Ethical, legal, and Social Issues in Biomedical Informatics

301 MEDICAL INFORMATICS

Dr. Ahmed Albarrak
Associate Professor of Health Informatics
Chairman, Medical Informatics,
College of Medicine
King Saud University
albarrak@ksu.edu.sa

Agenda:

Ethical Issues in Health Informatics:

- General Principles of Informatics Ethics
- Stakeholders in Health Informatics Ethics
- Primary sources of ethical attention in informatics
- Ethics Resources
- Health informatics applications:
    - Appropriate use, users, and contexts
    - Privacy, confidentiality, and data sharing
    - Electronic clinical and research data
- Legal and regulatory matters
- Legal issues in Healthcare Informatics
    - Liability under Tort Law
    - Computer Programs as Potential Expert Witnesses
    - Privacy and Confidentiality
    - Copyrights, Patents, and Intellectual Property:
- Health Insurance Portability and Accountability Act (HIPAA)

Ethical Issues in Health Informatics:

- Confidentiality of electronic patient information
- Proper selection/use of informatics tools in clinical settings
- Determination of who uses these tools
- The role of system evaluation
- The obligations of system developers, maintainers, vendors
- The use of computers to track clinical outcomes to guide future practice.
- Considering ethical issues in health informatics - explore a significant intersection among several professions:

1. Healthcare delivery and administration
2. Applied computing
3. Ethics

Cont.

- What is the Difference between Law and Ethics?
- Legal Issues in Health Informatics: why?
- Liability under Tort Law, apply to clinical use of software systems:
  - Negligence theory
  - Strict product liability
- Privacy and Confidentiality
- HIPPA- “administrative simplification”
- Copyright, Patents, and Intellectual Property.

Introduction ….

- The move to a widely accepted, Electronic Medical Records (EMRs) and e-health applications is accelerating,
- Of course, professionals are motivated by the great benefits to patient care, medicine, and health care in general that can derive from this effort however,
- By putting personal medical records on-line, and/or on different digital mediums is increasing the risk of exposing highly private and sensitive information to outsiders?

Ethics historical ……

- However, there is a strong expectation that such information will be used only in the context of providing health care, and otherwise, will be kept secret.
- This expectation is based on a number of assumptions, beginning with the Medical Oath of more than 2,000 years ago, and reinforced by acts and codes including the Code of Ethics of the American Medical Association and the federal Privacy Act of 1973.
- Eventually, security and privacy of health care information is a people problem. Privacy generally applied to people while confidentiality is best applied to information.

Ethical Issues in Health Informatics:

- Human values should govern research and practice in health professions. Healthcare informatics, like other health professional, encompasses issues of appropriate and inappropriate behavior, of honorable and disreputable actions, and of right and wrong. Students and practitioners of health sciences share an important obligation to explore the moral underpinnings and ethical challenges related to their research and practice.
- Informatics now constitutes a source of some of the most important and interesting ethical debates in all health care professions.

Ethical Issues in Health Informatics:

- Health Informatics Ethics is encompassing ethical issues resulting from the use of technology in managing and utilizing information in healthcare .
- Ethics is a social concept of good behavior. It is a collective concept that evolves gradually, usually over years, as a result of interaction between individuals living or working together.
- Ethics could be considered therefore as a concept with no compelling force other than popular opinion.

Ethics Resources:

1) Codes of ethics

Ethics codes are formal documents that list ethical principles and duties. Such as World Health Organization (WHO) code of ethics and International Medical Informatics Association (IMIA) code of ethics.

2) Case studies

There are often available reference to similar ethical conflicts and situations in the past that may have been resolved in a certain manner. These cases can be applied as jurisprudence.

3) Ethics committees and personnel

Organizations can have committees and trained staff to discuss and resolve ethics issues. These may include ethics boards or ethics professionals that are contacted for consultation when ethical conflicts occur.

4)Informal discussions

Chats with friends or colleagues can lead to informal advice about how an ethical conflict can be resolved.

Stakeholders in Health Informatics Ethics

- It is important to identify the stakeholders involved in the health informatics setting because ethical conflicts arise as a result of interactions between these stakeholders.

1- Patient

2- Healthcare professionals

3- Institutions and employers

4- Society

5- Regulator

6-Others

Note for clarification

It is important to identify the stakeholders involved in the health informatics setting because ethical conflicts arise as a result of interactions between these stakeholders. From the BCS (British Computer Society) /IMIA (American Medical Informatics Association) code, six types of professional relationships are listed that the health informatics professional is involved with:

1- Patient

This refers to anyone who makes use of healthcare services, which generate electronic records for that individual, i.e. electronic medical records (EMRs), patient medical records (PMRs), etc.

2- Healthcare professionals

This includes doctors, nurses, and other medical staff that care for patients. They are different from health informatics professionals, i.e. those who work with health informatics systems.

3- Institutions and employers

Institutions/employers refer to who the health informatics professional is working for. This can be software agencies or healthcare facilities.

4- Society

This is a generalization of everyone else to whom the health informatics professional has duties, excluding patients, healthcare professionals, and employers.

5- Self

The health informatics professional has personal ethical duties, to which they should adhere.

6 -Profession

Health informatics professionals relate with colleagues, and represent the health informatics profession in general.

Electronic Medical Records

- Medical records contain much routine information about patients , such as:
  - height , weight, blood pressures, and notes about issues like flu, cuts, or broken bones.
  - Furthermore, information about issues including fertility and abortions, emotional problems and psychiatric care, sexual behaviors, sexually transmitted diseases, HIV, substance abuse, physical abuse problems, and genetic predispositions to diseases, etc.
- Disclosure or misuse of such information can harm concerned person by causing social embarrassment or prejudice, by affecting insurability, or by limiting ability to get and hold a job.
- Of course, such damage can occur no matter whether medical records are in paper or electronic form.

Cont…

- medical records contain information of the utmost sensitivity, yet this information is only useful when it is shared only with the medical providers and system under which to get health care.
- physicians need and should access complete medical records in order to help diagnose diseases, to avoid duplicative risky or expensive tests, and to design effective treatment plans that take into account many complicating factors.
- The desirable sharing goes beyond personal care and includes relationships to society as a whole through support of medical research, public health management, and law enforcement.

Cont…

There are three concepts involved in protecting health care information:

- **Privacy** :the right and desire of a person to control the disclosure of personal health information.
- **Confidentiality** : the controlled release of personal health information to a care provider or information custodian under an agreement that limits the extent and conditions under which that information may be used or released further.
- **Security**: a collection of policies, procedures, and safeguards that help maintain the integrity and availability of information systems and control access to their contents.

Cont…

- Medical records also serve a variety of functions for organizations not involved directly in care.
- Records are sent to insurers (government and private) to justify payment for medical services rendered, and to detect fraud.
- Used for quality reviews, administrative reviews, and utilization studies to manage the business aspects of health care.
- Used for societal purposes, such as medical research, public health management, social service and welfare system management, law enforcement, screening and licensing and determining life insurance eligibility.
- Education and medical training

Cont…

- A hacker infiltrated the University of Washington Medical Center's computer system and stole at least 5000 cardiology and rehabilitation medicine patients' records
- A Dutch Hacker had pointed out the vulnerabilities of the system, because he had penetrated an unidentified medical centre in New York and another in Holland [19].
- The University of Michigan Medical Center patients' records were left exposed to the public on the Internet because they thought that they were on a special server protected with special password [20]. It was an innocent mistake but the patient's confidentiality was breached.
- The case of the Florida state public health worker who sent the names of 4000 HIV positive patients to two Florida newspapers was a case of abuse of access privilege and access for the purpose of profit.

The standard view of appropriate use:

- The standard view state that, when adequate decision-support tools are developed, they should be used as supplementary and subservient to human clinical judgment. e.g. clinical expert systems
- Corollaries of the standard view:

1-Practitioners have an obligation to use any computer-based tool responsibly, through adequate user training and by understanding of the system abilities and limitations.

2- Practitioners must not abrogate their clinical judgment reflexively when using computer based decision aids.

The standard view of appropriate use:

- Users of most clinical systems should be health professionals who are qualified to address the question at hand on the basis of their licensure, clinical training and experience . Software systems should be used to augment or supplement , BUT to replace such individual's decision making.
- All uses of informatics tools, especially in patient care , should be preceded by adequate training and instruction, which should include review of all available forms or previous product evaluations.

Obligations and Standards for systems Developers and Maintainers

- Users depend on the developers and maintainers of a system and must trust evaluators who have validated a system for clinical use.

- Health care software applications are the most complex tools in the technological armamentarium, which commits system developers , designers and maintainers to adhere to standards and acknowledge their moral responsibility.

Obligations and Standards for systems Developers and Maintainers

- People who develop, maintain and sell healthcare computing systems and components have obligations which include holding patient care as the leading value.
- Professional-patient relationship principal- also applies to the people who produce and attend to healthcare information systems.
- Quality standards should stimulate scientific progress and innovation while safe guarding against systems error and abuse.

Obligations and Standards for systems Developers and Maintainers

- “best practices” in health informatics must include a way to measure whether a systems performs as intended.

- this provides the ground for quality control, and is the obligations for system developers, users, maintainers and administrators.
- Sample evaluation criteria:
  - Does the system work as designed?
  - Is it used as anticipated?
  - Does it produce the desired results?
  - Does it work better than the procedures it replaced?
  - Is it cost effective?

Continue sample evaluation criteria:

- How well have individuals been trained to use it?
- What are the anticipated long term effects on how departments interact?
- What are the long-tern effects on the delivery of medical care?
- Will the system have an impact on the control in the organization?
- To what extent do effects depend on practice setting?

Appropriate users and educational standards:

Who should use a healthcare related computer application?

- An early paper on ethical issues in informatics noted that user of such system include physicians, nurses, student to health sciences, patients, and insurance and government evaluators
- Are members of all these group appropriate users?

Ethical principles for appropriate use of decision support system:

1-A computer program should be used in clinical practice only after appropriate evaluation of its efficacy and documentation that it performs its intended task at an acceptable cost in time and money.

2-Users of most clinical systems should be health professionals who are qualified to address the question at hand on the basis of their licensure, clinical training, and experience. In addition, software system should be used to augment or supplement, NOT to replace individuals decision making.

3-All uses of informatics tools, especially in patient care, should be preceded by adequate training and instructions.

Privacy, confidentiality, and data sharing

Some of greatest challenges in healthcare is placing information in the computer applications while upholding traditional principles. One challenge involves balancing two competing values:

- Free access to information
- Protection of patients' privacy and confidentiality.

Protection of privacy and confidentiality is not an option, a favor or a helping hand offered to patients ; it is a duty that does not vary with the malady or the data storage medium.

Technologies Helps Protect Health Care Information

- In paper-based patient records, access control is almost entirely manual and procedural
- Technological security tools are an integral part of EMR systems and offer varieties of advantages
- Confidentiality and privacy
- Information and data security
- The appropriate use of informatics tools in clinical sitting.
- The determination of who should use such tools.
- The role of system evaluation.
- The obligations of system developers, maintainers, and vendors.
- Use of computer to track clinical outcomes to guide future practice.

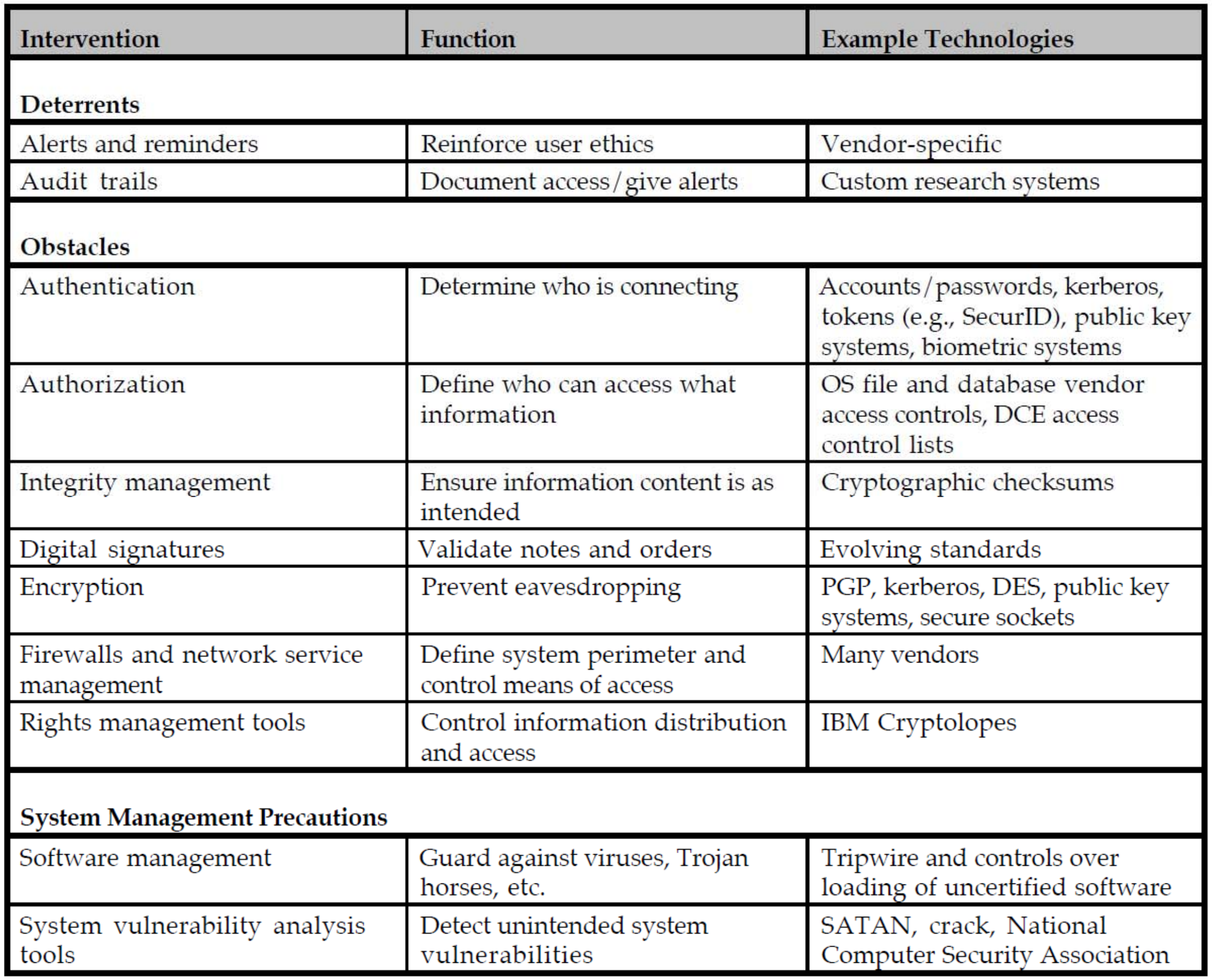
Importance of computer application in healthcare:

At the highest level with respect to ethics and security, it serves five key functions:

- *Availability : ensuring that accurate and up-to-date information is available* when needed at appropriate places.
- *Accountability : ensure that health care providers are responsible for* their access , and uses of information are based on a documented need and right to know
- *Perimeter Definition : knowing and controlling the boundaries of trusted* access to the information system, both physically and logically.
- *Role-Limited Access : enabling access for personnel only to information* essential to the performance of their jobs, and limiting the real or perceived temptation to access information beyond a bona fide need.
- *Comprehensibility and Control : ensuring that record owners, data stewards,* and patients can understand and have effective control over appropriate aspects of information privacy and access.

- there are three general classes of technological interventions to improve system security
- Deterrents depend upon the ethical behavior of people and provide reminders and oversight to reinforce those standards.
- Obstacles directly control the ability of a user to get at information, with the goal of constraining access only to information for which they have a need or right to know.
- System management precautions involve proactively surveying an information system to ensure that known sources of vulnerability are eliminated.
- It has been shown that deterrents , alerts, reminders, and education of users are very effective in reinforcing already highly ethical behavior of the great majority of health care providers
- systems, will record the identities and circumstances of all users accessing information, and that these records are reviewed regularly, ethical users will think twice about abusing their privileges.

Technologies Applicable to Information System Security Management



Intervention	Function	Example Technologies
Deterrents		
Alerts and reminders	Reinforce user ethics	Vendor-specific
Audit trails	Document access/give alerts	Custom research systems
Obstacles		
Authentication	Determine who is connecting	Accounts/passwords, kerberos, tokens (e.g., SecurID), public key systems, biometric systems
Authorization	Define who can access what information	OS file and database vendor access controls, DCE access control lists
Integrity management	Ensure information content is as intended	Cryptographic checksums
Digital signatures	Validate notes and orders	Evolving standards
Encryption	Prevent eavesdropping	PGP, kerberos, DES, public key systems, secure sockets
Firewalls and network service management	Define system perimeter and control means of access	Many vendors
Rights management tools	Control information distribution and access	IBM Cryptolopes
System Management Precautions		
Software management	Guard against viruses, Trojan horses, etc.	Tripwire and controls over loading of uncertified software
System vulnerability analysis tools	Detect unintended system vulnerabilities	SATAN, crack, National Computer Security Association

The consensus among health care CIOs is that the most important threats to patient information confidentiality are the following, in decreasing frequency of occurrence:

- From inside the patient care institution:

  Accidental Disclosures : medical personnel make innocent mistakes and cause unintentional disclosures. A conversation may be overheard between care providers in the corridor or elevator.

  A lab technician may notice test results for an acquaintance. Information may be left on a computer screen where it can be seen by a passerby, or email or FAX messages may be misaddressed. Insider Curiosity : medical personnel abuse their record access privileges out of curiosity or for their own purposes. Some do so out of concern for the well being of fellow employees or family members. Some want to know about celebrities being treated. Some may be concerned about the possibility of sexually transmitted diseases in a colleague they are dating.

  Insider Subornation : medical personnel knowingly access information and release it to outsiders for spite, revenge, or profit. Embarrassing health information about prominent people finds its way into grocery-store tabloids or the public press with relative ease. It is said that Nicole Brown Simpson's (paper) medical records were available to the press within a week of her murder in 1994.

Conti…

The London Sunday Times reported in November 1995 that the contents of anyone's (electronic) medical record in Great Britain could be purchased on the street for £200.

- From within secondary user settings

Uncontrolled secondary usage : those who have access rights to patient information for a purpose in support of primary care may exploit that access for other purposes not envisioned in patient consent forms , broadly (data Mining) in modern parlance .

- From Outsider intrusion into medical information systems: Unauthorized access , vindictive former employees, angry patients, network intruders, or others may steal information, damage systems, or disrupt operations.

A recent NRC study of security practices in health care institutions found no examples of (detected) outside intruder break-ins. Nevertheless, reports abound of intrusions in business, academic, and government sites on the Internet. It must be considered an artifact of the fact that the US health care industry is still almost totally reliant on paper records

- Insider abuse Accidental disclosures ----Education, alerts, reminders
- Insider curiosity --- Education, authentication, authorization, audit trail, rights
- management tools (future possibility)
- Insider subornation --- Same as above
- Secondary users --- Rights management tools (future possibility)
- Outsider intrusion --- All available obstacles and system management precautions

Importance of privacy and confidentiality:

1- Privacy and confidentiality are widely regards as rights to all people, and such protection help to accord them respect.

2-Protecting privacy and confidentiality benefits for both individuals and society. patients who know that their healthcare data will not be shared inappropriately are more comfortable disclosing those data with clinicians. This trust is important in patient-physician relationship.

3- Privacy and confidentiality protection is important for public health. People who fear disclosure of personal information are less likely to seek out professional assistance which will increase the risks that contagion will be speared.

- The obligations to protect privacy and to keep confidences fall to system designers and maintainers, to administrators, to physicians, nurses, and other people who elicit the information in first place.
- The upshot for all of them is this: protection of privacy and confidentiality is not an option; it is a duty that does not vary with the malady or the data storage medium.

Electronic clinical and research data:

- Access to electronic patients records hold promise for clinicians and for other people who need timely, accurate patient data. On other hand, systems that make it easy for clinicians to access data also make it easy for other people to access it.
- The proper approach to such challenges is one will ensure both that
  1-Appropriate clinicians and other people have rapid, easy access to patient records.
  2-Other people do not have access.

Way to restrict inappropriate access to electronic records:

- They are generally divided into technological methods and policy approaches.

1- Technological methods: computers can provide the means for maximizing their own security by making sure that users are who they say they are, prohibiting people without professional need from access health information, and using audit trials or logos of people who do inspect confidential records so that patients and other people can review the logs.

2- Policy approaches: the National Research Council has recommended that hospitals and other healthcare organizations create security and confidentially committees and establish education and training programs

Electronic data and human subject research:

- The use of patient information for clinical research and quality assessment raises interesting ethical challenges .
- The benefits of public health loom large in considering record-based research .
- The benefit of electronic health record is ability to access vast numbers of patient records to determine the incidence and prevalence of diseases, to track the efficacy of clinical interventions, and to plan efficient resource allocation.

Method to safeguard electronic data:

1- Establish mechanisms to anonymize the information in individual records or to decouple the data contained in the records from any unique patients identifiers.

- This task is not always straightforward: a specific job description, or rare disease diagnosis coupled with demographic data may act as a surrogate unique identifier. Such challenges point to a second means.

2- Use of institutional panel such as medical record committees or institutional review boards. Submission of research to appropriate institutional scrutiny is one way to best use of more or less anonymous electronic patient records.

Legal and regulatory matters:

- **Difference between law and ethics:**

As might be anticipated, ethical and legal issues often overlap.

- **Ethical considerations** apply in attempts to determine what is good or meritorious and which behaviors are desirable or correct in accordance with higher principles.
- **Legal principles** are generally derived from ethical ones but deal with the practical regulation of morality or behaviors and activities .
- **laws** directly tell us how to behave under various specific circumstances and prescribe remedies or punishments for individuals who do not comply with the law.

Legal issues in Healthcare Informatics

- Major legal issues related to the use of software applications in clinical practice and in biomedical research include:
- Liability under tort law
- Potential use of computer applications as expert witnesses in the court room.
- Legislation governing privacy and confidentiality.
- Copyrights, patents, and intellectual property issues.

Liability under Tort Law

- A key legal distinction is difference between products and services .
- **Products** are physical objects, such as stethoscopes, that go through the process of design, manufacture, distribution ,sale and subsequent use by purchasers.
- **Services** are intangible activities provided to consumers at a price by qualified individuals.

Liability under Tort Law(cont.)

- Clinical software applications can be viewed as either

➢ **Goods** :software programs designed, tested debugged, placed on diskettes or other media, and distributed physically to purchasers.

or

➢ **Services** :applications that provide advice to practitioners engaged in a service such as delivering health care.

Liability under Tort Law(cont.)

- Two ideas from tort law potentially apply to the clinical use of software systems:

1. **Negligence theory.**
2. **Strict product liability.**

Negligence theory

- Providers of goods and services are expected to uphold the standards of the community in producing goods and delivering services.
- When individuals suffer harm due to substandard goods or services, they may sue the service providers to recover damages. Malpractice litigation in healthcare is based on negligence theory.
- Patients who are harmed by clinical practices based on imperfect software applications may sue the health care providers for negligence or malpractice.

.

Strict product liability

- In contrast to negligence, strict product liability applies only to harm cussed by defective products and not applicable to services.
- The primary purpose of strict product liability is to compensate the injured parties rather than to punish negligent individuals.

Strict product liability(cont.)

- For strict product liability to apply, three conditions must be met:

1-The product must be purchased and used by individual.

2-The purchaser must suffer physical harm as a result of a design or manufacturing defect in the product.

3-The product must be shown in court to be unreasonably dangerous in manner that is the demonstrable cause of the purchaser's injury.

Computer Programs as Potential Expert Witnesses

- Reasons which prevent using of clinical decision support system as expert witnesses:

1-The witnesses must be able to be sworn to tell the truth. Expert system cannot be made to do so in any meaningful manner.

2-Courts do not admit hearsay evidence (external information that cannot be subjected to interactive questioning by opposing lawyers and by judges in the courtroom.)

- In the United States, Federal Register, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and National Committee on Vital and Health Statistics have strongly emphasized the importance of health privacy [21,22].
- The National Research Council has discussed in detail the limitations of Federal and State protection, technical approaches and organizational approaches for protection of privacy in medical records [23].
- In Australia, Parliament passed the Health Record and Information Privacy Act (HRIPA) in 2002

Privacy and Confidentiality:

- In the united states, a key federal initiative, the Health Insurance Portability and Accountability Act (HIPAA) of 1966, called for the legislative or executive branch of government to establish the first-ever nationwide protection of electronic patient records .

Copyrights, Patents, and Intellectual Property:

- Another underdeveloped area of law, with respect to clinical information systems, is **Intellectual Property** protection afforded to developers of software programs, biomedical knowledge base, and World Wide Web pages. **Copyright law** protects intellectual property from being copied verbatim, and Patents protect specific methods of implementing or instantiating ideas.

Health Insurance Portability and Accountability Act (HIPAA):

- In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was endorsed by the U.S. Congress.
- HIPAA is composed of several sets of standards like transactions and code sets, privacy and security.
- The main purpose of the standards are to modify the administration of health insurance claims and lower costs, to give patients more easily access to their health care information.

HIPAA (cont.)

- HIPAA calls for:
  - Standardization of electronic patient health, administrative and financial data.
  - Unique health identifiers for individuals, employers, health plans and health care providers.
  - Security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present or future.

HIPAA (cont.)

- HIPAA's administrative simplification provision is composed of four parts, each of which have generated a variety of rules and standards.
- **The four parts of administrative simplification are:**
  - Electronic health transaction standards.
  - Unique identifiers.
  - Security and electronic signature standards.
  - Privacy and confidentiality standards.

HIPAA (cont.)

- The HIPAA Privacy Rule, also called the Standards for Privacy of Individually Identifiable Health Information, provided the first nationally-recognizable regulations for the use/disclosure of an individual health information. Essentially, the Privacy Rule defines how covered entities use individually-identifiable health information or the PHI (Personal Health Information). Covered entities is a term often used in HIPAA-compliant guidelines.
- A covered entity can be a:
  - Health plan.
  - Healthcare clearinghouse.
  - Healthcare provider.

HIPAA (cont.)

Overview of the Privacy Rule :

- Gives patients control over the use of their health information.
- Defines boundaries for the use/disclosure of health records by covered entities.
- Establishes national-level standards that healthcare providers must comply with.
- Helps to limit the use of PHI and minimizes chances of its inappropriate disclosure.
- Strictly investigates compliance-related issues and holds violators accountable with civil or criminal penalties for violating the privacy of an individual PHI.
- Supports the cause of disclosing PHI without individual consent for individual healthcare needs, public benefit and national interests.

selected References:

- Shortliffe, Perreualt, wiederhold, Fagan & Fagan (eds).Medical Informatics: Computer applications in healthcare and biomedicine.2nd edition. Springer. 2003.

- The IMIA Code of Ethics for Health Information Professionals.

- Samuel H, Zaïane O, Sobsey D. Towards a Definition of Health Informatics Ethics. 1st ACM International Health Informatics Symposium, IHI '10, November 11–12, 2010, Arlington, Virginia, USA.

- Val Verde Regional Medical Center. Health Insurance Portability and Accountability Act (HIPAA). [Online].2010[cited 2010 Nov 28];Available from: URL:http://www.vvrmc.org/hipaa.html

- Health Insurance Portability And Accountability Act. Hippa – Health Insurance Portability And Accountability Act. [Online].2010 July 27[cited 2010 Nov 28];Available from: URL: http://www.hipaagives.org/articles/hippa-health-insurance-portability-and-accountability-act/

- What is HIPPA?. [Online].2009 [cited 2010 Nov 28];Available from: URL: http://whatishipaa.org/