DASAR HUKUM

1. UU No. 8 tahun 1999 tentang Perlindungan Konsumen
2. UU No. 29 tahun 2004 tentang Praktik Kedokteran
3. UU No. 44 Tahun 2009 tentang Rumah Sakit
4. Permenkes No. 269/MENKES/PER/III/2008 tentang Rekam Medis

1. UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik
2. PP No. 82 tahun 2012 tentang Penyelenggaraan sistem dan Transaksi Elektronik
3. Perpres no. 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Eletronik
4. Peraturan Badan Siber dan Sandi Negara tentang Penyelenggaraan Sertifikasi Elektronik

TOP CYBER SECURITY THREATS

The most important cyber security concerns for healthcare providers and payers are coming from external sources, according to KPMG's survey of 223 healthcare executives, who named external attackers and third-parties as their top vulnerabilities. The top threats are malware and HIPAA violations. (See charts.)

HEALTHCARE SECTOR

GREATEST VULNERABILITIES IN DATA SECURITY

TOP INFORMATION SECURITY CONCERNS

What is?

PAPERLESS

1 Kg Kertas = 324 liter air

1 edisi NYTS = 75.000 pohon

93% kertas berasal dari pohon

1 ton Kertas :
- 683,5 galon minyak
- 26.500 liter air
- 17 pohon

- Kemudahan Akses Dokumen
- Hemat Waktu
- Simplifikasi Bisnis Proses
- Hemat Ruang
- Kepuasan Client
- Ramah Lingkungan
- Hemat SDM
- Minimalisir kerusakan
- Isu Keamanan?

Apa itu Rekam Medis Elektronik?

Penyimpanan informasi kesehatan pasien secara elektronik mengenai status dan layanan yang tersimpan sedemikian rupa untuk dapat digunakan sebagai rekam medik yang sah (Shortliffe – 2001)

Definisi Rekam Medis

berkas yang berisi catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lainnya yang telah diberikan kepada pasien

(PMK 269/2008 tentang Rekam Medis Pasal 1 ayat 1)

World

Australia

Ujicoba dimulai tahun 2004, dengan membu sistem rekam kesehat sehingga setiap ruma sakit dapat mengintegrasikan rek medis elektroniknya dengan sistem rekam kesehatan tersebut

Estonia

- **Menjadi negara pertam menerapkan rekam m elektronik yang terinte dengan sistem rekam secara nasional dari l meninggal.**
- **Ujicoba sejak tahun 2 mulai digunakan seca tahun 2008. Selain itu, juga telah menerapka tangan elektronik dala pendokumentasianny**

Canada dan Amerika Serikat

Menjadi pelopor pengembangan rekam medis elektronik. Walaupun awalnya adopsi rekam medis elektronik di negara tersebut agak lambat, namun sejak dikeluakannya peraturan Hitech (Health Information Technology for Economic and Clinical Health) Act 2009 perkembangannya mulai pesat,

Terdapat insentif dan penalti bagi yang belum atau kurang dalam penerapan rekam medis elektronik.

Rekam Medis adalah Dokumen Rahasia

UU 29/2004 Praktek Kedokteran (Pasal 46)	• Dokumen rekam medis berisi catatan dan identitas pasien. Termasuk hasil pemeriksaan, pengobatan, tindakan, dan pelayanan lain kepada pasien. • Dokumen rekam medis dimiliki oleh dokter, dokter gigi, atau sarana pelayanan kesehatan. Sedangkan isinya merupakan kepemilikan pasien. • Rekam medis harus disimpan dan dijaga kerahasiaannya oleh dokter atau dokter gigi, dan pimpinan sarana pelayanan kesehatan.
UU 44/2009 Tentang Rumah Sakit (Pasal 38)	• Segala sesuatu yang berhubungan dengan temuan dokter atau dokter gigi dalam rangka pengobatan, dicatat dalam rekam medis yang dimiliki pasien dan bersifat rahasia
PMK 269/2008 (Pasal 12)	• Ringkasan rekam medis hanya bisa didapatkan pasien, keluarga pasien, orang yang diberi kuasa pasien atau keluarga pasien. Selain itu, orang yang mendapat persetujuan tertulis dari pasien atau keluarga pasien.

UU ITE Pasal 16 (1)

PERSYARATAN PENYELENGGARAAN SISTEM ELEKTRONIK

a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;

b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;

c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;

d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan

e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

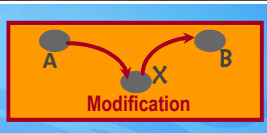
Dampak kerawanan

- Sifat kerahasiaan isi rekaman medis di samping merupakan hak bagi pasien, juga merupakan kewajiban bagi tenaga kesehatan untuk menyimpan rahasia jabatan.
- Sanksi pelanggaran yang dapat dikenakan Pasal 79 butir c Undang-undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran mengancam sanksi pidana kurungan paling lama 1 (satu) tahun atau denda paling banyakRp. 50.000.000,- (Lima puluh juta rupiah).

Menurut Ponemon Institute, dalam *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data* disebutkan bahwa sektor kesehatan menyumbang sekitar 44% dari seluruh kasus pelanggaran data selama tahun 2013. Sekitar 65% dari seluruh fasilitas pelayanan kesehatan yang ada melaporkan kasus *cyber security* pada tahun yang sama

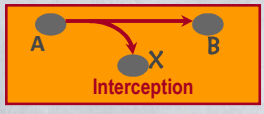
KERAWANAN REKAM MEDIS/ KESEHATAN ELEKTRONIK

Otentikasi, metode identifikasi/ pengenalan pihak-pihak yang mengakses RM, baik secara kesatuan sistem maupun informasinya, baik isi datanya atau waktu pengiriman



Integrity, metode untuk meyakinkan bahwa data RM tidak mengalami perubahan oleh yang tidak berhak atau oleh suatu hal lain yang tidak diketahui

Nir-penyangkalan, usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi/Data RM oleh yang mengirimkan/ membuat;



Confidentiality : Kerahasiaan, meyakinkan bahwa data/informasi yang ditransmisikan/Dsimpan tidak diketahui oleh pihak yang tidak berhak/ berwenang untuk mengetahuinya

RM/K ELEktronik MEMERLUKAN MEKANISME KEAMANAN DENGAN METODE KRIPTOGRAFI/ PERSANDIAN

Ancaman	Keamanan
Pihak Tidak Sah	Otentikasi
Kebocoran Data	Kerahasiaan
Pemalsuan Data	Integritas
Penyangkalan	Nir-Sangkal

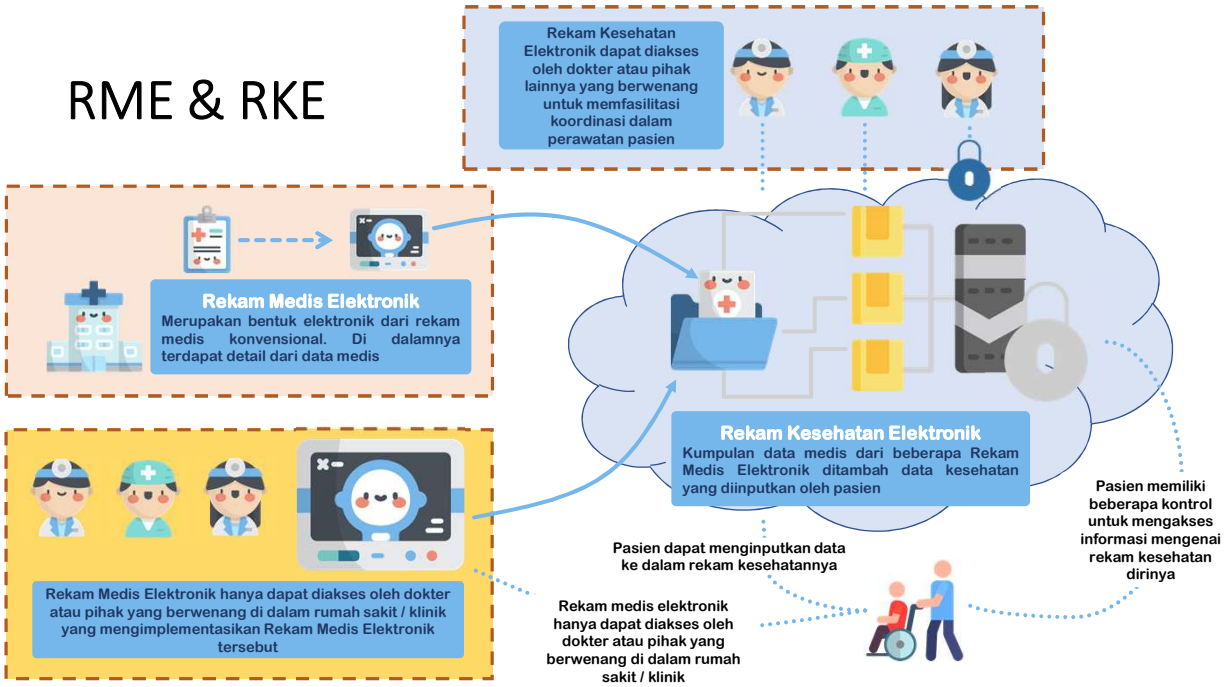
10

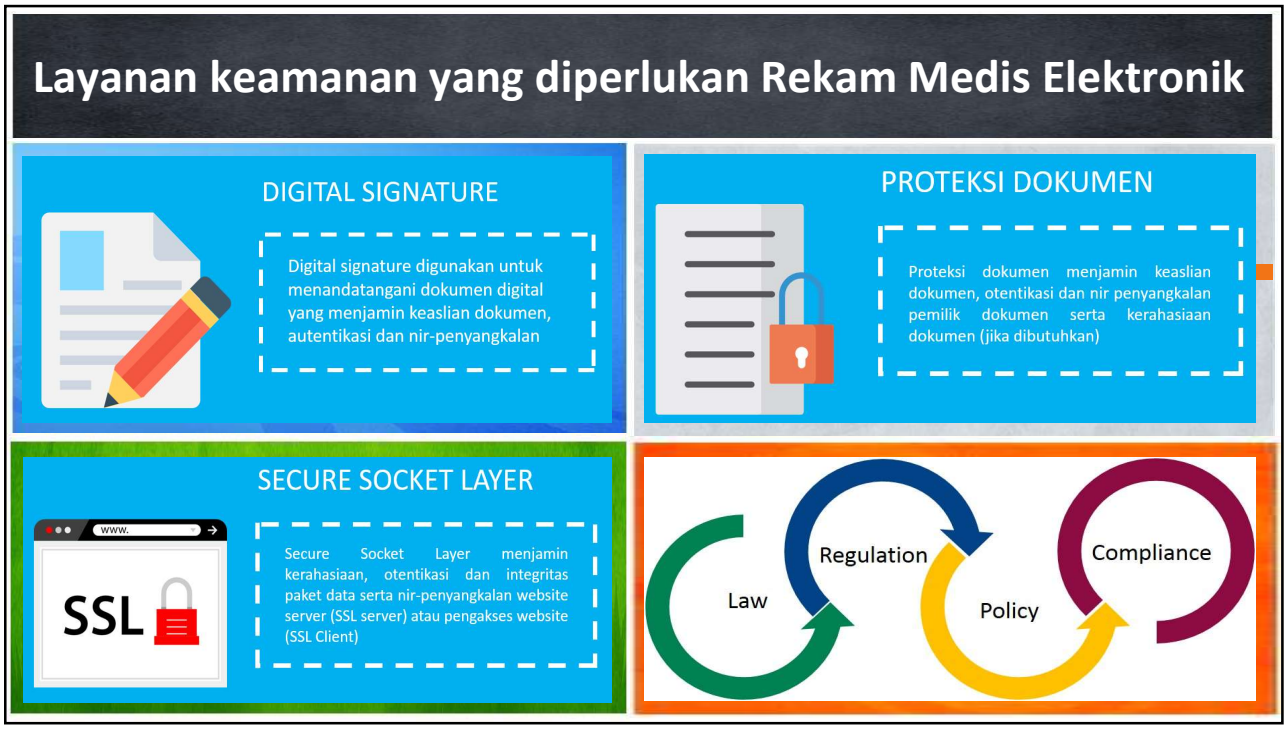
Tips melindungi data RME/RMK

- SOP Penanganan informasi kesehatan pasien
- Security Awareness kepada seluruh petugas medis bahwa rekam medis pasien bersifat rahasia.
- Prosedur pembatasan hak akses terhadap informasi pasien sesuai dengan hak dan wewenangnya.
- Secure RME/RMK untuk melindungi data
- Merekrut SDM bidang *cyber security* untuk mengetahui dengan cepat apabila terjadi penyalahgunaan informasi dan meminimalisir informasi yang telah disalahgunakan tersebar luas.

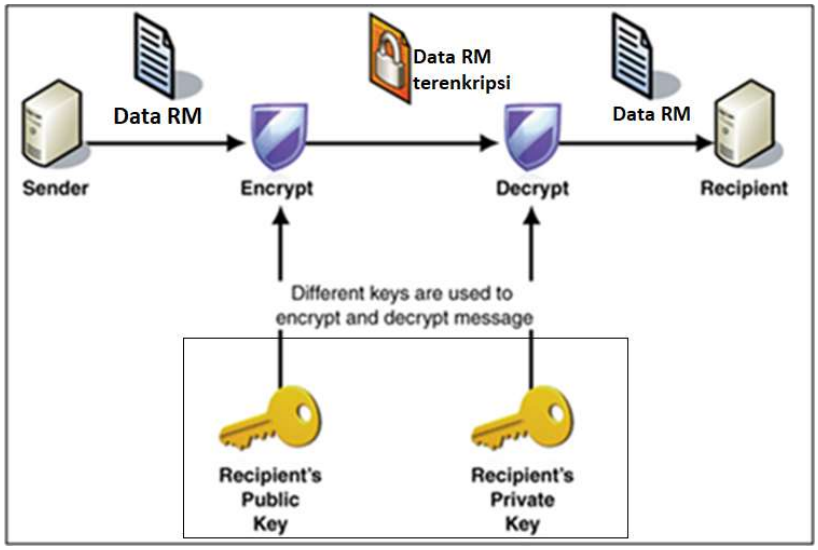
Transaksi Elektronik adalah **perbuatan hukum** yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media **elektronik** lainnya.

RME & RKE





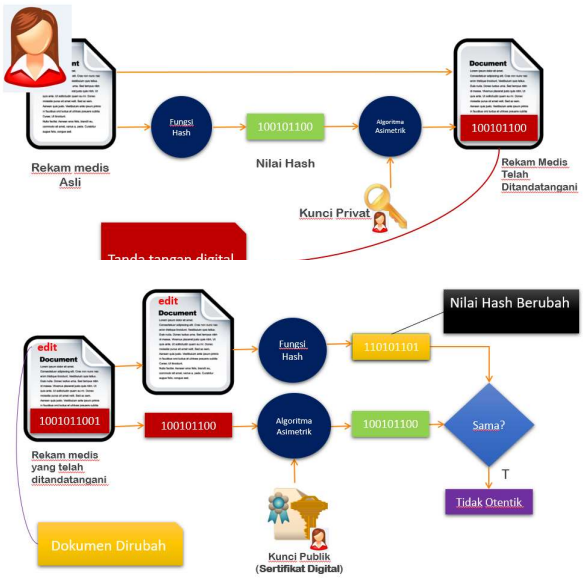
Proteksi Rekam Medik Elektronik

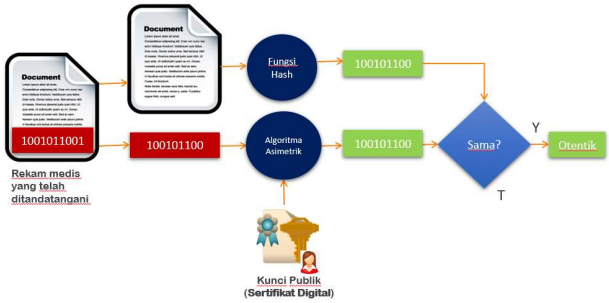


Solusi Jaminan Kerahasiaan (Proteksi Dokumen RME)

- Proteksi dokumen dilakukan dengan memanfaatkan sertifikat elektronik, sehingga dokumen yang akan disimpan pada sistem rekam medis elektronik akan di-enkripsi menggunakan kunci publik dari sistem.
- Untuk mengakses data rekam medis pada sistem, user harus terlebih dahulu diautentikasi identitasnya, jika mempunyai hak akses, maka sistem akan mendekripsi data rekam medis menggunakan kunci privat sistem.
- Kunci Publik dan Kunci Privat merupakan pasangan kunci yang terdapat dalam sertifikat elektronik

Digital Signature (Td Tangan Elektronik) RME





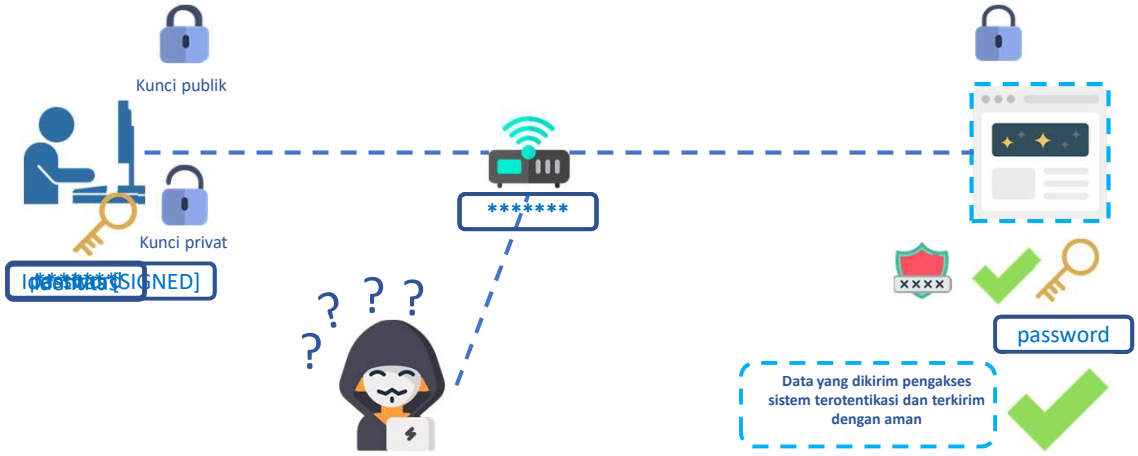
Landasan Hukum : (UU ITE Pasal 11&12)
- Tanda Tangan Elektronik memiliki kekuatan hukum & akibat hukum yg sah
- Terdapat syarat syah tanda tangan elektronik

Solusi Jaminan Kutuhan, Keaslian dan Nir-Sangkal (*Digital Signature*)

- **Dengan menerapkan tanda tangan elektronik yang dilekatkan pada data rekam medis elektronik maka akan memberikan jaminan keutuhan, keaslian dan Anti penyangkalan.**
- **DS dilakukan Ketika user/dokter/petugas medis berwenang akan menyetujui atau mengunggah data rekam medis. DS dilakukan dengan menginputkan passphrase dari sertifikat elektronik yang dimiliki. Sistem akan menghitung nilai hash data rekam medis dan menghitung nilai tanda tangan menggunakan kunci privat yang ada di sertifikat elektronik user.**
- **Untuk memverifikasi keaslian data rekam medis, akan diverifikasi nilai hash dari dokumen dengan nilai hash yang tersimpan dalam tanda tangan dokumen.**

SECURE SOCKET LAYER (Client)

Mengotentikasi pengakses sistem dan mengamankan jalur komunikasi dari pengakses sistem ke server



Solusi Jaminan Autentikasi akses terbatas (SSL Client)

- Setiap akses terhadap data rekam medis harus dapat diidentifikasi identitas pengguna yang mengaksesnya. Oleh karena itu sertifikat elektronik dapat digunakan untuk autentikasi user dengan menerapkan SSL Client.

- Pada penerapan SSL Client, dilakukan penandatanganan secara elektronik terhadap request ke server, sehingga akses yang terautentikasi tidak dapat disangkal identitasnya oleh user yang mengakses