Modul Proteksi dan Pertukaran Informasi Kesehatan

ONLINE 7 dan 8

Privacy, Security, and Confidentiality: Toward Trust

Trust is having confidence in how another party will behave in a given situation. If you have a high degree of confidence in how another party will behave in a given situation, then you have a high degree of trust in that other party. If the behavior of another party is unknown in a given situation, then the degree of trust in that party is low. Laws, rules, regulation, and contracts exist to foster trust. They define how particular parities should behave in given situations. In a contract, one party might promise to do A in situation Z and B in situation X. The contract establishes expected behaviors in given situations and acts as a mechanism to enforce behaviors or apply penalties if a party does not behave as required by the contract. As parties behave according to the contract over time, more and more trust is established.

Laws, administrative rules, and regulations work in much the same way. A law might say if Z occurs, then all regulated parties must do A. The law or regulation will carry with it enforcement penalties to which regulated parties will be subject if they do not comply with the law. As parties comply with the law or regulation over time, more and more trust is established across the society.

These concepts of trust, built over time through contract, laws, and regulations, are paramount in developing a successful health information exchange (HIE). Health-care providers and health plans are trusted by their patients and members to safeguard health information. In order for these entities to share health information, a sufficient fabric of trust must be created by the HIE through contracts and practices, as well as laws and regulations at both state and federal levels. Compliance with HIE contracts as well as applicable laws and regulations is demonstrated through strong HIE governance (as described in chapter: Engaging and Sustaining Stakeholders: Toward Governance), which breads further trust.

As HIE participants work together over time, they develop a higher degree of certainty in how each other will act in a given situation, which translates into a higher degree of trust. The concepts of privacy, security, and confidentiality are established through contracts, laws, and regulations. They represent situations in which parties must develop a high degree of certainty around how other parties will act (ie, trust) in order for an HIE initiative to be successful. It is the combination of contracts, laws, and regulations that define expected behaviors around privacy, security, and confidentiality
that establish the trust necessary for a successful HIE.

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.

Sensitive Data

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. State laws will generally impose more stringent patient consent requirements on the disclosure of these types of data. HIPAA and federal law generally do not provide additional protections or consent requirements upon communicable or sexually transmitted diseases. 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).

These types of data require specific patient consent each time they are disclosed. It is important for any HIE initiative to research state and federal laws relating to sensitive data and determine how such data will be handled by the HIE. Many HIEs take the approach of prohibiting their participants from sending HIPAA psychotherapy notes and Part II drug and alcohol addiction treatment information. They will also take the same approach with respect to state-regulated sensitive data. This way the HIE never handles data that have special consent requirements attached to it. Rather than outright prohibiting such types of data, some HIEs require that their participants specifically represent and warrant that consent for disclosure has been obtained for any data that are shared with the HIE. This allows sensitive data types to be shared via the HIE, but imposes additional administrative burdens upon HIE participants.

HIPAA and the HITECH Act The primary federal laws applicable to HIE initiatives is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act). HIPAA was passed in 1996 and allowed for the Department of Health and Human Services (HHS) to issue privacy and security regulations. HHS implemented these regulations in what are known as the Privacy Rule (finalized in December of 2000) and the Security Rule (finalized in February of 2003). In 2009, as part of the American Recovery and Reinvestment Act (ARRA or the Stimulus Package), the HITECH Act was passed and, among other things, made a number of changes to

HIPAA, which were implemented through regulations issued by HHS (most of which were finalized in Jan. 2013, some of which are still forthcoming). These two laws (HIPAA and HITECH) and their implementing regulations (the Privacy Rule and the Security Rule) create the federal floor of laws and regulations that impact HIE's use and disclosure of PHI.

What is Regulated?

HIPAA, by virtue of the Privacy Rule, the Security Rule, and the HITECH Act, applies to "covered entities" and their "business associates." 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 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.

HIPAA requires that all covered entities have contracts with their business associates (called business associate agreements or BAAs). BAAs must contain a number of specific provisions regarding confidentiality and security. Before the HITECH Act, business associates were not directly subject to HIPAA, they were merely obligated to comply with the terms of their BAAs with covered entities. This left the federal government in a difficult position whenS a business associate suffered a breach of PHI.

The federal government had no direct recourse against the business associate; it was left to the covered entity to pursue contractual remedies against the business associate under its BAA. To avoid this lack of recourse, the HITECH Act provided that business associates must now comply with all aspects of the Security Rule and virtually all of the aspects of the Privacy Rule. This means that the federal government now has a direct cause of action against a business associate in the event of a breach.

Having established that covered entities and business associates are the entities regulated by HIPAA, the next question is: What type of information is subject to HIPAA? HIPAA regulates *protected health information*, which is individually identifiable health information transmitted or maintained in any form or medium (excluding certain education records and student medical records). *Individually identifiable health information* is health information, including demographic information, created or received by a covered entity that relates to the past, present, or future physical or mental health or condition of an individual that identifies the individual or could reasonably be used to identify the individual.

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

1. Names

2. 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
3. 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
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code, except for certain coding systems that allow for reidentification of data.

These identifiers are broad and show that HHS takes an expansive view in determining what might reasonably be used to identify an individual. Many individuals hold the false belief that if they simply remove a name they have deidentified PHI. The truth is that only once these 18 identifiers are removed from PHI, will the PHI be considered “deidentified” under HIPAA and no longer subject to regulation under HIPAA?. Covered entities (and their business associates with permission from their covered entity) may deidentify PHI and use deidentified information for any purpose. This is an important term to consider in any covered entity–business associate relationship:

Will the covered entity permit the business associate to deidentify PHI and use the deidentified information for other purposes? Many vendors seek to deidentify information and monetize it through sales or licensing arrangements. Some HIEs could benefit and increase their sustainability if they are permitted to deidentify PHI and use the deidentified data for other purposes. Deidentification can raise privacy concerns as individuals may feel that a third party should not profit from the use of their deidentified data.

Deidentified data can also be used for many public goods by researchers looking to promote public health or analyze the efficacy of different treatments. The issue of deidentification is an important one to discuss with HIE stakeholders and reach agreement upon how the issue will be addressed by an HIE.

The Privacy Rule and the Security Rule Knowing who (covered entities and business associates) and what (PHI) is regulated by HIPAA, the next question is: What is

required under HIPAA? The Privacy Rule establishes permissible uses and disclosures of PHI and the Security Rule establishes a set of required and addressable security controls. The Privacy Rule Under the Privacy Rule, covered entities and business associates may only use or disclose PHI if the Privacy Rule permits the particular use or disclosure or if the person who is the subject of the PHI authorizes the use or disclosure. 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:

1. To the individual to whom the PHI relates
2. For treatment, payment, or health-care operations
3. For public health activities
4. As required by law
5. For certain research activities where a privacy board or an institutional review board has waived the authorization requirement.

Except in the case of treatment, the Privacy Rule requires that covered entities and business associates make reasonable efforts to limit uses and disclosures of PHI to the minimum amount necessary to accomplish the intended use or disclosure. For the purposes of an HIE, most uses and disclosures will be for treatment, health-care operations, or public health activities. Just because the Privacy Rule permits a particular use or disclosures does not mean that a business associate (or an HIE) may automatically make such use or disclosure; the business associate (or an HIE) must obtain permission from its covered entity(ies) to make a particular use or disclosure. It is critical that an HIE establish the types of uses and disclosures that will be made of data shared with the HIE and obtain appropriate permissions for such uses and disclosures in its agreement (including a BAA) with the HIE participants.

HIE use cases for treatment purposes are fairly straightforward and self-explanatory. For example, providing data at the point of care or delivering a clinical lab result is a treatment disclosure. Public health use cases encompass, for example, delivering immunization reports to public health authorities or providing data for public health syndromic surveillance. Health-care operations use cases that are emerging as the next frontier of HIE use cases. Health-care operations includes, among other things, conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities; population-based activities relating to improving health or reducing health-care costs, protocol development, case management and care coordination, contacting of health-care providers and patients with information about treatment alternatives; and related functions that do not include treatment.

These uses and disclosures, sometimes called “secondary use,” are some of the higher value services that an HIE can offer. As these are permitted under the privacy rule without patient authorization, it is important for an HIE to secure permission from its covered entity participants for the HIE to make these uses of PHI if these services are part of the HIE’s plans. An important change that the HITECH Act made to the Privacy Rule is in the area of requests by patients for their information not to be shared in certain circumstances. The Privacy Rule provides that patients may request that covered entities not to make certain uses or disclosures of their information.

The Privacy Rule goes on to state that covered entities are not obligated to grant such requests except in one situation. That situation is when a patient pays out-of-pocket in full for health care and requests that their health-care provider not share information relating to such health care with the patient’s health plan. In this situation the provider must honor the request and refrain from sharing the information with the patient’s health plan. This can create unique challenges for HIEs that share data with health plans, as many do and as more and more will to increase their sustainability. HIEs must have in place a mechanism for their health-care provider participants to either; (1) not send information that is subject to a restriction request or z2) notify the HIE that certain data are subject to a restriction request so that the HIE can take steps to ensure that the data are not shared with the patient’s health plan. This right is rarely exercised by patients, but it is nonetheless something for which HIEs must be prepared if they are going to share data with health plans.

The Privacy Rule establishes the situations in which covered entities and business associates may use and disclose PHI. The Privacy Rule is sometimes used as an excuse for providers and health plans to not share data with each other. The truth is that the Privacy Rule is designed to allow sharing of health data among healthcare providers and health plans in the interest of patient treatment, improving quality, and population health management. If an entity is declining to share data because “HIPAA does not allow it,” it is important to do a deep analysis to determine what provision of HIPAA does not allow the particular data sharing.

The truth is that if the sharing would enhance patient care or public health, then it is probably allowed under HIPAA. HIPAA does a good job of protecting confidentiality by limiting uses and disclosures to covered entities and business associates and then ensuring confidentiality by imposing security control requirements upon covered entities and business associates under the Security Rule.

The Security Rule The Privacy Rule establishes permissible uses and disclosures of PHI. The Security Rule is equally as important in establishing the baseline security controls that are required or addressable by covered entities and business associates. The Security Rule establishes a number of general requirements that apply to all covered entities and business associates and then describes a number of implementation specifications that are either “required” or “addressable” by covered entities and business associates. This framework provides a great deal of flexibility and allows covered entities and business associates to consider their size, complexity, capabilities, technical infrastructure, cost and probability and criticality of potential risks when implementing security controls.

If a particular control is required (shown as (R) in Table 6.1), then it must be implemented by a covered entity or business associate. If a particular control is addressable (shown as (A) in Table 6.1), then the covered entity or business associate must assess whether each control is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting PHI and either implement the control or document its decision to not implement the control. The controls are divided into three categories: Administrative, Physical, and Technical, as shown and described in Table 6.1.

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: • Risk assessment (R) • Reduce risk to an appropriate level (R) • Workforce sanctions (R) • Review system activities (R)	*Facility access controls*—Policies and procedures to limit physical access to PHI, including: • Contingency operations plans (A) • Facility security plan (A) • Access control and validation procedures (A) • 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: • Unique user identification (R) • Emergency access (R) • Automatic logoff (A) • 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: • Authorization and supervision of employees (A) • Clearance of workforce members (A) • 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: • 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: • Isolating health-care clearinghouse functions (R) • Access authorization policies (A) • 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: • Disposal of media (R) • Media reuse (R) • Accountability for movement (A) • 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: • Security reminders (A) • Protection from malicious software (A) • Log-in monitoring (A) • Password management (A) *Security incident procedures*—Policies and procedures to address security incidents through response and reporting (R) *Contingency plan*—Policies and procedures for responding to emergencies and system failures, including: • Data backup (R) • Disaster recovery plan (R) • Emergency operation plan (R) • Testing and revision of plans (A) • Application and data criticality analysis (A) *Evaluation*—Perform periodic technical and nontechnical evaluations of security controls (R) *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: • Integrity controls (A) • Encryption (A)

Istilah keamanan (security) dan proteksi (protection)sering digunakan secara bergantian. Untuk menghindari kesalahpahaman, istilah keamanan mengacupada seluruh masalah keamanan dan istilah mekanisme proteksi mengacu ke mekanisme system yang digunakan untuk memproteksi/melindungi informasi pada system computer. Keamanan diperlukan adalah untuk menjhaga dan menjamin sumber daya tidak dicuri ataupun dimodifikasi orang tak terotorisasi. Pemanganan termasuk masalah teknis, manajerial, legalitas dan politis. Keamanan system terbagi menjadi tiga, yaitu :

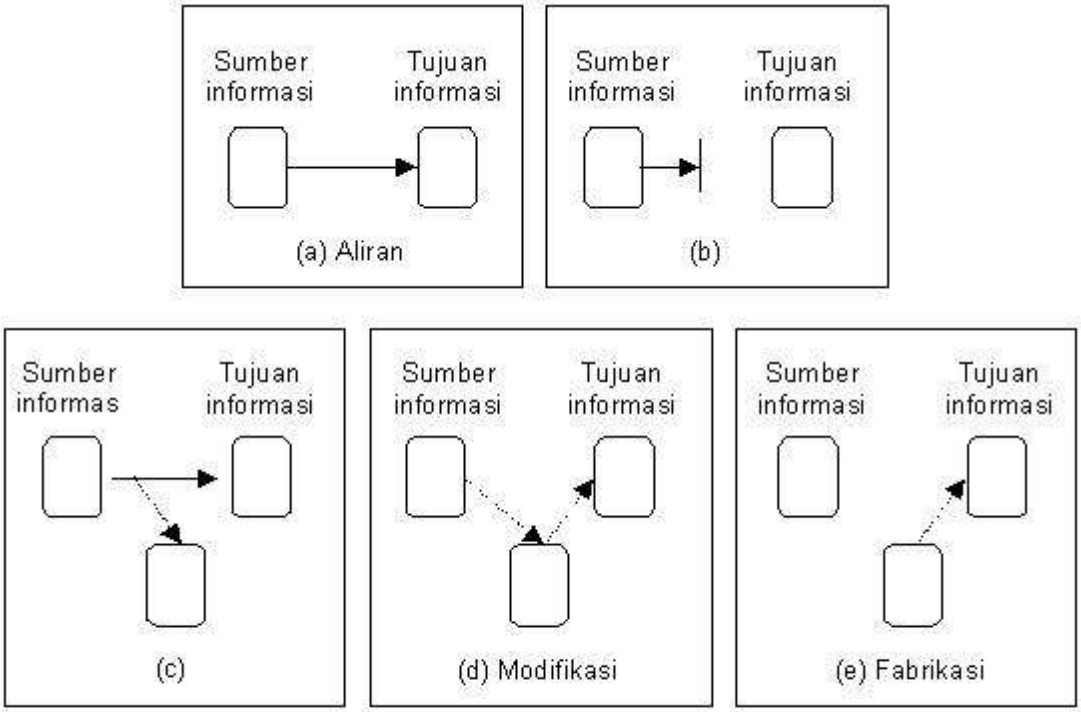
1. External Security: External Security atau keamanan eksternal adalah keamanan yang berkaitan dengan pemanganan fasilitas computer dari penyusup atau hacker dan bencana seperti kebakaran dan kebanjiran.
2. User Interface Security: User Interface Security atau keamanan interface pemakai adalah keamanan yang berkaitan dengan identifikasi pemakai sebelum pemakai diijinkan mengakses program dan data yang disimpan.
3. Internal Security: Internal Security atau keamanan internal adalah keamanan yang berkaitan dengan pengamanan beragam kendali yang dibangun pada perangkat keras dan system operasi yang menjamin operasi yang handal dan tak terkorupsi untuk menjaga integritas program dan data.

Untuk menghindari, mencegah dan mengatasi ancaman itulah sasaran dari pengamanan. Kebutuhan keamanan system computer dikatagorikan tiga aspek, yaitu :

1. Kerahasiaan (secrecy): Kerahasiaan dalah keterjaminan bahwa informasi disistem komputer hanya dapat diakses oleh pihak-pihak yang diotorisasi dan modifikasi tetap menjaga konsistensi dan keutuhan data di sistem.
2. Integritas (integrity): Integritas adalah keterjaminan bahwa sumber daya sistem komputer hanya dapat dimodifikasi oleh pihak-pihak yang diotorisasi.
3. Ketersediaan (availability): Ketersediaan adalah Adalah keterjaminan bahwa susmber daya sistem komputer tersedia bagi pihak-pihak yang diotorisasi saat diperlukan.

Tipe-tipe ancaman terhadap keamanan sistem dapat dimodelkan dengan memandang fungsi sistem komputer sebagai penyedia informasi. Berdasarkan fungsi ini, ancaman terhadap sistem komputer dapat dikategorikan menjadi empat ancaman,yaitu :

1. Interupsi (interuption). Sumber daya sistem komputer dihancurkan atau menjadi tak tersedia atau tak berguna. Interupsi merupakan ancaman terhadap ketersediaan. Contoh : penghancuran bagian perangkat keras, seperti harddisk, pemotongan kabel komunikasi.
2. Intersepsi (interception). Pihak tak diotorisasi dapat mengakses sumber daya. Interupsi merupakan ancaman terhadap kerahasiaan. Pihak tak diotorisasi dapat berupa orang atau program komputer. Contoh : penyadapan untuk mengambil data rahasia, mengetahui file tanpa diotorisasi.
3. Modifikasi (modification). Pihak tak diotorisasi tidak hanya mengakses tapi juga merusak sumber daya. Modifikasi merupakan ancaman terhadap integritas. Contoh : mengubah nilai-nilai file data, mengubah program sehingga bertindak secara berbeda, memodifikasi pesan-pesan yang ditransmisikan pada jaringan.
4. Fabrikasi (fabrication). Pihak tak diotorisasi menyisipkan/memasukkan objek-objek palsu ke sistem. Fabrikasi merupakan ancaman terhadap integritas. Contoh : memasukkan pesan-pesan palsu ke jaringan, penambahan record ke file.



Gambar 9.1 : Skema ancaman-ancaman terhadap sistem komputer.

Keamanan Sistem Operasi

Telah disebutkan bahwa keamanan system operasi dapat kita dapatkan dengan menggunakan protocol user, proaktif password, firewall, enkripsi yang mendukung, logging, mendeteksi penyusup, dan keamanan system file

1. Protokol

   User Datagram Protocol salah satu protokol lapisan transpor TCP/IP yang mendukung komunikasi yang tidak andal (unreliable), tanpa koneksi (connectionless) antara host-host dalam jaringan yang menggunakan TCP/IP. Protokol ini didefinisikan dalam RFC 768.

   Karakteristik User datagram protocol memiliki beberapa karakteristik, yaitu :

   a. Connectionless (tanpa koneksi): Pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negosiasi koneksi antara dua host yang hendak berukar informasi.
   b. Unreliable (tidak andal): Pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan acknowledgment. Protokol lapisan aplikasi yang berjalan di atas UDP harus melakukan pemulihan terhadap pesan-pesan yang hilang selama transmisi. Umumnya, protokol lapisan aplikasi yang berjalan di atas UDP mengimplementasikan layanan keandalan mereka masing-masing, atau mengirim pesan secara periodik atau dengan menggunakan waktu yang telah didefinisikan.
   c. UDP menyediakan mekanisme untuk mengirim pesan-pesan ke sebuah protokol lapisan aplikasi atau proses tertentu di dalam sebuah host dalam jaringan yang menggunakan TCP/IP. Header UDP berisi field Source Process Identification dan Destination Process Identification.

d. UDP menyediakan penghitungan checksum berukuran 16-bit terhadap keseluruhan pesan UDP. Penggunaan UDP UDP juga sering digunakan untuk melakukan tugas-tugas seperti berikut :
    a) Protokol yang "ringan" (lightweight): Untuk menghemat sumber daya memori dan prosesor, beberapa protokol lapisan aplikasi membutuhkan penggunaan protokol yang ringan yang dapat melakukan fungsi-fungsi spesifik dengan saling bertukar pesan. Contoh dari protokol yang ringan adalah fungsi query nama dalam protokol lapisan aplikasi Domain Name System.
    b) Protokol lapisan aplikasi yang mengimplementasikan layanan keandalan: Jika protokol lapisan aplikasi menyediakan layanan transfer data yang andal, maka kebutuhan terhadap keandalan yang ditawarkan oleh TCP pun menjadi tidak ada. Contoh dari protokol seperti ini adalah Trivial File Transfer Protocol (TFTP) dan Network File System (NFS).
    c) Protokol yang tidak membutuhkan keandalan. Contoh protokol ini adalah protokol Routing Information Protocol (RIP).
e. Transmisi broadcast: Karena UDP merupakan protokol yang tidak perlu membuat koneksi terlebih dahulu dengan sebuah host tertentu, maka transmisi broadcast pun dimungkinkan. Sebuah protokol lapisan aplikasi dapat mengirimkan paket data ke beberapa tujuan dengan menggunakan alamat multicast atau broadcast. Hal ini kontras dengan protokol TCP yang hanya dapat mengirimkan transmisi one-to-one. Contoh: query nama dalam protokol NetBIOS Name Service.

2. Firewall

Firewall adalah adalah suatu sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk bisa melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman. Umumnya, sebuah tembok-api diterapkan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dengan jaringan Internet.

Tembok-api digunakan untuk membatasi atau mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini, istilah firewall menjadi istilah lazim yang merujuk pada sistem yang mengatur komunikasi antar dua macam jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke Internet dan juga tentu saja jaringan berbadan hukum di dalamnya, maka perlindungan terhadap perangkat digital perusahaan tersebut dari serangan para peretas, pemata-mata, ataupun pencuri data lainnya, menjadi kenyataan.

Jenis-Jenis Firewall

a. Personal Firewall: Personal Firewall didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki. Firewall jenis ini akhir-akhir ini berevolusi menjadi sebuah kumpulan program yang bertujuan untuk mengamankan komputer secara total, dengan ditambahkannya beberapa fitur pengaman tambahan semacam perangkat proteksi terhadap virus, anti-spyware, anti-spam, dan lainnya. Bahkan beberapa produk firewall lainnya dilengkapi dengan fungsi pendeteksian gangguan keamanan jaringan (Intrusion Detection System).

Contoh dari firewall jenis ini adalah MicrosoftWindows Firewall (yang telah terintegrasi dalam sistem operasi Windows XP Service Pack 2, Windows Vista dan Windows Server 2003 Service Pack 1),Symantec Norton Personal Firewall, Kerio Personal Firewall, dan lain-lain. Personal Firewall secara umum hanya memiliki dua fitur utama, yakni Packet Filter Firewall dan Stateful Firewall.

b. Network Firewall: Network ‘”’Firewall didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya dijumpai dalam dua bentuk, yakni sebuah perangkat terdedikasiatau sebagai sebuah perangkat lunak yang diinstalasikan dalam sebuah server. Contoh dari firewall ini adalah Microsoft Internet Security and Acceleration Server (ISA Server), Cisco PIX, Cisco ASA, IPTables dalam sistem operasi GNU/Linux, pf dalam keluarga sistem operasi Unix BSD, serta SunScreen dari Sun Microsystems, Inc. Yang dibundel dalam sistem operasi Solaris. Network Firewall secara umum memiliki beberapa fitur utama, yakni apa yang dimiliki oleh personal firewall (packet filter firewall dan stateful firewall), Circuit Level Gateway, Application Level Gateway, dan juga NAT Firewall. Network Firewall umumnya bersifat transparan (tidak terlihat) dari pengguna dan menggunakan teknologi routing untuk menentukan paket mana yang diizinkan, dan mana paket yang akan ditolak.

Firewall memiliki beberapa fungsi yang sangat penting, diantaranya adalah :

a. Mengatur dan mengontrol lalu lintas jaringan.
b. Melakukan autentikasi terhadap akses.
c. Melindungi sumber daya dalam jaringan privat.
d. Mencatat semua kejadian, dan melaporkan kepada administrator.

3. Enkripsi

Enkripsi adalah Enkripsi adalah proses mengacak data sehingga tidak dapat dibaca oleh pihak lain. Pada kebanyakan proses enkripsi, Anda harus menyertakan kunci sehingga data yang dienkripsi dapat didekripsikan kembali.Ilmu yang mempelajari teknik enkripsi disebut kriptografi. Gambaran sederhana tentang enkripsi, misalnya mengganti huruf a dengan n, b dengan m dan seterusnya. Model penggantian huruf sebagai bentuk enkripsi sederhana ini sekarang tidak dipergunakan secara serius dalam penyembunyian data.

ROT-13 adalah program yang masih suka dipergunakan. Intinya adalah mengubah huruf menjadi 23 huruf didepannya. Misalnya b menjadi o dan seterusnya. Pembahasan enkripsi akan terfokus pada enkripsi password dan enkripsi komunikasi data.f. Otentifikasi Pemakai Kebanyakan proteksi didasarkan asumsi sistem mengetahui identitas pemakai. Masalah identifikasi pemakai ketika login disebut otentifikasi pemakai (user authentication). Kebanyakan metode otentifikasi didasarkan pada tiga cara, yaitu :

a. Sesuatu yang diketahui pemakai, misalnya :
    a) Password.
    b) Kombinasi kunci.
    c) Nama kecil ibu mertua.
    d) Dan sebagainya.
b. Sesuatu yang dimiliki pemakai, misalnya :

a) Badge.
b) Kartu identitas.
c) Kunci.
d) Dan sebagainya.

c. Sesuatu mengenai (ciri) pemakai, misalnya :
a) Sidik jari.
b) Sidik suara.
c) Foto.
d) Tanda tangan.

4. Password

Pemakai memilih satu kata kode, mengingatnya dan mengetikkan saat akan mengakses sistem komputer. Saat diketikkan, komputer tidak menampilkan dilayar. Teknik ini mempunyai kelemahan yang sangat banyak dan mudah ditembus. Pemakai cenderung memilih password yang mudah diingiat. Seseorang yang kenal dengan pemakai dapat mencoba login dengan sesuatu yang diketahuinya mengenai pemakai.
Proteksi password dapat ditembus dengan mudah, antara lain :

a. Terdapat file berisi nama depan, nama belakang, nama jalan, nama kota dari amus ukuran sedang, disertai dengan pengejaan dibalik), nomor plat mobil yang valid, dan string-string pendek karakter acak.
b. Isian di file dicocokkan dengan file password. Upaya untuk lebih mengamankan proteksi password, antara lain :
a) Salting. Menambahkan string pendek ke string password yang diberikan pemakai sehingga mencapai panjang password tertentu.
b) One time password. Pemakai harus mengganti password secara teratur. Upaya ini membatasi peluang password telah diketahui atau dicoba-coba pemakai lain. Bentuk ekstrim pendekatan ini adalah one time password, yaitu pemakai mendapat satu buku berisi daftar password. Setiap kali pemakai login, pemakai menggunakan password berikutnya yang terdapat di daftar password Dengan one time password, pemakai direpotkan keharusan menjaga agar buku passwordnya jangan sampai dicuri.
c) Satu daftar panjang pertanyaan dan jawaban. Variasi terhadap password adalah mengharuskan pemakai memberi satudaftar pertanyaan panjang dan jawabannya. Pertanyaan-pertanyaan dan jawabannya dipilih pemakai sehingga pemakai mudah mengingatnya dan tak perlu menuliskan di kertas. Pertanyaan berikut dapat dipakai, misalnya : Dimana Tempat Lahir Anda ?; Apa hobi ayah Anda ? Pada saat login, komputer memilih salah satu dari pertanyaan-pertanyaan secara acak, menanyakan ke pemakai dan memeriksa jawaban yang diberikan.
d) Tantangan tanggapan (chalenge response). Pemakai diberi kebebasan memilih suatu algoritma, misalnya x3. Ketika pemakai login, komputer menuliskan di layar angka 3. Dalam kasus ini pemakai mengetik angka 27. Algoritma dapat berbeda di pagi, sore, dan hari berbeda, dari terminal berbeda, dan seterusnya.

5. Identifikasi Fisik
   Pendekatan lain adalah memberikan yang dimiliki pemakai, seperti : Kartu berpita magnetik Kartu pengenal dengan selarik pita magnetik. Kartu ini disisipkan ke suatu perangkat pembaca kartu magnetik jika akan mengakses komputer. Teknik ini biasanya dikombinasikan dengan password, sehingga pemakai dapat login sistem komputer bila memenuhi dua syarat berikut :
   a. Mempunyai kartu.
   b. Mengetahui password yang spesifik kartu itu.
   c. ATM merupakan mesin yang bekerja dengan cara ini.

6. Sidik jari
   Pendekatan lain adalah mengukur ciri fisik yang sulit ditiru, seperti:
   a. Sidik jari dan sidik suara.
   b. Analisis panjang jari.
   c. Pengenalan visual dengan menggunakan kamera diterapkan.
   d. Dan sebagainya.

7. Analisis tanda tangan
   Disediakan papan dan pena khusus dimana pemakai menulis tanda tangan. Pada teknik ini, bukan membandingkan bentuk tanda tangan tapi gerakan (arah) dan tekanan pena saat menulis. Seorang dapat meniru bentuk tanda tangan tapi sulit meniru persis cara (gerakan dinamis dan irama tekanan) saat pembuatan tanda tangan.
   Analisis suatu yang dipunyai pemakai Pendekatan lain adalah meniru perilaku kucing dan anjing dalam menandai batas wilayah, yaitu urine. Disediakan alat urunalysis. Bila pemakai ingin login, maka pemakai harus membawa sampel urine-nya. Sampel urine dimasukkan ke tabung dan segera dilakukan analisis dan ditentukan apakah termasuk salah satu pemakai sistem. Urinalysis harus dapat dilakukan sesaat. Pendekatan pengamanan yang bagus, tapi tidak diterima secara psikologis.

8. Analisis darah
   Disediakan satu jarum dimanan pemakai dapat mencobloskan jari sampai menetes darahnya. Darah itu kemudian dianalisis dengan spektografi (blood spectographic analysis). Dari analisis dapat ditentukan mengenai pemilik darah. Pendekatan ini relatif aman tapi tidak diterima secara psikologis.

Keamanan data (security) merupakan metode proteksi/sistem terhadap akses atau modifikasi yang sah. Dalam bidang kesehatan (*health care*) masalah privacy merupakan topik yang sangat serius di Amerika Serikat. *Health Insurance Portability and Accountability Act* (HIPPA), dikatakan akan mulai digunakan di tahun 2002, mengatakan bahwa rumah sakit, perusahaan asuransi, dan institusi lain yang berhubungan dengan kesehatan harus menjamin keamanan dan privacy dari data-data pasien.

Data-data yang dikirim harus sesuai dengan format standar dan mekanisme pengamanan yang cukup baik. Dalam pasal 13 ayat (1) huruf b permenkes 269 tahun 2008 tentang pemanfaatan rekam medis “sebagai alat bukti hukum dalam proses penegakkan hukum, disiplin kedokteran dan kedokteran gigi dan penegakkan etika kedokteran dan etika kedokteran gigi”.

Karena rekam medis merupakan dokumen hukum,maka keamanan berkas sangatlah penting untuk menjaga keabsahan data baik Rekam Kesehatan kertas maupun Rekam Kesehatan Elektronik (RKE). RKE juga merupakan alat bukti hukum yang sah. Hal tersebut juga ditunjang dengan Undang-Undang Informasi dan Transaksi Elektronik (ITE) pada pasal 5 dan 6 yaitu:

Pasal 5 :

Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

Informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik yang sesuai dengan ketentuan yang diatur dalan Undang-Undang ini

Pasal 6:

Dalam hal terdapat ketentuan lain selain yang diatur dalam pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi elektronik dan/atau dokumen elektronik dianggab sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Keamanan computer mencakup empat aspek yaitu :

1. Privacy
2. Integrity
3. Authentication
4. Availability
5. sedangkan untuk dunia kedokteran maka terdapat aspek lain yang harus juga diperhatikan yaitu access control dan non-repudiation

Privacy

Serangan terhadap aspek privacy misalnya adalah usaha untuk melakukan penyadapan (dengan program *sniffer*). Usaha-usaha yang dapat dilakukan untuk meningkatkan *privacy* dan *confidentiality* adalah dengan menggunakan teknologi kriptografi (dengan enkripsi dan dekripsi).

Integrity

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, *trojan horse*, atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi. Sebuah e-mail dapat saja “ditangkap” (*intercept*) di tengah jalan, diubah isinya (*altered*, *tampered, modified*), kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan *enkripsi* dan *digital signature*, misalnya, dapat mengatasi masalah ini.

Authentication

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul

orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli.
Masalah pertama, membuktikan keaslian dokumen, dapat dilakukan dengan teknologi *watermarking* dan digital signature. Watermarking juga dapat digunakan untuk menjaga "*intelectual property*", yaitu dengan menandai dokumen atau hasil karya dengan "tanda tangan" pembuat.

Masalah kedua biasanya berhubungan dengan access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. Dalam hal ini pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya dengan menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya. Ada tiga hal yang dapat ditanyakan kepada orang untuk menguji siapa dia:
• What you have (misalnya kartu ATM)
• What you know (misalnya PIN atau password)
• What you are (misalnya sidik jari, biometric)

Availability
Aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi. Contoh hambatan adalah serangan yang sering disebut dengan "*denial of service attack*" (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubitubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down*, *hang*, *crash*.
Contoh lain adalah adanya *mailbomb*, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya (apalagi jika akses dilakukan melalui saluran telepon). Bayangkan apabila anda dikirimi 5000 email dan anda harus mengambil (download) email tersebut melalui telepon dari rumah. Serangan terhadap availability dalam bentuk DoS attack merupakan yang terpopuler pada saat naskah ini ditulis

Access Control
Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data (public, private, confidential, top secret) & user (guest, admin, top manager, dsb.), mekanisme authentication dan juga privacy. Access control seringkali dilakukan dengan menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain (seperti kartu, biometrics).

Non-repudiation
Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Sebagai contoh, seseorang yang mengirimkan email untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan email tersebut. Aspek ini sangat penting dalam hal *electronic commerce*. Penggunaan *digital signature*, *certifiates*, dan teknologi kriptografi secara umum dapat menjaga aspek ini. Akan tetapi hal ini masih harus didukung oleh hukum sehingga status dari *digital signature* itu jelas legal. Hal ini akan dibahas lebih rinci pada bagian tersendiri.

Serangan Terhadap Keamanan Sistem Informasi

Security attack, atau serangan terhadap keamanan sistem informasi, dapat dilihat dari sudut peranan komputer atau jaringan komputer yang fungsinya adalah sebagai penyedia informasi. Menurut W. Stallings [40] ada beberapa kemungkinan serangan (*attack*):

• *Interruption*: Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (*availability*) dari sistem. Contoh serangan adalah "denial of service attack".

• *Interception*: Pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (*wiretapping*).

• *Modification*: Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesanpesan yang merugikan pemilik web site.

• *Fabrication*: Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesanpesan palsu seperti e-mail palsu ke dalam jaringan komputer.