id/detail?id=20385625

ISO. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems. https://www.iso.org/standard/54534.html

Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. https://peraturan.bpk.go.id/Details/245372/permenkes-no-24-tahun-2022

Kumalahadi. (2018). Manajemen informasi kesehatan. Yogyakarta: Deepublish. https://deepublishstore.com/product/manajemen-informasi-kesehatan/

Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson. https://www.pearson.com/en-us/subject-catalog/p/computer-security-principles-and-practice/P200000003295

World Health Organization. (2016). Guidance on electronic health records security. https://www.who.int/publications/i/item/WHO-HIS-HIN-16.1

MATERI 10

PERLINDUNGAN DATA PRIBADI PASIEN

STUDI KASUS ATAU ANALISIS DATA

1. **Analisis Kasus Penyalahgunaan Data Pasien:**
   Kasus penyalahgunaan data pasien di rumah sakit umumnya terjadi akibat lemahnya penerapan prinsip perlindungan data dan kurangnya penghormatan terhadap hak pasien. Dalam beberapa kasus, rumah sakit menggunakan data rekam medis pasien untuk kepentingan penelitian, publikasi, atau tujuan lain tanpa memperoleh persetujuan yang jelas dari pasien. Praktik ini berujung pada pelanggaran etika dan hukum, sehingga rumah sakit dikenakan denda besar oleh otoritas yang berwenang.

   Penyalahgunaan data tersebut menunjukkan bahwa rumah sakit gagal menerapkan prinsip transparansi dan akuntabilitas dalam pengelolaan data pasien. Data medis bukan sekadar sumber informasi, melainkan hak pribadi pasien yang dilindungi oleh peraturan perundang-undangan. Ketika data digunakan tanpa persetujuan, pasien kehilangan kendali atas informasi pribadinya, yang dapat berdampak pada kerugian psikologis, sosial, maupun ekonomi.

   Kasus ini menegaskan pentingnya penerapan kebijakan perlindungan data yang ketat serta mekanisme persetujuan (informed consent) yang jelas. Rumah sakit tidak hanya bertanggung jawab secara hukum, tetapi juga secara moral untuk memastikan bahwa setiap penggunaan data pasien dilakukan secara etis dan sesuai ketentuan yang berlaku.

2. **Keberhasilan Rumah Sakit dalam Melindungi Data Pribadi Pasien:**
   Sebaliknya, rumah sakit yang berhasil melindungi data pribadi pasien menunjukkan komitmen tinggi terhadap keamanan dan hak pasien. Penerapan teknologi enkripsi memastikan bahwa data medis tidak dapat diakses atau dibaca oleh pihak yang tidak berwenang, meskipun terjadi pelanggaran sistem. Selain itu, kontrol akses yang ketat, seperti pembatasan hak akses berdasarkan peran, membantu mencegah penyalahgunaan data oleh pihak internal.

   Keberhasilan tersebut juga ditunjang oleh kebijakan yang memberikan hak penuh kepada pasien atas data medis mereka, termasuk hak untuk mengetahui, mengakses, dan memberikan persetujuan atas penggunaan data. Pendekatan ini menciptakan hubungan yang lebih transparan antara rumah sakit dan pasien, serta meningkatkan kepercayaan terhadap layanan kesehatan.

   Dengan menggabungkan aspek teknologi, kebijakan, dan kesadaran sumber daya manusia, rumah sakit mampu menciptakan sistem perlindungan data yang tidak hanya aman secara teknis, tetapi juga menghormati hak pasien sebagai pemilik data.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Apa saja hak-hak yang dimiliki oleh pasien terkait data pribadi mereka, dan bagaimana rumah sakit dapat melindunginya?**
   Pasien memiliki sejumlah hak terkait data pribadi medis, antara lain hak atas kerahasiaan data, hak untuk mengakses informasi medis, hak untuk memperoleh penjelasan mengenai penggunaan data, serta hak untuk memberikan atau menolak persetujuan atas pemanfaatan data tersebut. Hak-hak ini menegaskan bahwa data medis merupakan milik pasien, sementara rumah sakit hanya bertindak sebagai pengelola data.

   Rumah sakit dapat melindungi hak-hak tersebut dengan menerapkan kebijakan perlindungan data yang jelas, menggunakan sistem keamanan teknologi seperti enkripsi dan audit trail, serta memberikan edukasi kepada tenaga kesehatan mengenai etika dan hukum kerahasiaan data pasien. Dengan langkah tersebut, rumah sakit tidak hanya memenuhi kewajiban regulasi, tetapi juga menjaga kepercayaan pasien.

2. **Mengapa penting bagi rumah sakit untuk mendapatkan persetujuan pasien sebelum menggunakan data medis mereka?**
   Persetujuan pasien sebelum penggunaan data medis sangat penting karena merupakan bentuk penghormatan terhadap hak otonomi pasien. Informed consent memastikan bahwa pasien mengetahui tujuan, manfaat, dan risiko dari penggunaan data medis mereka, serta memiliki kebebasan untuk menyetujui atau menolak.

   Tanpa persetujuan, penggunaan data medis dapat dianggap sebagai pelanggaran privasi dan hak asasi pasien. Selain berisiko menimbulkan sanksi hukum, praktik tersebut juga dapat merusak hubungan kepercayaan antara pasien dan rumah sakit. Oleh karena itu, persetujuan pasien merupakan prinsip fundamental dalam pengelolaan data medis yang etis, legal, dan profesional.

REFERENSI

Hatta, G. R. (2013). Pedoman manajemen informasi kesehatan di sarana pelayanan kesehatan. Jakarta: UI Press. https://lib.ui.ac.id/detail?id=20385625

Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. https://peraturan.bpk.go.id/Details/245372/permenkes-no-24-tahun-2022

Kumalahadi. (2018). Manajemen informasi kesehatan. Yogyakarta: Deepublish. https://deepublishstore.com/product/manajemen-informasi-kesehatan/

OECD. (2013). OECD guidelines on the protection of privacy and transborder flows of personal data. https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

World Health Organization. (2016). Guidance on electronic health records security. https://www.who.int/publications/i/item/WHO-HIS-HIN-16.1

MATERI 11

KEAMANAN DATA DI CLOUD UNTUK INFORMASI KESEHATAN

STUDI KASUS ATAU ANALISIS DATA

1. **Analisis Kasus Kebocoran Data di Cloud:**
   Pemanfaatan cloud computing di rumah sakit memberikan banyak keuntungan, namun juga menimbulkan risiko apabila tidak diimbangi dengan sistem keamanan yang memadai. Salah satu kasus yang sering terjadi adalah kebocoran data medis pasien akibat kelemahan enkripsi yang diterapkan oleh penyedia layanan cloud. Dalam kasus ini, data rekam medis pasien dapat diakses oleh pihak tidak berwenang karena mekanisme perlindungan data tidak memenuhi standar keamanan yang seharusnya.

   Dampak kebocoran data di cloud sangat signifikan bagi rumah sakit. Selain merusak reputasi institusi dan menurunkan kepercayaan masyarakat, rumah sakit juga harus menanggung biaya pemulihan yang besar, termasuk perbaikan sistem, audit keamanan, serta potensi denda akibat pelanggaran regulasi perlindungan data. Kebocoran ini menunjukkan bahwa ketergantungan pada penyedia cloud tanpa pengawasan dan evaluasi keamanan yang ketat dapat menjadi celah serius dalam perlindungan data medis.

   Kasus tersebut menegaskan bahwa rumah sakit tetap bertanggung jawab atas keamanan data pasien, meskipun pengelolaan infrastruktur dilakukan oleh pihak ketiga. Oleh karena itu, pemilihan penyedia cloud harus mempertimbangkan standar enkripsi, kepatuhan terhadap regulasi, serta adanya perjanjian layanan (SLA) yang jelas terkait perlindungan data.

2. **Keberhasilan Penggunaan Cloud Computing di Rumah Sakit:**
   Sebaliknya, terdapat rumah sakit yang berhasil mengimplementasikan cloud computing secara aman dan efektif. Keberhasilan ini dicapai melalui penerapan enkripsi data yang kuat, baik saat data disimpan (data at rest) maupun saat ditransmisikan (data in transit), serta penerapan kontrol akses yang ketat berbasis peran pengguna.

   Dengan sistem keamanan yang baik, rumah sakit mampu meningkatkan efisiensi operasional, seperti kemudahan akses data rekam medis antar unit pelayanan dan percepatan proses pengambilan keputusan klinis. Selain itu, penggunaan cloud memungkinkan skalabilitas sistem dan penghematan biaya infrastruktur tanpa mengorbankan aspek keamanan data.

Keberhasilan ini menunjukkan bahwa cloud computing dapat menjadi solusi yang aman dan andal bagi sektor kesehatan, asalkan diimplementasikan dengan kebijakan keamanan yang tepat, pengawasan berkelanjutan, serta komitmen terhadap perlindungan data pasien.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Mengapa enkripsi end-to-end sangat penting dalam penyimpanan data medis di cloud?**
   Enkripsi end-to-end sangat penting dalam penyimpanan data medis di cloud karena memastikan bahwa data hanya dapat dibaca oleh pihak yang berwenang. Dengan enkripsi ini, data dilindungi sejak dikirim dari sistem rumah sakit hingga disimpan di cloud, sehingga meskipun terjadi kebocoran atau peretasan, data tetap tidak dapat dimanfaatkan oleh pihak yang tidak memiliki kunci enkripsi.

   Dalam konteks data medis yang bersifat sangat sensitif, enkripsi end-to-end menjadi lapisan perlindungan utama untuk menjaga kerahasiaan dan integritas informasi pasien. Penerapan enkripsi ini juga membantu rumah sakit memenuhi standar keamanan dan regulasi perlindungan data yang berlaku. Enkripsi end-to-end sangat penting dalam penyimpanan data medis di cloud karena memastikan bahwa data hanya dapat dibaca oleh pihak yang berwenang. Dengan enkripsi ini, data dilindungi sejak dikirim dari sistem rumah sakit hingga disimpan di cloud, sehingga meskipun terjadi kebocoran atau peretasan, data tetap tidak dapat dimanfaatkan oleh pihak yang tidak memiliki kunci enkripsi.

   Dalam konteks data medis yang bersifat sangat sensitif, enkripsi end-to-end menjadi lapisan perlindungan utama untuk menjaga kerahasiaan dan integritas informasi pasien. Penerapan enkripsi ini juga membantu rumah sakit memenuhi standar keamanan dan regulasi perlindungan data yang berlaku.

2. **Jelaskan bagaimana kontrol akses berbasis peran (RBAC) dapat meningkatkan keamanan data di cloud?**
   Kontrol akses berbasis peran (Role-Based Access Control/RBAC) meningkatkan keamanan data di cloud dengan membatasi akses pengguna sesuai dengan tugas dan tanggung jawabnya. Dalam sistem rumah sakit, tenaga medis hanya dapat mengakses data yang relevan dengan perannya, sementara staf administrasi memiliki akses terbatas sesuai kebutuhan kerja.

   Dengan RBAC, risiko penyalahgunaan data oleh pihak internal dapat diminimalkan karena tidak semua pengguna memiliki akses penuh terhadap seluruh data medis. Selain itu, RBAC memudahkan pengelolaan hak akses dan meningkatkan akuntabilitas, karena setiap aktivitas pengguna dapat dilacak berdasarkan peran yang dimilikinya.

3. **Apa tantangan terbesar yang dihadapi sektor kesehatan dalam mengimplementasikan solusi cloud computing?**
   Tantangan terbesar dalam implementasi cloud computing di sektor kesehatan adalah aspek keamanan dan kepatuhan regulasi. Data medis memiliki tingkat sensitivitas yang tinggi, sehingga rumah sakit harus memastikan bahwa penyedia cloud memenuhi standar keamanan dan peraturan yang berlaku. Selain itu, masih terdapat keterbatasan sumber daya manusia yang memahami keamanan cloud secara mendalam.

   Tantangan lainnya meliputi kekhawatiran terhadap privasi data, ketergantungan pada pihak ketiga, serta integrasi sistem cloud dengan sistem informasi rumah sakit yang sudah ada. Oleh karena itu, implementasi cloud computing memerlukan perencanaan matang, kebijakan keamanan yang jelas, serta pengawasan berkelanjutan agar manfaat teknologi dapat diperoleh tanpa mengorbankan perlindungan data pasien.

REFERENSI

Hatta, G. R. (2013). Pedoman manajemen informasi kesehatan di sarana pelayanan kesehatan. Jakarta: UI Press. https://lib.ui.ac.id/detail?id=20385625

ISO. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems. https://www.iso.org/standard/54534.html

Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. https://peraturan.bpk.go.id/Details/245372/permenkes-no-24-tahun-2022

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

World Health Organization. (2016). Guidance on electronic health records security. https://www.who.int/publications/i/item/WHO-HIS-HIN-16.1

MATERI 12

TEKNOLOGI BLOCKCHAIN DALAM PERLINDUNGAN DATA KESEHATAN

STUDI KASUS ATAU ANALISIS DATA

1. **Keberhasilan Implementasi Blockchain di Rumah Sakit:**
   Penerapan teknologi blockchain di rumah sakit menunjukkan potensi besar dalam meningkatkan keamanan dan transparansi pengelolaan data medis. Dengan karakteristik blockchain yang bersifat terdistribusi, tidak dapat diubah (immutable), dan transparan, setiap transaksi atau akses terhadap data rekam medis dapat tercatat secara permanen dan sulit dimanipulasi. Hal ini secara signifikan mengurangi risiko pemalsuan dan penyalahgunaan data pasien.

   Keberhasilan implementasi blockchain juga berdampak pada efisiensi administrasi rumah sakit. Proses pertukaran data antar unit pelayanan atau antar fasilitas kesehatan menjadi lebih cepat dan aman, sehingga mengurangi biaya operasional yang sebelumnya timbul akibat duplikasi data dan prosedur administratif yang kompleks. Selain itu, pasien memperoleh akses yang lebih transparan terhadap data medis mereka, sehingga meningkatkan rasa percaya dan kepuasan terhadap layanan kesehatan.

   Dengan sistem blockchain, pasien tidak lagi diposisikan sebagai objek data, melainkan sebagai pemilik data yang memiliki kendali atas siapa saja yang dapat mengakses informasi medisnya. Pendekatan ini sejalan dengan prinsip perlindungan data dan hak pasien dalam pelayanan kesehatan modern.

2. **Analisis Potensi Keuntungan dan Tantangan Blockchain dalam Kesehatan:**
   Meskipun menawarkan tingkat keamanan yang tinggi, penerapan blockchain di sektor kesehatan tidak terlepas dari berbagai tantangan. Salah satu keuntungan utama blockchain adalah kemampuannya menjamin integritas dan keaslian data medis, karena setiap perubahan data harus melalui mekanisme konsensus yang ketat. Hal ini sangat relevan dalam konteks rekam medis elektronik yang menuntut keakuratan dan keandalan informasi.

   Namun, tantangan utama dalam implementasi blockchain adalah tingginya biaya awal, termasuk investasi infrastruktur, pengembangan sistem, dan pelatihan sumber daya manusia. Selain itu, masih diperlukan edukasi kepada pasien agar memahami cara kerja dan manfaat teknologi blockchain, terutama terkait pengelolaan hak akses data.

Keterbatasan adopsi teknologi oleh penyedia layanan kesehatan juga menjadi kendala. Tidak semua rumah sakit memiliki kesiapan teknis dan organisasi untuk mengintegrasikan blockchain ke dalam sistem informasi yang sudah ada. Oleh karena itu, penerapan blockchain perlu dilakukan secara bertahap dengan dukungan kebijakan, regulasi, dan kesiapan SDM yang memadai.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Apa keuntungan menggunakan teknologi blockchain dalam pengelolaan rekam medis elektronik pasien?**
   Penggunaan teknologi blockchain dalam pengelolaan rekam medis elektronik memberikan sejumlah keuntungan, antara lain peningkatan keamanan data melalui mekanisme kriptografi, transparansi akses data, serta jaminan integritas informasi medis. Blockchain memungkinkan pencatatan aktivitas akses dan perubahan data secara permanen, sehingga memudahkan proses audit dan pelacakan insiden keamanan.

   Selain itu, blockchain memberikan kontrol yang lebih besar kepada pasien atas data medis mereka. Pasien dapat menentukan pihak mana saja yang berhak mengakses data, sehingga risiko penyalahgunaan informasi dapat diminimalkan. Keuntungan lainnya adalah meningkatnya interoperabilitas antar sistem kesehatan, karena blockchain memungkinkan pertukaran data yang aman dan terstandar.

2. **Jelaskan bagaimana smart contracts dapat diterapkan di sektor kesehatan untuk melindungi data pasien.**
   Smart contracts merupakan program otomatis yang berjalan di atas blockchain dan dapat diterapkan untuk mengatur akses serta penggunaan data medis pasien. Dalam sektor kesehatan, smart contracts dapat digunakan untuk memastikan bahwa data pasien hanya dapat diakses oleh pihak yang telah memperoleh persetujuan dari pasien.

   Sebagai contoh, smart contracts dapat mengatur bahwa data rekam medis hanya dapat dibuka oleh dokter tertentu dalam jangka waktu tertentu dan untuk tujuan tertentu. Setelah masa akses berakhir, sistem secara otomatis menutup akses tanpa campur tangan pihak lain. Dengan mekanisme ini, perlindungan data pasien menjadi lebih terjamin, transparan, dan akuntabel.

   Penerapan smart contracts juga mengurangi ketergantungan pada proses manual, sehingga meminimalkan kesalahan manusia dan meningkatkan efisiensi pengelolaan data medis.

REFERENSI

Hatta, G. R. (2013). Pedoman manajemen informasi kesehatan di sarana pelayanan kesehatan. Jakarta: UI Press. https://lib.ui.ac.id/detail?id=20385625

Kumalahadi. (2018). Manajemen informasi kesehatan. Yogyakarta: Deepublish. https://deepublishstore.com/product/manajemen-informasi-kesehatan/

Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. https://peraturan.bpk.go.id/Details/245372/permenkes-no-24-tahun-2022

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. Healthcare, 7(2), 56. https://doi.org/10.3390/healthcare7020056

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. Proceedings of the 2nd International Conference on Open and Big Data. https://ieeexplore.ieee.org/document/7573685

World Health Organization. (2016). Guidance on electronic health records security. https://www.who.int/publications/i/item/WHO-HIS-HIN-16.1

MATERI 13

KEAMANAN DATA PADA SISTEM REKAM MEDIS ELEKTRONIK (RME)

STUDI KASUS ATAU ANALISIS DATA

1. **Kasus Kebocoran Data RME di Rumah Sakit:**
   Kebocoran data Rekam Medis Elektronik (RME) di rumah sakit umumnya disebabkan oleh lemahnya penerapan kontrol akses terhadap sistem informasi kesehatan. Dalam studi kasus ini, rumah sakit mengalami kebocoran data pasien akibat penggunaan akun bersama, kata sandi yang lemah, serta tidak adanya pembatasan akses berdasarkan peran pengguna. Kondisi tersebut memungkinkan pihak yang tidak berwenang mengakses dan menyalin data medis pasien.

   Setelah insiden kebocoran terjadi, rumah sakit melakukan evaluasi menyeluruh terhadap sistem keamanannya. Langkah perbaikan yang dilakukan meliputi penerapan otentikasi dua faktor (two-factor authentication), penetapan kebijakan kata sandi yang lebih kuat, serta pelaksanaan audit sistem secara rutin. Audit ini bertujuan untuk memantau aktivitas pengguna dan mendeteksi potensi ancaman sejak dini.

   Langkah-langkah tersebut menunjukkan bahwa perbaikan sistem keamanan tidak hanya berfokus pada teknologi, tetapi juga pada tata kelola dan pengawasan yang berkelanjutan. Dengan penerapan kontrol akses yang tepat, risiko kebocoran data RME dapat ditekan secara signifikan.

2. **Keberhasilan Pengelolaan Keamanan Data di Rumah Sakit dengan RME:**
   Berbeda dengan kasus sebelumnya, terdapat rumah sakit yang berhasil mengelola keamanan data RME dengan tingkat perlindungan yang tinggi. Rumah sakit ini menerapkan enkripsi penuh terhadap data pasien, baik saat data disimpan maupun saat ditransmisikan antar sistem. Selain itu, otentikasi multi-faktor diterapkan untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses sistem RME.

   Pengawasan sistem dilakukan secara ketat melalui pemantauan aktivitas pengguna dan audit keamanan berkala. Setiap akses dan perubahan data tercatat dalam audit trail, sehingga memudahkan proses penelusuran apabila terjadi aktivitas mencurigakan. Pendekatan ini tidak hanya melindungi data pasien dari akses tidak sah, tetapi juga meningkatkan kepercayaan pasien terhadap layanan rumah sakit.

   Keberhasilan ini menunjukkan bahwa pengelolaan keamanan RME yang komprehensif mampu menjaga kerahasiaan, integritas, dan ketersediaan data medis secara optimal.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Mengapa penting untuk mengenkripsi data yang disimpan dalam sistem RME?**
   Enkripsi data dalam sistem RME sangat penting karena data medis merupakan informasi yang bersifat rahasia dan sensitif. Enkripsi memastikan bahwa data yang tersimpan tidak dapat dibaca atau digunakan oleh pihak yang tidak memiliki otorisasi, meskipun terjadi kebocoran atau akses ilegal terhadap sistem.

   Selain melindungi kerahasiaan data, enkripsi juga menjaga integritas informasi medis dengan mencegah perubahan data tanpa izin. Penerapan enkripsi dalam RME membantu rumah sakit memenuhi standar keamanan dan regulasi perlindungan data kesehatan yang berlaku.

2. **Bagaimana penggunaan RBAC dapat membantu melindungi data pasien dalam RME?**
   Role-Based Access Control (RBAC) berperan penting dalam melindungi data pasien dalam sistem RME dengan membatasi akses pengguna berdasarkan peran dan tanggung jawabnya. Tenaga medis hanya dapat mengakses data pasien yang relevan dengan tugas klinisnya, sementara staf administrasi memiliki akses terbatas sesuai kebutuhan kerja.

   Dengan RBAC, risiko penyalahgunaan data oleh pihak internal dapat diminimalkan karena tidak semua pengguna memiliki hak akses penuh terhadap seluruh data pasien. Selain itu, RBAC meningkatkan akuntabilitas karena setiap aktivitas pengguna dapat ditelusuri berdasarkan peran yang dimilikinya, sehingga mendukung pengawasan dan audit keamanan sistem.

REFERENSI

Hatta, G. R. (2013). Pedoman manajemen informasi kesehatan di sarana pelayanan kesehatan. Jakarta: UI Press. https://lib.ui.ac.id/detail?id=20385625

Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. https://peraturan.bpk.go.id/Details/245372/permenkes-no-24-tahun-2022

Kumalahadi. (2018). Manajemen informasi kesehatan. Yogyakarta: Deepublish. https://deepublishstore.com/product/manajemen-informasi-kesehatan/

ISO. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems. https://www.iso.org/standard/54534.html

World Health Organization. (2016). Guidance on electronic health records security. https://www.who.int/publications/i/item/WHO-HIS-HIN-16.1

MATERI 14

TINJAUAN AKHIR DAN IMPLEMENTASI KEAMANAN DATA KESEHATAN

STUDI KASUS ATAU ANALISIS DATA

1. **Keberhasilan Implementasi Sistem Keamanan di Rumah Sakit:**
   Keberhasilan rumah sakit dalam melindungi data pasien sangat dipengaruhi oleh penerapan kebijakan keamanan informasi yang ketat dan terintegrasi. Dalam studi kasus ini, rumah sakit menerapkan kebijakan keamanan data yang jelas, mencakup pengaturan akses data, penggunaan teknologi keamanan, serta pengawasan berkelanjutan terhadap sistem informasi kesehatan.

   Penerapan teknologi enkripsi memastikan bahwa data medis pasien terlindungi baik saat disimpan maupun saat ditransmisikan. Selain itu, penggunaan otentikasi multi-faktor memperkuat proses verifikasi identitas pengguna sehingga hanya pihak yang berwenang yang dapat mengakses sistem. Kontrol akses berbasis peran (Role-Based Access Control/RBAC) juga diterapkan untuk membatasi hak akses pengguna sesuai dengan tugas dan tanggung jawabnya.

   Kombinasi kebijakan dan teknologi tersebut terbukti efektif dalam menurunkan risiko kebocoran data serta meningkatkan kepercayaan pasien terhadap layanan rumah sakit. Keberhasilan ini menunjukkan bahwa keamanan data medis bukan hanya tanggung jawab unit teknologi informasi, tetapi merupakan bagian dari tata kelola rumah sakit secara keseluruhan.

LATIHAN ATAU PERTANYAAN REFLEKSI

1. **Apa yang dapat dilakukan rumah sakit untuk mengurangi risiko kebocoran data medis pasien?**
   Untuk mengurangi risiko kebocoran data medis pasien, rumah sakit dapat menerapkan sejumlah langkah strategis, antara lain menyusun dan menerapkan kebijakan keamanan data yang jelas dan konsisten, melakukan pelatihan rutin kepada tenaga kesehatan dan staf terkait keamanan informasi, serta menerapkan teknologi pengamanan seperti enkripsi dan kontrol akses yang ketat.

   Selain itu, rumah sakit perlu melakukan audit sistem secara berkala untuk mendeteksi potensi kelemahan keamanan sejak dini. Pemantauan aktivitas pengguna dan pencatatan audit trail juga penting untuk memastikan akuntabilitas dan memudahkan penelusuran apabila terjadi insiden keamanan. Dengan pendekatan yang komprehensif, risiko kebocoran data dapat diminimalkan secara signifikan.

2. **Mengapa enkripsi dan autentikasi multi-faktor sangat penting dalam melindungi data medis pasien?**

   Enkripsi dan otentikasi multi-faktor merupakan komponen penting dalam sistem keamanan data medis pasien. Enkripsi berfungsi untuk melindungi kerahasiaan data dengan mengubah informasi menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang. Dengan enkripsi, data tetap aman meskipun terjadi kebocoran atau akses ilegal terhadap sistem.

   Sementara itu, otentikasi multi-faktor meningkatkan keamanan akses dengan mewajibkan pengguna untuk melalui lebih dari satu tahap verifikasi identitas. Hal ini secara signifikan mengurangi risiko penyalahgunaan akun akibat pencurian kata sandi. Kombinasi enkripsi dan otentikasi multi-faktor menciptakan lapisan perlindungan yang kuat dalam menjaga keamanan data medis pasien.

REFERENSI

Hatta, G. R. (2013). Pedoman manajemen informasi kesehatan di sarana pelayanan kesehatan. Jakarta: UI Press. https://lib.ui.ac.id/detail?id=20385625

Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. https://peraturan.bpk.go.id/Details/245372/permenkes-no-24-tahun-2022

Kumalahadi. (2018). Manajemen informasi kesehatan. Yogyakarta: Deepublish. https://deepublishstore.com/product/manajemen-informasi-kesehatan/

ISO. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems. https://www.iso.org/standard/54534.html

World Health Organization. (2016). Guidance on electronic health records security. https://www.who.int/publications/i/item/WHO-HIS-HIN-16.1