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

Agenda:

Ethical Issues in Health Informatics:

- Stakeholders in Health Informatics Ethics
- Primary sources of ethical attention in informatics
- 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
  - Privacy and Confidentiality
- 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

Introduction ….

- The move to 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, 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 healthcare information.
- 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.

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

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 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…

- A hacker infiltrated the University of Washington Medical Center's computer system and stole at least 5000 cardiology and rehabilitation medicine patients' records
- In another incidence, 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.

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 practise setting?

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.

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

- 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