**JURNAL SABHANGA**

**Vol. 2 No. 1 Januari 2020 : 18-29**
e-journal.stikessatriabhakti.ac.id

# KEAMANAN INFORMASI DI RUMAH SAKIT

**Mohamad Nur Afif**[1]
[1]Sandiman Muda pada Subdirektorat Audit Keamanan Informasi,
Direktorat Proteksi Pemerintah, BSSN
Email: nur.afif@bssn.go.id

**Abstract**

The health sector is one of the fields of work that is closely related to privacy issues or a person's personal data, especially data or information from patients. So that the health sector becomes one of the three fields that are very vulnerable to data or information leakage. The latest incident related to patient information is the alleged theft of citizen data related to Covid-19 by hackers sold on the dark web Rapid Forums forum. The data sold are complete, some of the information is in the form of name, citizenship status, date of birth, age, telephone number, home address, population identification number (NIK), and address of the corona test results, where the information is generally also submitted by the patient or asked when registering to health services, both at the Community Health Center (Puskesmas), Polyclinic, or at the Hospital (RS).

Therefore, in the health sector itself, it is necessary to implement an information security management system, starting from the patient registration process until the data or information is accessed or stored.

## PENDAHULUAN

Bidang kesehatan merupakan salah satu bidang pekerjaan yang sangat erat kaitannya dengan masalah privasi atau data pribadi seseorang terutama adalah data atau informasi dari pasien. Sehingga bidang kesehatan menjadi salah satu dari tiga bidang yang sangat rentan terhadap kebocoran data atau informasi. Berdasarkan Laporan Data *Breach Industry Forecast* 2019 oleh *Experian Data Breach Resolution*, bahwa tiga bidang tersebut adalah kesehatan, pemerintahan dan keuangan.

Peristiwa terbaru yang terkait dengan informasi pasien adalah dugaan pencurian data warga terkait covid-19 oleh peretas yang dijual di forum *dark web Rapid Forums*. Data-data yang dijual terbilang lengkap, beberapa informasi tersebut berupa nama, status kewarganeraan, tanggal lahir, umur, nomor telepon, alamat rumah, nomor indentititas kependudukan (NIK), dan alamat hasil tes corona, dimana informai tersebut umumnya juga diserahkan oleh pasien atau diminta ketika akan mendaftar ke layanan kesehatan, baik di Pusat Kesehatan Masyarakat (Puskesmas), Poliklinik, maupun di Rumah Sakit (RS).

Oleh karena itu di bidang kesehatan sendiri perlu menerapkan sistem manajemen keamanan informasi, mulai dari proses pendaftaran pasien sampai dengan data atau informasi tersebut diakses maupun disimpan. Selain itu juga, di perguruan tinggi bidang kesehatan sudah mulai diperkenalkan mengenai

keamanan informasi sehingga saaat para lulusannya baik dokter, perawat, maupun bidan telah bekerja di institusi kesehatan mereka sudah mampu menerapkan keamanan informasi.

**Jenis Informasi di Rumah Sakit**

**Definisi Informasi**

Berdasarkan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun non elektronik. Dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dijelaskan juga mengenai definisi dari Informasi Elektronik, yakni bahwa Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail),* telegram, teleks, *telecopy*atau sejenisnya, huruf, tanda, angka, Kode Akses, symbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Jenis-jenis informasi di Rumah Sakit mengikuti pembagian jenis informasi yang ada di Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik. Jenis informasi tersebut adalah:

1. Informasi yang wajib disediakan dan diumumkan
   a. Informasi yang wajib disediakan dan diumumkan secara berkala
      Meliputi:
      1) Informasi yang berkaitan dengan badan publik;
      2) Informasi mengenai kegiatan dan kinerja Badan publik terkait;
      3) Informasi mengenai laporan keuangan; dan
      4) Informasi lain yang diatur dalam peraturan perundang-undangan.
   b. Informasi yang wajib diumumkan secara serta merta
      Meliputi informasi yang dapat mengancam hajat hidup orang banyak dan ketertiban umum.
   c. Informasi yang wajib tersedia setiap saat
      Meliputi:
      1) Daftar seluruh informasi publik yang berada di bawah penguasaannya, tidak

termasuk informasi yang dikecualikan;

2) Hasil keputusan badan publik dan pertimbangannya;
3) Seluruh kebijakan yang ada berikut dokumen pendukungnya;
4) Rencana kerja proyek termasuk di dalamnya perkiraan pengeluaran tahunan Badan publik;
5) Perjanjian badan publik dengan pihak ketiga;
6) Informasi dan kebijakan yang disampaikan Pejabat Publik dalam pertemuan yang terbuka untuk umum;
7) Prosedur kerja pegawai badan publik yang berkaitan dengan pelayanan masyarakat; dan atau
8) Laporan mengenai pelayanan akses Informasi Publik sebagaimana diatur dalam Undang-Undang ini.

2. Informasi yang dikecualikan

Meliputi, Informasi Publik yang apabila dibuka dan diberikan kepada pemohon informasi publik dapat:

a. Menghambat proses penegakan hukum;
b. Menggangu kepentingan perlindungan hak atas kekayaan intelektual dan perlindungan dari persaingan usaha tidak sehat;
c. Membahayakan pertahanan dan keamanan negara;
d. Mengungkapkan kekayaan alam Indonesia;
e. Merugikan ketahanana ekonomi nasional;
f. Merugikan kepentingan hubungan luar negeri;
g. Mengungkapkan isi akta otentik yang bersifat pribadi dan kemauan terakhir ataupun wasiat seseorang;
h. Mengungkap rahasia pribadi;
i. Memorandum atau surat-surat antar badan publik atau intra badan publik, yang menurut sifatnya dirahasiakan kecuali atas putusan komisi informasi atau pengadilan;
j. Informasi yang tidak boleh diungkapkan berdasarkan undang-undang.

**Peraturan Perundang-undangan Terkait Keamanan Informasi di Rumah Sakit**

Terkait dengan keamanan informasi di rumah sakit selain Undang-Undang Nomor

14 Tahun 2008 tentang Keterbukaan Informasi Publik, ada juga peraturan perundang-undangan lainya yang mengatur, seperti:

1. Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran, terutama pada Pasal 46 dan Pasal 47 yang menyatakan bahwa dokumen rekam medis harus disimpan dan dijaga kerahasiannya oleh dokter atau dokter gigi dan pimpinan sarana pelayanan kesehatan. Kemudian juga pada Pasal 48 yang menyatakan bahwa setiap dokter atau dokter gigi dalam melaksanakan praktik kedokteran wajib menyimpan rahasia kedokteran. Rahasia kedokteran dapat dibuka hanya untuk kepentingan kesehatan pasien, memenuhi permintaan aparatur penegak hukum dalam rangka penegakan hukum, permintaan pasien sendiri, atau berdasarkan ketentuan perundang-undangan.
2. Undang-Undang Nomor 36 Tahun 2014 tentang Tenaga Kesehatan, pada Pasal 73 menyatakan bahwa, setiap tenaga kesehatan dalam melaksanakan pelayanan kesehatan wajib menyimpan rahasia kesehatan penerima pelayanan kesehatan. Rahasia kesehatan penerima pelayanan kesehatan dapat dibuka hanya untuk kepentingan kesehatan penerima pelayanan kesehatan, pemenuhan permintaan aparatur penegak hukum bagi kepentingan penegakan hukum, permintaan penerima pelayanan kesehatan sendiri, atau pemenuhan ketentuan peraturan perundang-undangan.
3. Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit, pada Pasal 38 menyatakan bahwa, setiap rumah sakit harus menyipan rahasia kedokteran. Rahasia kedokteran tersebut hanya dapat dibuka untuk kepentingan kesehatan pasien, untuk pemenuhan permintaan aparat penegak hukum dalam rangka penegakan hukum, atas persetujuan pasien sendiri atau berdasarkan ketentuan peraturan perundang-undangan.
4. Peraturan Pemerintah Nomor 10 Tahun 1966 tentang Wajib Simpan Rahasia Kedokteran, yang menyatakan bahwa orang-orang yang melakukan pekerjaan dalam lapang kedokteran wajib menyimpan rahasia. Orang-orang tersebut yakni tenaga kesehatan, mahasiswa kedokteran, murid yang

bertugas dalam lapangan pemeriksaan, pengobatan dan/atau perawatan dan orang lain yang ditetapkan oleh Menteri Kesehatan.

5. Peraturan Menteri Kesehatan Nomor 269/MENKES/PER/III/2008 tantang Rekam Medis, terutama pada Pasal 12 dan Pasal 13 yang menyatakan bahwa berkas rekam media milik sarana pelayanan kesehatan, isi rekam medis merupakan milik pasien yang diberikan dalam bentuk ringkasan medis. Ringkasan medis ini dapat diberikan, dicatat, atau dicopy oleh pasien atau orang yang diberi kuasa atau atas persetujuan tertulis pasien atau keluarga pasien yang berhak untuk itu. Begitu juga dengan pemanfaatannya yang berkaitan untuk keperluan pendidikan dan penelitian, penyebutan identitas pasien harus mendapatkan persetujuan secara tertulis dari pasien atau ahli warisnya dan harus dijaga kerahasiaanya. Namun, bila dilakukan untuk kepentingan negara maka tidak diperlukan persetujuan pasien.

**Ancaman Terhadap Keamanan Informasi di Rumah Sakit**

**Keamanan Informasi**

Secara umum keamanan informasi diartikan sebagai usaha untuk menjaga keamanan informasi, meliputi perlindungan terhadap privasi (*privacy*), keutuhan (*integrity*) dan ketersediaan (*availability*). Sedangkan berdasarkan dokumen NIST SP 800 – 12 Rev 1 *An Introduction to Information Security*, bahwa yang dimaksud dengan keamanan informasi adalah perlindungan informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan yang tidak sah untuk memastikan kerahasiaan *(confidentiality*), keutuhan/integritas*(integrity*), dan ketersediaan (*availability*).

1. Memastikan kerahasiaan yakni dengan menjaga pembatasan resmi pada akses informasi dan pengungkapan, termasuk cara untuk melindungi privasi pribadi dan informasi hak milik.
2. Memastikan keutuhan/integritas yakni menjaga dari modifikasi atau perusakan informasi yang tidak tepat dan memastikan informasi tidak dapat disangkal dan terjamin keasliannya. Integritas data yakni property yang datanya belum diubah dengan cara tidak sah. Integritas

data mencakup data dalam penyimpanan, selama pemrosesan, dan saat dalam perjalanan. Integritas sistem yakni kualitas yang dimiliki sistem ketika menjalankan fungsi yang dimaksudkan dengan cara yang tidak terganggu, bebas dari manipulasi sistem yang tidak sah, baik disengaja atau tidak disengaja.

3. Memastikan ketersediaan yakni memastikan akses tepat waktu dan dapat diandalkan ketika informasi tersebut akan digunakan.

Dalam menerapkan keamanan informasi, tidak terlepas dari adanya ancaman terhadap informasi. Ancaman informasi dapat ditelusuri dari siapa pelakunya (hacker), berikut beberapa pelaku:

1. Individu dan grup kecil hacker, merupakan kategori pertama para penyerang. Mereka termovitasi oleh mencari keuntungan dan ketenaran. Oleh karena itu, biasanya mereka memilih target mereka sesuai dengan peluang dan memanfaatkan sarana yang tidak canggih.
2. Grup politik dan paparazzi, mereka termotivasi oleh kegiatan hacktivism tetapi juga keuntungan politik dan finansial. Mereka paling sering bertujuan untuk memalukan, mendeskreditkan, memeras atau menjual informasi tentang orang-orang terkenal. Hacktivism dimaksudkan juga untuk menarik perhatian publik terhadap sesuatu yang diyakini oleh hacker sebagai masalah atau penyebab penting, seperti kebebasan informasi atau hak asasi manusia.
3. Organisasi kriminal, mereka termotivasi oleh perolehan finansial dan kegiatan kriminal yang lebih luas seperti pemerasan dan pemaksaan. Mereka mungkin bertujuan mendapaykan catatan medis tentang target individu, mengancam mereka atau menyebabkan kerusakan fisik pada mereka. Mereka juga dapat mengambil untung dari eksploitasi volume *Electronic Health Record* (HER)/ catatan kesehatan elektronik yang tidak ditargetkan dalam volume.
4. Teroris, mereka termotivasi untuk menimbulkan rasa takut dan meyebabkan kerugian. Tujuan

mereka biasanya untuk menyakiti atau mengancam invidu.

5. Yang terakhir, penyerangnya adalah orang-orang yang diperintah oleh negara dan ini menjadi ancaman terbesar dengan tujuan untuk melukai atau mengancam invidu. Selain itu, motivasi mereka mungkin juga untuk mendapatkan *personally indentifiable information* (PII)/ informasi pribadi dan/atau *Electronic Health Record* (HER)/ catatan kesehatan elektronik untuk eksploitasi massal.

**Ancaman Terhadap Informasi**

Berdasarkan *Cyber Security Report 2020* yang dikeluarkan oleh *Check Point Research* bahwa pada tahun 2019 ada serangan siber yang meningkat berupa *ransomware* yang menyasar industri-industri tertentu, pemerintahan dan organisasi kesehatan termasuk rumah sakit. Selain itu, Dikutip dari *healthitsecurity.com*bahwa serangan *ransomware* terhadap penyedia layanan kesehatan meningkat 350% selama kuartal terakhir 2019 dengan laju serangan yang cepat telah berlanjut sepanjang 2020. Selain itu bahwa lebih dari 91% serangan ransomware adalah akibat dari eksploitasi phising.*Ransomware* menurut John Villasenor, seorang Profesor di The University of California, Los Angeles, merupakan sejenis malware yang mampu mengambil alih kendali atas sebuah komputer dan mencegah penggunanya untuk mengakses data hingga tebusan dibayar.

Beberapa kerugian yang diakibatkan oleh ransomware karena membayar tebusan, berdasarkan *Cyber Security Report 2020* antara lain: Pemerintah Kota Lake City, Florida, Amerika Serikat harus membayar tebusan sebanyak $500.000 setelah serangan ransomware melumpuhkan sistem komputer pemerintah kota selama 2 pekan. Serangan ini dijuluki "*Triple Threat*" yakni mengkombinasikan tiga metode serangan yang berbeda, menyerang jaringan sistem komputer, jaringan telepon dan jaringan e-mail. Dikutip dari hipaaajournal.com bahwa *University of California San Fransisco* harus membayar tebusan $1,14 juta kepada operator ransomware NetWalker untuk menyelesaikan serangan berupa enkripsi data pada fakultas kesehatan tersebut. Serangan tersebut terjadi pada tanggal 1 Juni 2020, pihak UCSF telah mengisolasi server tersebut namun tidak mencegah enkripsi file. Fakultas Kesehatan UCSF sendiri terlibar dalam penelitian untuk menemuka obat untuk Covid-19 dan

terlibat juga dalam pengujian antibodi. Selain terkena ransomware beberapa file informasi di UCSF juga dicuri.

Berdasarkan dokumen *State of Cybersecurity & Cyber Threats In Healthcare Organizations* yang dikeluarkan oleh *ESSEC Business School,* bahwa serangan-serangan tersebut sangat mirip dan menunjukan pola sebagai berikut:

1. Peretas mendapatkan akses ke fasilitas sistem informasi dengan menggunakan beragam metode, misalnya melalui kehadiri fisik (melalui USB drive), eksploitasi perangkat lunak yang rentan dan telah kadaluwarsa (expired), dan pencurian perangkat selular staf dan bahkan e-mail phising atau berbahaya.
2. Setelah peretas memiliki akses ke fasilitas sistem informasi, mereka menggunakan virus khusus yang menahan sistem dengan mengenkripsi data yang dikandungnya. Oleh karena itu, sistem informasi tersebut sepenuhnya tidak dapat diakses dan tidak dapat digunakan sampai peretas dibayar tebusannya. Tebusan tersebut biasanya dalam bentuk Bitcoin untuk membuatnya tidak dilacak.
3. Apa yang membuat rumah sakit menjadi sasaran empuk itu adalah karena sensitifitas informasi yang ada pada rumah sakit tersebut, tanpa akses cepat ke catatan kesehatan pasien (rekam medis), dapat mengakibatkan perawatan pasien mungkin tertunda dan dapat mengakibatkan konsekuensi yang serius pada kesehatan pasien bahkan dapat membawa pada kematian dan tuntutan secara hukum terhadap rumah sakit. Hal ini yang terkadang pihak rumah sakit tidak mau mengambil risiko dan langsung membayarkan tebusan tersebut.

Jenis serangan ini sangat populer karena sangat sederhana dalam segalal hal, seperti mudah diterapkan (cukup dengan mengirimkan tautan tertentu melalui e-mail yang akan dibuka oleh staf atau pegawai) dan ini adalah cara mudah untuk menghasilkan uang (pelaku hanya menunggu sampai rumah sakit membayar tebusan).

Serangan umum lainnya adalah serangan model lama “klasik” yakni berupa pencurian informasi. Peretas berhasil masuk ke sistem informasi rumah

sakit melalui phising atau melalui perangkat portable yang dicuri dan kemudian mencuri informasi sebanyak mungkin. Jenis serangan ini bahkan lebih berbahaya daripada ransomware tetapi lebih sulit dilakukan dan memakan waktu bagi perets. Namun, ini juga lebih menguntungkan bagi mereka. Di pasar gelap, harga jual data/informasi curian untuk kartu kredit kisan $ 1 - $ 3 dan nomor jaminan sosial bernilai $ 15, catatan kesehatan/rekam medis bernilai $ 50, dengan mengingat bahwa satu serangan dapat memberikan akses ke jutaan catatan pasien.

A. Cara Meningkatkan Keamanan Informasi di Rumah Sakit

Melihat fakta bahwa rumah sakit atau lembaga kesehatan lainnya menjadi salah satu sasaran strategis serangan siber, dan pengelolaan keamanan informasi yang belum maksimal bahkan kurang mendapatkan perhatian/bukan skala prioritas, maka perlu ada penanganan khusus terhadap keamanan informasi di rumah sakit atau lembaga kesehatan. Sebagaimana disampaikan oleh A.Le Bris dan W. El Asri dalam dokumen *State of Cybersecurity & Cyber Threat in Healthcare Organization,* ada beberapa hal yang dapat dilakukan guna meningkatkan keamanan informasi di rumah sakit atau lembaga kesehatan lainnya, antara lain:

1. Membentuk Tim Khusus yang tujuan utamanya adalah mempelajari kebijakan keamanan informasi yang saat ini ada di rumah sakit atau lembaga kesehatan lainnya, menetapkan prosedur untuk meningkatkan keamanan informasi dan mengurangi kerentanannya sebanyak mungkin.
2. Mendedikasikan sebagian dari sumber daya untuk. Meningkatkan kesadaran keamanan informasi pegawainya melalui sosialisasi, bimbingan teknis, workshop, seminar, dan media lainnya. Meningkatkan kesadaran keamanan informasi bagi pegawai ini sangat penting karena sebagian besar insiden keamanan informasi dipengaruhi oleh faktor manusia, seperti kesalahan dalam konfigurasi sistem informasi, penggunaan perangkat software/aplikasi bajakan, pengiriman informasi yang sifatnya sensitif/berklasifikasi melalui jaringan terbuka/tidak ada pengamana tambahan.
3. Menerapkan rencana aksi bila ada serangan/peretasan, siapkan prosedur investigasinya dan

lakukan pengumpulan informasi dari serangan/peretasan tersebut meliputi jenis serangan yang terjadi (misal ransomware atau pencurian informasi), diagnosis peralatan yang terkena dampak, analisa mengenai titik rentan atau rawan yang menjadi celah adanya peretasan) dan mempunyai daftar kontak lembaga pemerintah yang terkait untuk penanganan lebih lanjut.

Dikutip dari pusdatin.kemkes.go.id, disebutkan bahwa keamanan informasi yang baik dapat dicapai melalui penerapan sejumlah upaya-upaya teknis (operasional) yang didukung oleh berbagai kebijakan dan prosedur manajemen yang sesuai. Sistem manajemen keamanan informasi (SMKI) adalah sistem manajemen yang diterapkan perusahaan untuk mengamankan aset informasi terhadap ancaman yang dapat terjadi. SMKI menjadi penting diterapkan agar informasi yang beredar dalam perusahaan dapat dikelola dengan benar sehingga dapat menunjang *business process*serta memberikan layanan terbak kepada pelanggan, mitra kerja atau pihak terkait yang bekerjasama.Dalam mendukung pelaksanaan keamanan informasi diperlukan kesadaran seluruh anggota organisasi atau pegawai perusahaan. Upaya-upaya yang dapat dilakukan terkait dengan pengamanan informasi di area kerja adalah sebagai berikut:

1. Selalu mengunci perangkat komputer ketika akan meninggalkan meja kerja dengan menekan *windows* + L, atau mengaktifkan kunci otomatis pada perangkat komputer melalui pengaturan screen saver.
2. Memastikan password pada sistem dan perangkat komputer terdiri dari minimal 7 karakter yang menggunakan kombinasi huruf, angka dan karakter spesial (@#*!), serta jangan membagikan atau menuliskan *password* pada perangkat atau pada meja kerja.
3. Memastikan tidak ada dokumen rahasia di atas meja kerja pada saat meninggalkan area kerja.
4. Memastikan informasi atau dokumen rahasia tersimpan dalam lemari yang terkunci dan tertata rapi.
5. Memusnahkan dokumen rahasia secara aman dengan mesin penghancur kertas.
6. Tidak menyimpan dokumen perusahaan ke dalam media penyimpanan pribadi, serta selalu

mengecek media penyimpanan informasi.

7. Selalu melakukan *back-up* data secara berkala agar tidak terjadi kehilangan data.
8. Memastikan antivirus pada perangkat yang digunakan selalu *update* dan melakukan *full scan* secara berkala.
9. Tidak memasang aplikasi bajakan dan aplikasi *games* pada perangkat komputer perusahaan.

B. Kesimpulan

Keamanan informasi telah menjadi isu strategis untuk fasilitas kesehatan. Dicap sebagai sasaran empuk dengan pertahanan yang usang dan unit keamanan informasi yang buruk menjadikan peretas tidak ragu menyerang mereka untuk mendapatkan keuntungan. Melumpuhkan sistem informasi dengan ransomware, meretas ke dalam database rumah sakit dan menjual informasi pasien ke tingkat tertinggi penawar, mengancam akan merilis informasi pribadi. Situasi ini dapat disebabkan oleh faktor internal dan eksternal. Faktor dari internal disebabkan oleh kurangnya kesadaran keamanan informasi para pegawainya dan kurangnya dukungan manajemen terhadap keamanan informasi. Sedangkan faktor eksternal disebabkan oleh keuntungan yang menjanjikan dari jual beli data pribadi selain itu juga dapat dipengaruhi oleh situasi politik global yang menjadikan aktor yang didukung oleh negara menjadikan kegiatan peretasan sebagai kegiatan untuk mengumpulkan informasi dari negara lain atau organisasi lain demi tujuan tertentu.

Mewujudkan keamanan informasi bukan hanya tanggungjawab unit keamanan informasi semata, melainkan tanggungjawab semua dari mulai unsur pimpinan hingga unsur staf. Keamanan informasi bukan hanya masalah aspek teknis seperti *firewall* maupun antivirus, melainkan juga aspek manajemennya seperti ketersediaan kebijakan, prosedur, program pelatihan, dan sosialisasi keamanan informasi.

**DAFTAR PUSTAKA**

https://www.cnnindonesia.com/teknologi/20200623160834-185-516532/deretan-peristiwa-kebocoran-data-warga-ri-sejak-awal-2020 tanggal akses 26 Juni 2020, 10.05 WIB

Daftar Informasi Publik dan Dokumentesi dan Informasi Yang Dikecualikan Tahun 2017 di RSUD Dr. Moewardi, Jawa Tengah;

Keputusan Direktur Umum Rumah Sakit Umum Daerah R.A Kartini Kabupaten Jepara Nomor 445/21.5 Tahun 2018 tentang Klasifikasi Informasi Publik Yang Dikecualikan Pada Rumah Sakit Umum Daerah R.A Kartini.

https://www.voaindonesia.com/a/apa-itu-ransomware/3921984.html tanggal akses 30 Juni 2020 pkl 14.47 WIB

Security Report Health Care-Hospitals, Providers and More oleh Corvus

https://www.hipaajournal.com/university-of-california-san-francisco-pays-1-14-million-ransom-to-resolve-netwalker-ransomware-attack/ tanggal akses 1 Juli 2020, 10.30 WIB

Le Bris, A., El Asri, W.: State of Cybersecurity & Cyber Threat in Healthcare Organization, ESSEC Business School, 12 p. (2016)

https://pusdatin.kemkes.go.id/article/view/15040600001/sistem-manajemen-keamanan-informasi.html tanggal akses 1 Juli 2020 15.01 WIB.

Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit;

Undang-Undang Nomor 36 Tahun 2014 tentang Tenaga Kesehatan;

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;