# MODUL PROTEKSI DAN PERTUKARAN INFORMASI KESEHATAN
# PROTEKSI

## PERTEMUAN 6 (ONLINE)

“Information is an asset which, like other **important business assets**, has value to an organization and consequently needs to be suitably **protected**”

“… Whatever form the information takes, or means by which it is shared or stored, **it should always be appropriately protected**” ISO/IEC 27002:2007

Privacy is the freedom to choose what information is shared or not shared with other parties. For example, privacy is an individual’s right to not disclose information about themselves to others, such as not disclosing an individual’s genetic predisposition to cancer on an employment application. Legislatures may choose to enact laws that prohibit the compelled disclosure of information in order to protect an individual’s privacy.

Confidentiality is the obligation to keep secret information with which one is entrusted. For example, confidentially obligations are imposed under the Health Insurance Portability and Accountability Act (HIPAA) by prohibiting covered entity health-care providers from disclosing protected health information (PHI) to the media without a patient’s authorization. Confidentiality obligations are often mislabeled as privacy obligations. For example, the HIPAA Privacy Rule would be more appropriately labeled as the Confidentiality Rule as it imposes obligations upon covered entities not to make certain disclosures of information (ie, to maintain confidentiality).

Security is the combination of administrative, technical, and physical safeguards that ensure confidentiality and promote privacy. Security is comprised of the safeguards that prevent inappropriate uses and disclosures of information. For example, strong passwords, encryption, and door locks all represent security safeguards that exist to keep information in the right hands.

Many states have enacted laws that are more stringent than HIPAA with respect to several categories of “sensitive data.” Data considered sensitive under state laws are often mental and behavioral health data, communicable disease data, genetic information, and sexually transmitted disease data.

HIPAA and federal law do provide specific protections for psychotherapy notes (under HIPAA) and drug and alcohol addiction treatment data (under 42 CFR Part II).

A covered entity is (1) a health-care provider that engages in certain electronic transactions (essentially any health-care provider that accepts insurance of any kind will engage in covered electronic transactions), (2) a health plan, or (3) a health-care clearinghouse (an entity that converts health information into standard formats required by HIPAA).

A business associate is a person or entity (other than a member of a covered entity’s workforce) that creates, receives, maintains, or transmits PHI for or on behalf of a covered entity; essentially a person or entity that performs services for a covered entity that involve PHI. Examples of business associates include billing companies, practice management companies, hosted EHR vendors, and lawyers. Under the HITECH Act, a health information organization (or an HIE) is specifically named as a business associate

The Privacy Rule lists 18 specific identifiers that, when paired with some type of health information, result in PHI. Those identifiers are as follows:

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if certain population requirements are met
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account number
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers 16. Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images.
- Any other unique identifying number, characteristic, or code, except for certain coding systems that allow for reidentification of data

It is important to note the distinction between “use” and “disclosure.” A use of PHI is the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information . A disclosure of PHI is the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information. Under the Privacy Rule, the following are the primary uses and disclosures of PHI that are permitted without a patient’s authorization:

- To the individual to whom the PHI relates
- For treatment, payment, or health-care operations
- For public health activities

– As required by law

– For certain research activities where a privacy board or an institutional review board has waived the authorization requirement

**TABLE 6.1** HIPAA Security Rule Controls

| **Administrative Procedures** [28] | **Physical Safeguards** [29] | **Technical Security Measures** [30] |
|---|---|---|
| *Security management process*—Policies and procedures to prevent, detect, contain and correct security violations, including:<br>• Risk assessment (R)<br>• Reduce risk to an appropriate level (R)<br>• Workforce sanctions (R)<br>• Review system activities (R) | *Facility access controls*—Policies and procedures to limit physical access to PHI, including:<br>• Contingency operations plans (A)<br>• Facility security plan (A)<br>• Access control and validation procedures (A)<br>• Maintenance records (A) | *Access control*—Policies and procedures to allow PHI access only to those persons or programs that have been granted access rights, including:<br>• Unique user identification (R)<br>• Emergency access (R)<br>• Automatic logoff (A)<br>• Encryption (A) |
| *Security responsibility*—Identify a security official (R) | *Workstation use*—Policies and procedures that specify functions and physical attributes of workstations and the surrounding areas (R) | *Audit controls*—Hardware, software or mechanisms that record and examine activity in systems (R) |
| *Work force security*—Limit PHI access to appropriate members of the workforce, including:<br>• Authorization and supervision of employees (A)<br>• Clearance of workforce members (A)<br>• Procedures for terminating access to PHI as necessary (A) | *Workstation security*—Physical safeguards for all workstations that access PHI (R) | *Integrity*—Policies and procedures to protect PHI from improper alteration or destruction, including:<br>• Mechanism to authenticate PHI to ensure it has not been altered or destroyed (A) |
| *Information access management*—Access to PHI is limited as required by the Security Rule, including:<br>• Isolating health-care clearinghouse functions (R)<br>• Access authorization policies (A)<br>• Access modification policies (A) | *Device and media control*—Policies and procedures that govern the receipt and removal of hardware and media that contain PHI, including:<br>• Disposal of media (R)<br>• Media reuse (R)<br>• Accountability for movement (A)<br>• Data backup and storage (A) | *Person or entity authentication*—Procedures to verify that a person or entity seeking access to PHI is the one claimed (R) |

(*Continued*)

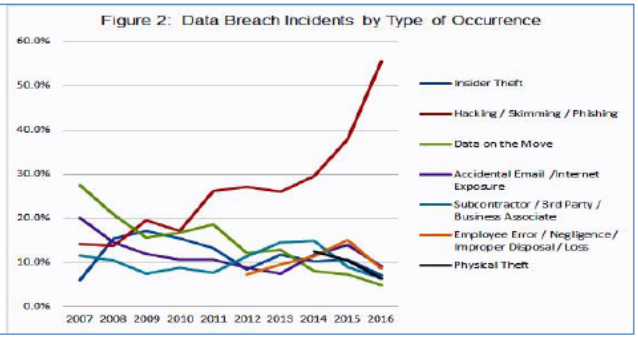
**TABLE 6.1** *Continued*

| Administrative Procedures [28] | Physical Safeguards [29] | Technical Security Measures [30] |
|---|---|---|
| *Security awareness and training*—A security and awareness training program for all workforce members, including:<br>• Security reminders (A)<br>• Protection from malicious software (A)<br>• Log-in monitoring (A)<br>• Password management (A)<br><br>*Security incident procedures*—Policies and procedures to address security incidents through response and reporting (R)<br><br>*Contingency plan*—Policies and procedures for responding to emergencies and system failures, including:<br>• Data backup (R)<br>• Disaster recovery plan (R)<br>• Emergency operation plan (R)<br>• Testing and revision of plans (A)<br>• Application and data criticality analysis (A)<br><br>*Evaluation*—Perform periodic technical and nontechnical evaluations of security controls (R)<br><br>*Business associates*—Covered entities and business associates must obtain written BAAs from their business associates and subcontractors, respectively (R) | | *Transmission security*—Technical security measures to guard against unauthorized access to PHI while in transit, including:<br>• Integrity controls (A)<br>• Encryption (A) |


**Keamanan Informasi** adalah terjaganya kerahasiaan (***confidentiality***), keutuhan (***integrity***), dan ketersediaan (***availability***) informasi.

Dewasa ini tidak ada satu-pun industri yang terbebas dari **hambatan, tantangan, ancaman, dan gangguan** (HTAG) pada sistem jaringan komputer mereka. Penggunaan TIK di bidang kesehatan meningkatkan aksesibilitas, kualitas, dan kesinambungan pelayanan kesehatan. Namun dibalik itu juga terdapat ancaman terhadap data yang dipertukarkan dan disimpan secara digital. Salah satu ancaman terbesar adalah **Cybersecurity.** Cybersecurity telah menjadi isu yang krusial untuk berbagai sektor termasuk kesehatan. Data kesehatan merupakan informasi yang paling sensitif dan kritikal yang dapat mengancam keamanan dan kesejateraan masyarakat.

Laporan *US Department of Health & Human Services, Office for Civil Rights, 2015* telah terjadi kebocoran data EMR pasien yang melibatkan kurang lebih 113 juta pasien di Amerika Serikat.




**2016 Healthcare Data Breaches of 500 or More Records***

| Year | Number of Breaches (500+) | Number of Records Exposed |
|---|---|---|
| 2016 | 329 | 16,471,765 |
| 2015 | 270 | 113,267,174 |
| 2014 | 307 | 12,737,973 |
| 2013 | 274 | 6,950,118 |
| 2012 | 209 | 2,808,042 |
| 2011 | 196 | 13,150,298 |
| 2010 | 198 | 5,534,276 |
| 2009 | 18 | 134,773 |
| **Total** | **1801** | **171,054,419** |

Laporan *Identity Theft Resources* di Amerika Serikat (Maret 2017), 25% dari HTAG terjadi pada sistem jaringan komputer di sektor pelayan kesehatan, kerugian USD 5.6 miliar per tahun-nya.

Ancaman siber dalam industri kesehatan mendeskripsikan bahwa terjadi kebocoran data EMR pasien yang melibatkan kurang lebih 113 juta pasien di Amerika Serikat, dan penyebab paling tinggi adalah disebabkan karena hacking/ skimming/ phishing dan selalu terjadi peningkatan dari awal tahun 2013.


- Menurut Cyber Security Intelligence Index yang dilakukan oleh IBM (2015): lebih dari 100 juta rekam kesehatan rentan atau memiliki risiko pada tahun 2015 di lebih dari 8000 perangkat dan di lebih dari 100 negara.
- Serangan siber di tahun 2016 adalah serangan dari ransomware di 150 kota di dunia dan mulai "heboh" di Indonesia pada tahun 2017.
- Industri kesehatan telah menjadi target utama dari serangan siber.
- Ini merupakan isyarat bahwa **industri kesehatan juga tidak bebas dari ancaman**


- Data rekam medis dan sejenisnya saat ini telah menjadi sebuah "tambang emas" yang sangat bernilai ekonomis yang bisa diperjual-belikan
- Budaya keamanan informasi di antara para profesional kesehatan masih perlu ditingkatkan
- Institusi pelayanan kesehatan di seluruh dunia termasuk industri yang lamban di dalam menerapkan sistem keamanan informasi
- Terbatasnya regulasi keamanan informasi di sektor kesehatan

*Sumber: Daryo Soemitro, Supriantoro, Ardi Sutedja*

Industri kesehatan banyak menjadi target utama dari serangan siber, hal ini sesuai dengan gambar diatas yang menyatakan bahwa data kesehatan bernilai ekonomis, rendahnya kepedulian, lambannya adopsi sistem keamanan, dan terbatasnya regulasi.

Secara global juga telah memiliki komitmen untuk menjamin keamanan data kesehatan melalui; Resolusi WHA tahun2005 nomor58.28 bahwa "*all countries have integrated the use of Information and Communication Technologies in their national health information systems and health infrastructure*". Untuk mewujudkan hal itu,WHO mendorong kepada setiap negara untuk:antara lain memobilisasi kerjasama lintas sektor dalam mengadopsi norma dan standar e-kesehatan, evaluasi, prinsip-prinsipcost-effectiveness dalam e-kesehatan untuk menjamin mutu, etika, dan **keamanan** dengan tetap mengedepankan **kerahasiaan**, **privasi**,equity,dan equality.

**Kebijakan Keamanan Informasi Kesehatan**

a. Kebijakan(pengaturan) keamanan informasi kesehatan: secara umum sudah ada (UU, PP, Permenkes, Kepmenkes) ;

   a). Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

   b). Undang-undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik
   c). Peraturan Pemerintah Nomor 46 Tahun 2014

   d). Peraturan Menteri Kesehatan Republik Indonesia Nomor 92 Tahun 2014

   e). Peraturan Menteri Kesehatan Republik Indonesia Nomor 4 Tahun 2017 tentang E-Kesehatan

b. Rujukan standar sebagian sudah ada yang mengacu pada standar nasional (SNI), internasional (ISO), HIPAA

# Kebijakan Keamanan Informasi Kesehatan

Peta Jalan Sistem Informasi Kesehatan 2015-2019

- Prinsip Keamanan dan kerahasian. Sistem Informasi yang dikembangkan dapat **menjamin keamanan dan kerahasiaan data**.
- Strategi 5. Meningkatkan dan menyelenggarakan sistem pengumpulan, penyimpanan, analisis, dan diseminasi data secara sistematis.
  - Tersedianya pedoman, standar, petunjuk teknis pengelolaan data kesehatan secara elektronik yang meliputi pengumpulan, penyimpanan, diseminasi, dan **keamanan data**.
  - Tersedianya kebijakan dan SOP untuk Mekanisme pertukaran informasi (data sharing) diantara pemangku kepentingan dengan penekanan pada **prinsip keamanan dan kerahasiaan data/informasi**.

Strategi e-Kesehatan Nasional 2015-2019

- Misi 3. Memperluas dan meningkatkan layanan dan aplikasi sistem teknologi informasi dan komunikasi yang mampu meningkatkan kualitas proses kerja pelayanan kesehatan.
  - Menyediakan layanan digital signature untuk mendukung **keamanan data elektronik**
- Misi 6. Menata dan menguatkan peraturan, kebijakan, dan pemenuhan kebijakan e-kesehatan nasional sebagai landasan, arah, dan tujuan implementasi e-kesehatan ke depan, serta **menjamin integritas sistem layanan kesehatan**.

# Rujukan Standar

- SNI

| | |
|---|---|
| SNI ISO 27789:2014 | Informatika kesehatan – Jejak audit untuk rekam kesehatan elektronik |
| SNI ISO 27799:2014 | Informatika kesehatan – Manajemen keamanan informasi dalam bidang kesehatan menggunakan SNI ISO/IEC 27002 |

# Rujukan Standar

- ISO

| | |
|---|---|
| ISO/TS 21547:2010 | Health informatics -- Security requirements for archiving of electronic health records – Principles |
| ISO/TR 21548:2010 | Health informatics -- Security requirements for archiving of electronic health records – Guidelines |
| ISO/TS 13606-4:2009 | Health informatics -- Electronic health record communication -- Part 4: Security |
| ISO/TR 11633-1:2009 | Health informatics -- Information security management for remote maintenance of medical devices and medical information systems -- Part 1: Requirements and risk analysis |
| ISO/TR 11633-2:2009 | Health informatics -- Information security management for remote maintenance of medical devices and medical information systems -- Part 2: Implementation of an information security management system (ISMS) |
| ISO/TS 14441:2013 | Health informatics -- Security and privacy requirements of EHR systems for use in conformity assessment |
| ISO 22857:2013 | Health informatics -- Guidelines on data protection to facilitate trans-border flows of personal health data |

Penyelenggara Sistem Elektronik yang menyelenggarakan **Sistem Elektronik Strategis harus** menerapkan standar **SNI ISO/IEC 27001** dan ketentuan pengamanan yang ditetapkan oleh Instansi Pengawas dan Pengatur Sektornya Permenkominfo No 4/2016 -SMPI.

Organisasi yang memproses informasi kesehatan, termasuk informasi kesehatan pribadi, harus memiliki kebijakan tertulis tentang keamanan informasi kesehatan, yang disetujui oleh manajemen, dipublikasikan, dan kemudian disampaikan kepada semua karyawan dan pihak eksternal yang relevan. SNI ISO 27799:2014 Informatika kesehatan

Resiko yang akan muncul dalam keamanan sistem informasi, yaitu :

1. Threats (Ancaman) atas sistem dan
2. Vulnerability (Kelemahan) atas sistem

Masalah tersebut pada gilirannya berdampak kepada 6 hal yang utama dalam sistem informasi yaitu :

- Efektifitas
- Efisiensi
- Kerahaasiaan
- Integritas
- Keberadaan (availability)
- Kepatuhan (compliance)
- Keandalan (reliability)

Untuk menjamin hal tersebut maka keamanan sistem informasi baru dapat terkriteriakan dengan baik. Adapun kriteria yag perlu di perhatikan dalam masalah keamanan sistem informasi membutuhkan 10 domain keamanan yang perlu di perhatikan yaitu :

1. Akses kontrol sistem yang digunakan
2. Telekomunikasi dan jaringan yang dipakai
3. Manajemen praktis yang di pakai
4. Pengembangan sistem aplikasi yang digunakan
5. Cryptographs yang diterapkan
6. Arsitektur dari sistem informasi yang diterapkan
7. Pengoperasian yang ada
8. Busineess Continuity Plan (BCP) dan Disaster Recovery Plan (DRP)
9. Kebutuhan Hukum, bentuk investigasi dan kode etik yang diterapkan
10. Tata letak fisik dari sistem yang ada

Dari domain tersebutlah isu keamanan sistem informasi dapat diklasifikasikan berdasarkan ancaman dan kelemahan sistem yang dimiliki. Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Ancaman yang mungkin timbul dari kegiatan pengolahan informasi berasal dari 3 hal utama, yaitu :

1. Ancaman Alam
2. Ancaman Manusia
3. Ancaman Lingkungan

Yang termasuk dalam kategori ancaman alam terdiri atas :

- Ancaman air, seperti : Banjir, Tsunami, Intrusi air laut, kelembaban tinggi, badai, pencairan salju
- Ancaman Tanah, seperti : Longsor, Gempa bumi, gunung meletus
- Ancaman Alam lain, seperti : Kebakaran hutan, Petir, tornado, angin ribut

Yang dapat dikategorikan sebagai ancaman manusia, diantaranya adalah :

- Malicious code
- Virus, Logic bombs, Trojan horse, Worm, active contents, Countermeasures
- Social engineering
- Hacking, cracking, akses ke sistem oleh orang yang tidak berhak, DDOS, backdoor
- Kriminal
- Pencurian, penipuan, penyuapan, pengkopian tanpa ijin, perusakan
- Teroris
- Peledakan, Surat kaleng, perang informasi, perusakan

Yang dapat dikategorikan sebagai ancaman lingkungan seperti :

- Penurunan tegangan listrik atau kenaikan tegangan listrik secara tiba-tiba dan dalam jangka waktu yang cukup lama
- Polusi
- Efek bahan kimia seperti semprotan obat pembunuh serangga, semprotan anti api, dll
- Kebocoran seperti A/C, atap bocor saat hujan

Besar kecilnya suatu ancaman dari sumber ancaman yang teridentifikasi atau belum teridentifikasi dengan jelas tersebut, perlu di klasifikasikan secara matriks ancaman sehingga kemungkinan yang timbul dari ancaman tersebut dapat di minimalisir dengan pasti. Setiap ancaman tersebut memiliki probabilitas serangan yang beragam baik dapat terprediksi maupun tidak dapat terprediksikan seperti terjadinya gempa bumi yang mengakibatkan sistem informasi mengalami mall function.

Sedangkan yang dimaksud kelemahan (Vulnerability) adalah cacat atau kelemahan dari suatu sistem yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh pelaku yang mencoba menyusup terhadap sistem tersebut. Cacat sistem bisa terjadi pada prosedur, peralatan, maupun perangkat lunak yang dimiliki, contoh yang mungkin terjadi seperti : Seting firewall yang membuka telnet sehingga dapat diakses dari luar, atau Seting VPN yang tidak di ikuti oleh penerapan kerberos atau NAT.

Suatu pendekatan keamanan sistem informasi minimal menggunakan 3 pendekatan, yaitu :

1. Pendekatan *preventif* yang bersifat mencegah dari kemungkinan terjadikan ancaman dan kelemahan.
2. Pendekatan *detective* yang bersifat mendeteksi dari adanya penyusupan dan proses yang mengubah sistem dari keadaan normal menjadi keadaan abnormal.
3. Pendekatan *Corrective* yang bersifat mengkoreksi keadaan sistem yang sudah tidak seimbang untuk dikembalikan dalam keadaan normal

Tindakan tersebutlah menjadikan bahwa keamanan sistem informasi tidak dilihat hanya dari kaca mata timbulnya serangan dari virus, mallware, spy ware dan masalah lain, akan tetapi dilihat dari berbagai segi sesuai dengan domain keamanan sistem itu sendiri.

Sejalan dengan perkembangan teknologi informasi dan upaya memenuhi kebutuhan penerapannya dalam system pelayanan kesehatan, sudah banyak pihak yang berusaha mengembangkan system informasi pelayanan kesehatan berbasi komputer. Pihak isntitusi pelayanan kesehatan memiliki kesempatan untuk memilih dan mengimplementasikan aplikasi komputer dan system penunjangnya yang komprehensif. Tahap memilih ini dilaksanakan dengan melakukan evaluasi berdasarkan beberapan kriteria tertentu, termasuk salah satunya yaitu fitur keamanannya.

Fitur keamanan data dalam informasi kesehatan elektronik (electronic health information) merupakan kombinasi dari segi teknologi dan segi organisasi. Metoda yang dipilih untuk ini akan berdampak pula terhadap biaya, kompleksitas, dan tingkat keamanan yang dihasilkan. Peranan segi organisasi sama pentingnya dengan segi teknologi.

Fitur keamanan dalam system ini dibutuhkan untuk menjaga integritasi dan konfidensialitas informasi kesehatan yang terkandung di dalamnya. Selain itu juga dibutuhkan untuk melindungi privasi pasien dan memenuhi tuntutan kebutuhan perlindungan hukum bagi pasien, petugas kesehatan, serta institusi kesehatan.

Fitur keamanan yang dimaksud meliputi hal-hal sebagai berikut (National Academy of Sciences, 1997):

1. Otentikasi (authentication)
2. Otorisasi (authorization)
3. Integritas (integrity)
4. Penelusuran jejak (audit trails)
5. Pemulihan pasca bencana (disaster recovery)
6. Penyimpanan dan transmisi data yang aman (secure data storage & transmission)

Keberadaan fitur keamanan ini diharapkan dapat menjaga informasi kesehatan dalam sistem rekam kesehatan berbasis komputer terhadap:

1. Akses dari orang yang tidak berhak
2. Modifikasi yang tidak sah, baik dalam media penyimpanan data, selama proses pengolahan data maupun dalam pengiriman data
3. Timbulnya hambatan penggunaan sistem dan
4. Pengambilalihan sistem oleh pengguna yang tidak sah

Penjagaan informasi kesehatan ini juga termasuk pengawasan akses untuk mendeteksi, mencatat, dan melawan/ menahan ancaman-ancaman terhadap sistem. Penjagaan ini dilaksanakan dari mulai lapis terendah dalam transportasi data meliputi kabel, switch, router, dan transmititer, sampai lapis-lapis berikutnya yaitu lapis jaringan ( network layer), lapis informasi ( information layer), lapis perangkat lunak (software application layer), dan lapis manajerial (managerial layer). Lapis manajerial bertanggung jawab terhadap pengelolaan administrasi dan proses operasional system yang semua ini dibutuhkan untuk menjamin dan memantau terlaksananya kebijakan keamanan data.

Empat prinsip dasar yang harus dipenuhi oleh berkas rekam kesehatan agar dapat diterima sebagai bukti/ catatan fakta, yaitu:

1. Didokumentasikan sesuai dengan aturan prosedur yang berlaku
2. Disimpabn sesuai dengan aturan prosedur yang berlaku
3. Dibuat pada saat, atau segera setelah pelayanan diberikan
4. Dibuat oleh petugas kesehatan yang berwenang (memiliki hak, pengetahuan, dan kemampuan sesuai standar dalam tugasnya)

Empat prinsip dasar tersebut juga berlaku bagi rekam kesehatan berbasis elektronik. Untuk menunjang aspek keakuratan dan kepercayaan dari rekam kesehatan berbasis komputer, The Comprehensive Guide to Electronic Health Records merekomendasikan hal-hal berikut ini untuk diperhatikan:

1. Jenis computer yang digunakan dan penerimaannya sebagai peralatan uang standard an efisien
2. Metode perekaman yang digunakan dalam perngoperasiannya
3. Metode dan keadaan dari persiapan perekaman data, meliputi:
    a. Sumber dari informasi
    b. Prosedur untuk memasukkan data/informasi dan untuk mengambil informasi dari komputer
    c. Pengendalian dan pengujian untuk memastikan akurasi dajn reliabilitas data
4. Keaslian data/ informasi yang direkam (belum dimodifikasi).

Keamanan dari rekam kesehatan berbasis computer tidak lepas dari 2 aspek yang saling berkait erat yaitu privacy dan security. Privacy mengandung makna penjagaan keamanan berkas dati pelepasan informasi yang tidak semestinya ( wrongful disclosure), sedangkan security mengandung makna penjagaan berkas dari kerusakan (destruction), pengubahan data yang tidak sah (tampering), dan ganggungan akses (unavailable access).

Ancaman terhadap keamanan sistem rekam kesehatan berbasis komputer, baik secara fisik maupun non fisik / informasi, semakin nyata dan komplek. Untuk membangun system pengamanan yang handal dan efektif, dibutuhkan langkah yang mengintegrasikan model tradisional dan teknologi informasi. Tiga keuntungan utama yang diharapkan dari integrasi ini yaitu:

1. Integrasi data: informasi yang dihasilkan akan memiliki akurasi tinggi, sehingga petugas klinis, peneliti dan petugas kesehatan lainnya menjadi yakin bahwa setiap tindakan yang direkomendasikan sudah berdasarkan data yang valid.
2. Kerahasiaan: petugas klinis dan staf lainnya akan lebih tenang dan yakin dalam menjalankan tugasnya, berkaitan dengan adanya peraturan penjagaan keamanan dan kerahasiaan data dalam hal pelepasan informasi.
3. Ketersediaan informasi; petugas pelayanan kesehatan akan lebih lancar menjalankan tugasnya bila informasi yang dibutuhkan selalu siap pada saat dibutuhkan.

Kinerja system pengamanan data yang baik bergantung kepada tiga komponen esensial, yaitu manusia (people), proses (process), dan teknologi (technology). Ketiga komponen ini dibutuhkan untuk membangun dan mengembangkan system pengamanan dan program manajemen resiko.

Jenis-jenis ancaman terhadap keamanan data dalam system rekam kesehatan berbasis komputer meliputi:

1. Kesalahan pada aspek pengguna (human error), termasuk diantaranya yaitu terhapus, kerusakan tak disengaja, pembuangan sampah yang tidak sepatutnya, dan sebagainya
2. Gangguan dari alam (nature), termasuk api, air, petir, gempa, dan sebagainya
3. Gangguan teknis (technical), termasuk kegelapan backup, kegagalan sistem, virus komputer, kehilangan daya listrik, dan sebagainya
4. Tindakan yang disengaja, misalnya mencari informasi diluar kewenangannya, mengubah data diluar kewenangannya

Setiap bentuk ancaman bisa memiliki karakteristik yang berbeda dalam hal motif, sumber daya, jalur akses, dan kemampuan teknis. Latar belakang karakteristik yang berbeda-beda ini bisa menimbulkan tingkat resiko yang berbeda dan membutuhkan cara pengendalian yang berbeda pula.

## Fitur Keamanan dalam Rekam Kesehatan Berbasis Komputer

### Otentikasi (authentication)

Otentikasi mengandung pengertian berkaitan dengan penjaminan/ pemastian terhadap identitas suatu subyek atau obyek. Misalnya, pemastian bahwa seorang pengguna yang sah/ terdaftar (otentikasi pengguna). Pemastian bahwa sekumpukan sumber data yang diterima adalah sesuai dengan yang dibutuhkan juga merupakan contoh otentikasi, dalam hal ini otentikasi keaslian data.

Metode untuk menerapkan otentikasi yang aman merupakan kebutuhan yang esensial dalam system rekam kesehatan berbasis computer. Setiap pengguna memikul

tanggung jawab terhadap informasi kesehatan yang mereka masukkan, tambahkan, validasi, dan mereka lihat dalam sistem. Oleh karena itu, setiap pengguna harus bisa diidentifikasi secara unik, dibedakan satu dari lainnya. Kebijakan khusus harus diterbitkan oleh pihak institusi untuk mengatur disiplin penggunaan berikut sangsi bagi individu yang membocorkan identitas otentikasinya kepada pengguna lain.

Dengan perkembangan teknologi, saat ini otentikasi dapat berupa sistem identifikasi biometric, misalnya uji sidik jari; pemindaian retina; dan pengenalan suara. Otentikasi juga bisa berupa penggunaan kartu pintar (smart card), token, password, atau kombinasi dari bentuk-bentuk tersebut. Bentuk yang paling umum digunakan dalam sistem rekam kesehatan berbasis komputer adalah password. Jika password turut dicatat dam disimpan dalam sistem, maka harus diacak (encrypted) untuk menjaga keamanannya. Password juga perlu dibatasi penggunaannya dengan menentukan batas waktu kadaluarsanya.

Untuk meminimalkan kemungkinan dimana pengguna yang tidak sah memanfaatkan sistem yang sedang aktif yang ditinggalkan oleh pengguna lain yang sah, maka perlu ditunjang dengan kemampuan automatic logoff apabila sistem ditinggalkan tanpa aktifitas dalam selang waktu tertentu atau bila pengguna yang sah tersebut mengakses kembali ke dalam sistem melalui terminal kerja yang lain.

**Otorisasi (authorization)**

Otorisasi mengandung pengertian berkaitan dengan pengesahan hak yang meliputi pengesahan akses berdasarkan hak akses. Otorisasi mengatur lingkup hak dari seorang pengguna yang sah, meliputi hak akses terhadap fungsi sistem dan informasi yang terkandung didalamnya. Otorisasi diperkuat dengan kemampuan kendali akses (access control),pelayanan kerahasiaan (confidentiality services), dan pelayanan non-repudiasi (non- refudiation services).

**Kendali akses ( access control)**

Fitur ini melindungi system terhadap penggunaan dari yang tidak berhak , termasuk penggunaan system computer, jaringan, aplikasi perangkat lunak, dan berkas (file) data. Kendali akses berperan dalam memastikan bahwa pengguna, sistem komputer, dan program hanya dapat menggunakan sumber data yang memang berhak mereka gunakan dan untuk tujuan yang memang menjadi hak mereka. Kendali akses juga melindungi sistem dari penggunaan oleh yang tidak berhak, pelepasan informasi (disclosure), modifikasi (modification) dan perusakan/ penghancuran (destruction) sumber data.

**Pelayanan Kerahasiaan ( confidentiality services)**

Fitur ini menjaga sistem dari kemungkinan pelepasan informasi kepada pihak yang tidak berhak untuk mendapatkan informasi tersebut. Bila kendali akses melindungi file data dalam media penyimpanan dari kemungkinan dibaca oleh pengguna yang tidak berhak, maka pelayanan kerahasiaan menjaga kemungkinan dibacanya file data tersebut diluar penyimpanan data, misalnya setelah digunakan (dicopy) secara tidak sah. Bentuk paling umum dari fitur ini adalah dengan menggunakan penyandian data (encryption)

**Pelayanan non-repudiasi ( non-repudiation services/nrs)**

Fitur ini menjamin terpenuhinya tuntutan pengguna yang dinyatakan maupun yang ditampilkan, baik yang berasal dari nrs maupun yang bukan. Repudiasi mengandung pengertian dimana pengguna secara tidak sengaja menginterupsi atau membatalkan proses yang tengah berlangsung. Dengan kata lain, nrs mencegah pengguna dari kemungkinan memodifikasi data/ informasi secara sepihak atau membatalkan proses transaksi data yang tengah berlangsung, yang mana hal ini dapat menyebabkan kerusakan data. Pengguna anonymous patient IDs merupakan metode untuk mengatur tampilan informasi baik di layar computer maupun di kertas dengan hanya mencantumkan nomor rekam medis atau kode identitas lain tanpa menampilkan nama pasien. Penerapan metode ini dapat mengurangi kemungkinan bocornya informasi kepada pihak yang tidak berwenang atau tidak perlu mengetahui ( National Academy of Sciences, 1997)

**Integritas (integrity)**

Integritas mengandung pengertian bahwa informasi yang tersedia hanya diubah/ diolah untuk kebutuhan tertentu dan oleh pengguna tertentu yang berhak. Pengertian ini dapat diterapkan pada data (data integrity), program (program integrity), sistem ( system integrity), dan jaringan komputer ( network integrity)

Integritas data berkaitan dengan akurasi ( accuracy), konsistensi (consistency), dan kelengkapan (completeness) dari data. Hal ini terkait secara langsung dengan kualitas data yang bersangkutan dan dapat berpengaruh terhadap kualitas pelayanan kesehatan yang diberikan. Pemantauan integritas data harus dapat memastikan bahwa data tidak diubah atau dirusak melalui cara yang tidak sah. Kebijakan pengendalian integritas data memiliki empat komponen esensial yaitu pemantauan keamanan (secutiry measures), pengendalian prosedur (procedurals controls), penentuan tanggung jawab (assigned responsibility), dan penelusuran jejak (audit trails). Untuk memastikan integritas informasi, maka harus bisa memantau sumber data, tanggal dan waktu, dan isi dari setiap pengubahan. Jadi penambahan dan pengubahan harus bisa terlacak sampai ke sumbernya.

Integritas program berkaitan dengan kualitas dari disain perangkat lunak dan penjagaannya dari kemungkinan pengubahannya. Gangguan pada perangkat lunak (software bugs) dan kompleksitas disain perangkat lunak dapat berperan dalam mengakibatkan ketidaklengkapan atau bahkan kehilangan informasi yang seharusnya dihasilkan.

Integritas sistem merupakan kemampuan dari suatu sistem otomatis untuk menjaga fungsinya dari gangguan dan manipulasi yang tidak sah. Fitur-fitur dari perangkat keras dan perangkat lunak harus diuji secara periodic untuk memastikan berfungsinya sistem tersebut secara benar. Tersedianya sistem penyalinan dan prosedur pemulihan data (backup and recovery procedure) sangat penting untuk mengantisipasi pemulihan sistem secara cepat dan aman apabila terjadi kegagalan sistem. Integritas jaringan merupakan perluasan fitur integritas sistem dalam jaringan lokal maupun jaringan yang lebih luas (local and wide area networks).

**Penelusuran jejak (audit trails)**

Fitur ini berfungsi untuk memantau setiap operasi terhadap sistem informasi. Penelusuran jejak harus mampu mencatat secara kronologis setiap aktifitas terhadap sistem. Pencatatan ini dilakukan segera dan sejalan dengan aktifitas yang terjadi (konkuren). Fitur ini dapat dimanfaatkan untuk mendeteksi dan melacak penyalahgunaan dan pelanggaran keamanan, menentukan dilaksanakan tidaknya kebijakan dan prosedur operasional yang berlaku, serta untuk merekontruksi rangkaian aktifitas yang dilakukan terhadap sistem.

Catatan yang dihasilkan oleh fitur penelusuran jejak hendaknya berisi informasi tentang identitas pengguna, sumber data yang diakses, identitas pasien yang diakses datanya, identitas fasilitas pelayanan kesehatan, kode lokasi akses, tanggal dan waktu akses, dan jenis aktifitas yang dilakukan (termasuk fungsi sistem yang diaktifkan dan jenis informasi yang diakses).

**Pemulihan pasca bencana ( disaster recovery)**

Fitur pemuliham pasca bencana merupakan proses yang memungkinkan institusi untuk memulihkan kembali data-data yang hilang atau rusak setelah terjadinya suatu gangguan/ bencana, misalnya kebakaran; banjir; huru-hara; bencana alam; atau kegagalan system.

Sistem yang difungsikan harus menunjang kemampuan tersedianya cadangan terhadap komponen sistem seperti misalnya prosesor, jalur jaringan (network links), dan basis data. Sistem juga harus memiliki kemampuan untuk penyalinan data (backup) tanpa mengganggu fungsi-fungsi lainnya dan mampu membangun kembali informasi dari salinan data tersebut.

**Penyimpanan dan transmisi data yang aman (secure data storage&transmission)**

Penyimpanan data berkaitan dengan media fisik dan lokasi dimana data disimpan dan dikelola. Transmisi data berkaitan dengan aktifitas petukaran data antara pengguna dan program atau antara program dan program, dimana pengirim dan penerima dipisahkan oleh suatu jarak.

Pertimbangan fisik dari media penyimpanan data meliputi keamanan fisik dari prosesor, media penyimpan, kabel, terminal kerja, dan sebagainya. Perawatan dan pengelolaan terhadap media ini ditujukan untuk menjaga media penyimpanan data terhadap kemungkinan sabotase dan gangguan fisik lainnya. Jadwal retensi juga perlu dipertimbangkan dan diterapkan dalam penggunaan media penyimpanan data elektronik ini. Jadwal retensi ini disesuaikan dengan peraturan yang berlaku dan juga dengan kebutuhan di lingkungan institusi yang bersangkutan, misalnya untuk kebutuhan pelayanan pasien;penelitian; dan pendidikan.

Transmisi data yang diimplementasikan dalam sistem rekam kesehatan berbasis komputer menjadi hal yang penting untuk diperhatikan karena sistem pelayanan kesehatan saat ini membutuhkan kemampuan untuk “menangkap” data dari berbagai tempat berpisah. Data yang telah berkumpul dari berbagai sumber ini juga akan

ditransmisikan ke berbagai sumber ini juga akan ditransmisikan ke berbagai tempat untuk berbagai keperluan. Sistem yang menunjang kemampuan untuk transmisi data harus juga mampu menjamin integritas dan kerahasiaan data yang dikelola (Computer-based Patient Record Institut, 1999; National Academy of Sciences, 1997)