มหาวิทยาลัยราชภัฏนครปฐม
Nakhon Pathom Rajabhat University

Topic 9

Ethical Issues in the use of Nursing Informatics

Natthaya Cherngchalard Chooprom (RN, MNS)
Faculty of Nursing, NPRU

Learning objectives

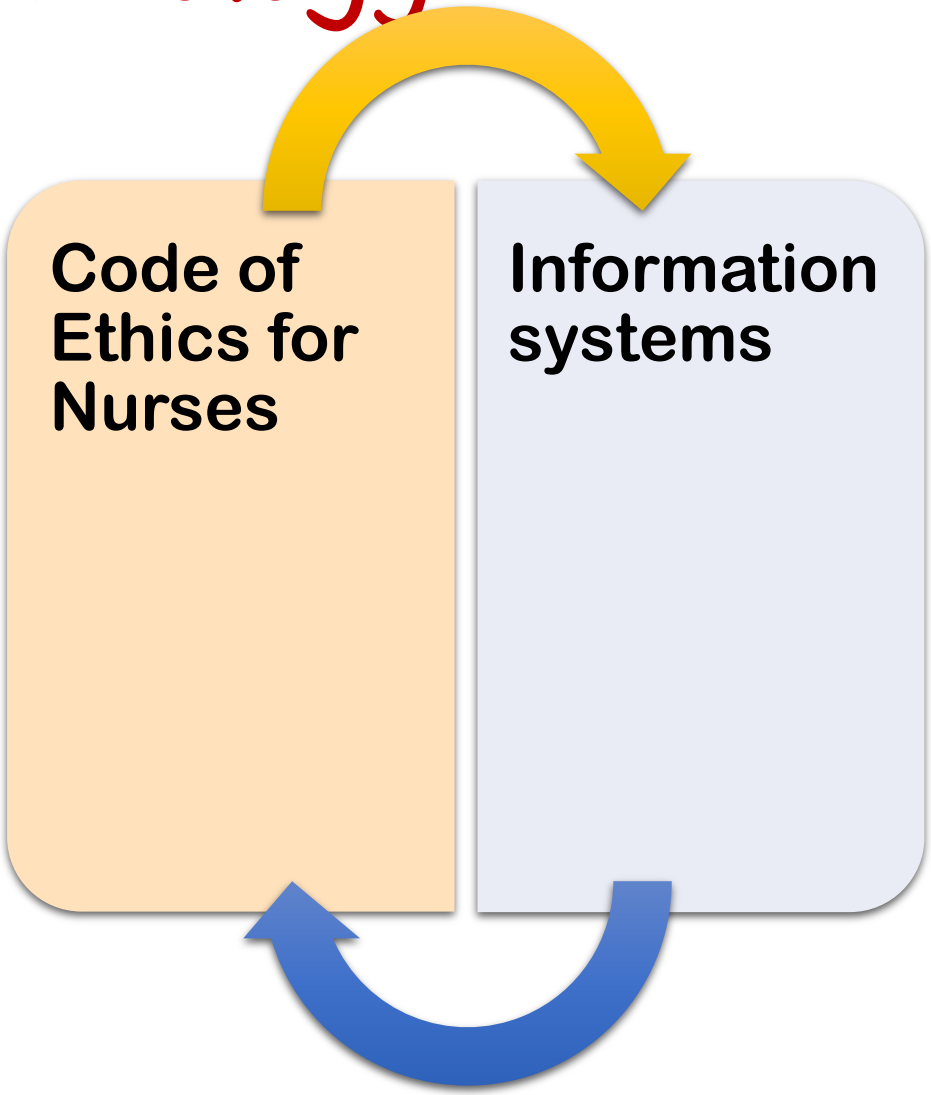
1. Explore about informatics ethics
2. Differentiate between privacy, confidentiality, information privacy, and information security.

Learning Topics

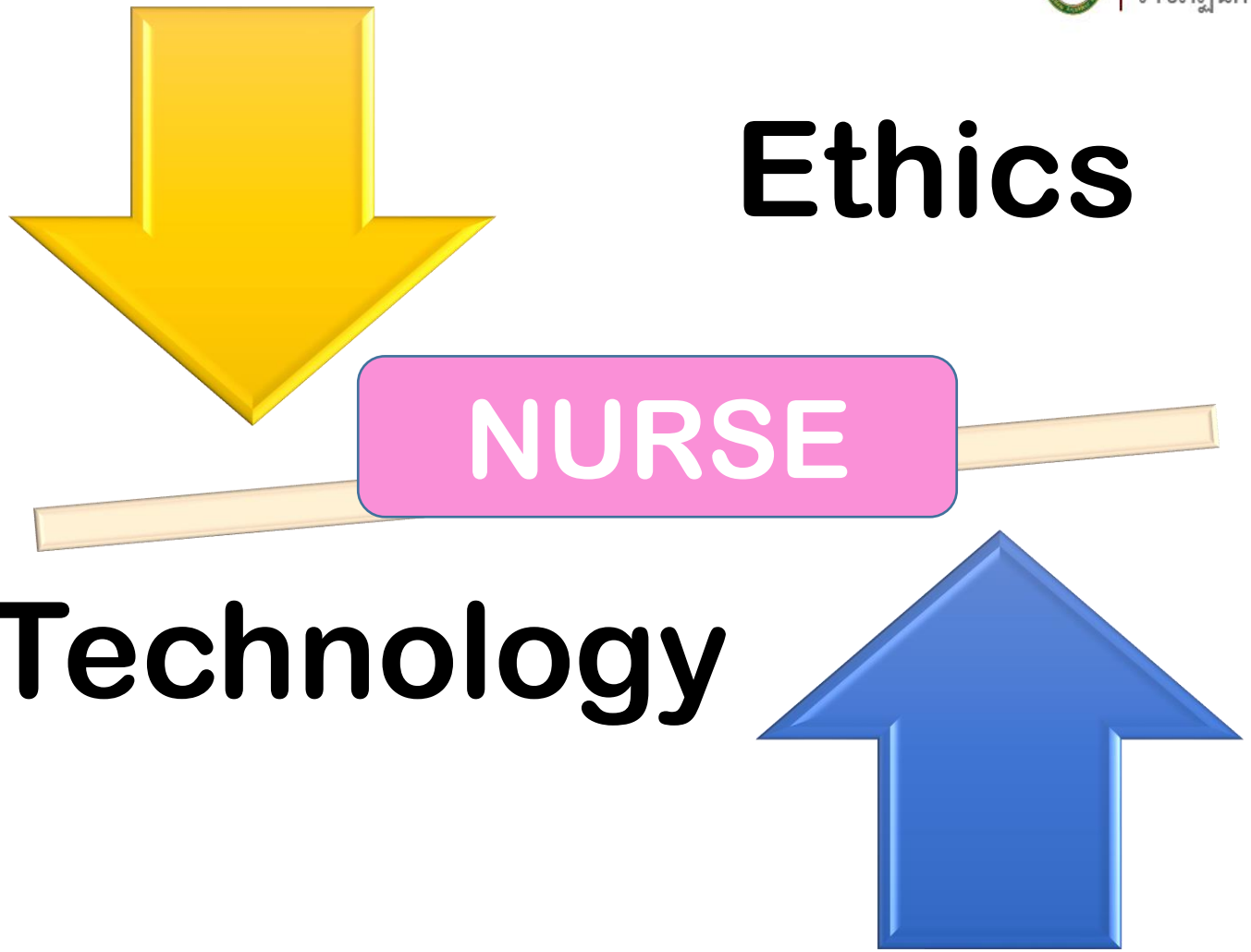
- Informatics Ethics
- Key concepts: privacy, confidentiality, information privacy, and information security.
- The effect of information system security on: privacy, confidentiality, and security.
- Potential threats to system security and information.

Nursing Ethical Dilemma with Using Informatics Technology

- culture
- religion
- education
- individual values and opinions

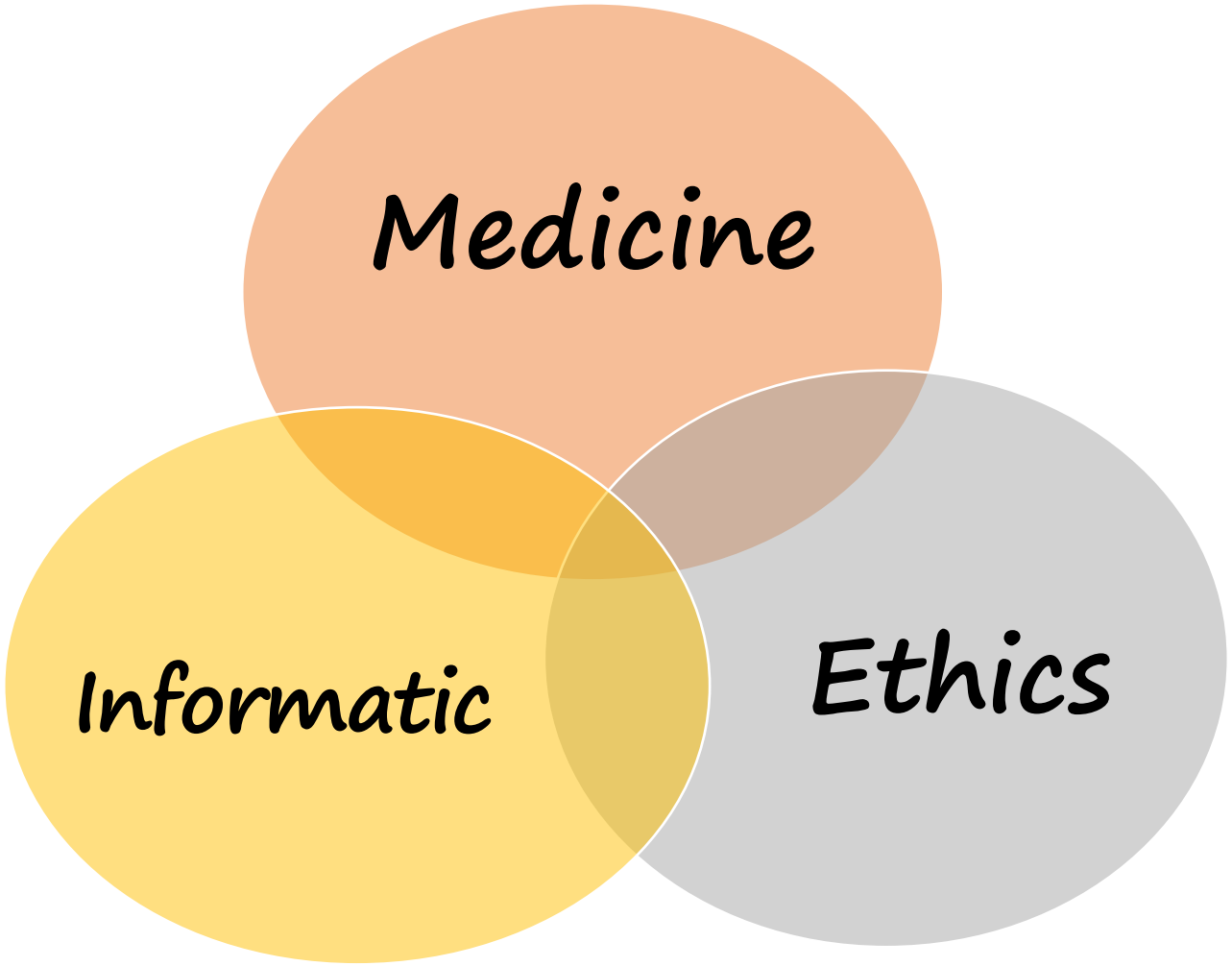


- New computer technologies
- The speed and efficiency of electronic information systems



Information ethics

(1)Respect for information
(2)Respect for privacy
(3)Equitable representation
(4)Non-maleficence



- increased access to health information
- Information technology is a prominent tool in healthcare management.
- often unable to report concerns about privacy, confidentiality and integrity of information.

Fundamental Ethical Principles

- Beneficence and Nonmaleficence
- Fidelity and Responsibility
- Integrity
- Justice
- Respect for People's Rights and Dignity
- Autonomy
- Paternalism

Beneficence and Nonmaleficence

Seek benefit from those who work with them and are careful not to harm.

Fidelity and Responsibility

- Develop trusting relationships
- Aware of their professional and scientific responsibilities

Integrity

- Seek to promote accuracy, honesty and honesty in science
- Teaching and practicing well

Justice

- Recognition of justice and justice qualify all people to access and benefit from the contributions
- Equal quality in the processes, procedures and services

Respect for People's Rights and Dignity

- Respect the dignity and worth of all people
- The rights of individuals to privacy, confidentiality and self-determination

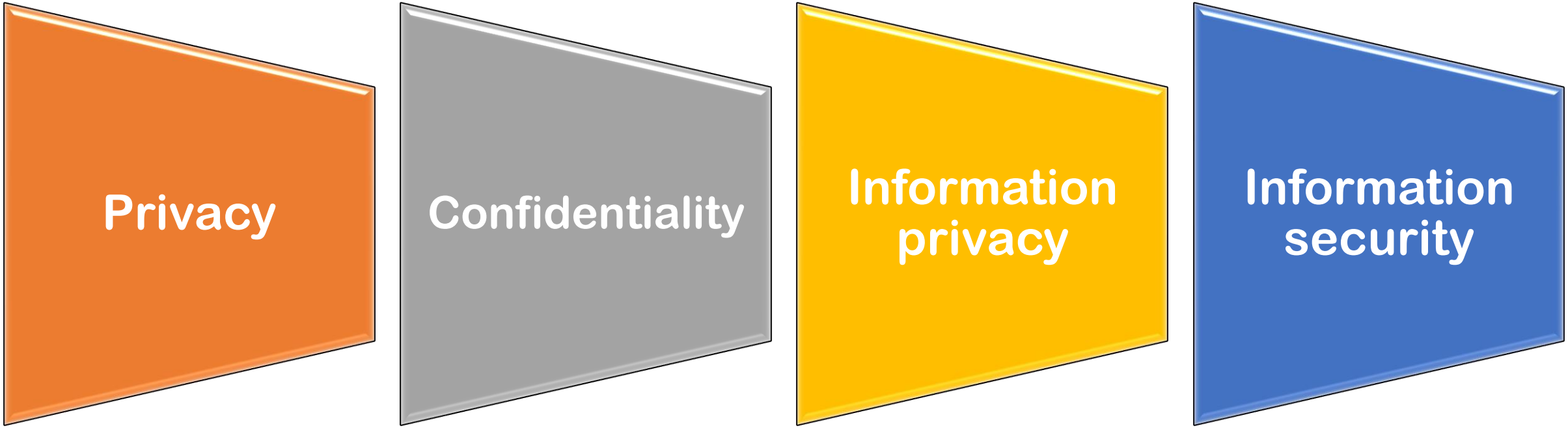
Autonomy

- Agree to respect the right of the other to self-determination
- Support independent decision-making

Paternalism

- Health care professionals make decisions about treating, and diagnosing the patient.
- This principle is heavily loaded as an application of authority to the patient

The Code of Ethics for Health Information Professionals


Privacy
Confidentiality
Information privacy
Information security

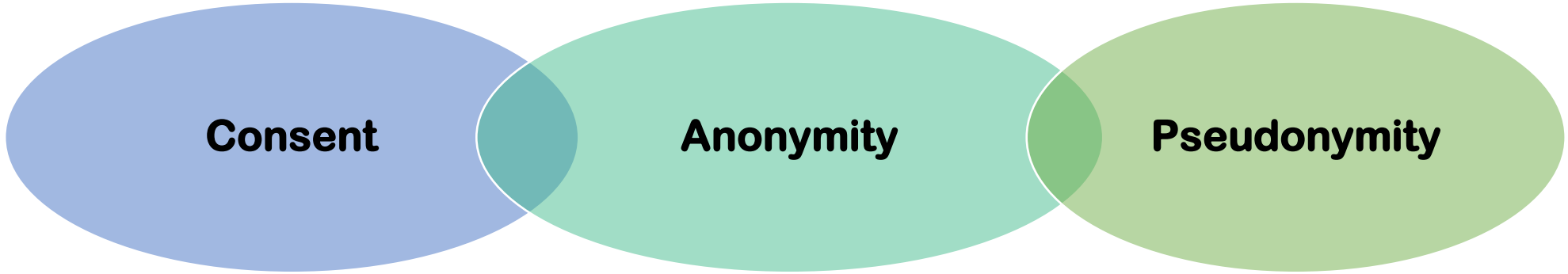
What is Confidentiality?

"The nondisclosure of information except to another authorized person"

- The ethical principle or legal right that a physician or other health professional will hold secret all information relating to a patient, unless the patient gives consent permitting disclosure"(American Heritage Medical Dictionary, 2007).

Confidentiality Breach

- A breach of confidentiality is a disclosure of private information to a third party not involved with the patient's care, without patient consent or court order. Disclosure can be oral or written, by telephone or fax, or electronically, for example, via e-mail or health information networks.
- Accessing the medical records of patient's without legitimate reason is also considered a breach of confidentiality.



Potential threats to system security and information

Steps to Security

- Assessment of risks and assets
- An organizational plan
- A “culture” of security
- The establishment and enforcement of policies

Threats to System Security and Information

- Viruses, worms
- Flooding sites
- Power fluctuations
- Revenge attacks

- Pirated Web sites
- Poor password management
- Compromised device
- Fires and natural disasters
- Human error
- Unauthorized insider access

- Thieves
- Hackers and crackers
- Denial of service attacks
- Terrorists

Information Security

Protection of information against threats to its integrity, inadvertent disclosure, or availability determines the survivability of a system

Security Measures

- Firewalls
  - barrier created from software and hardware
- Antivirus and spyware detection
- User sign-on and passwords or other means of identity management
- Access on a need-to-know basis- level of access
- Automatic sign-off
- Physical restrictions to system access

Password

- Collection of alphanumeric characters that the user types into the computer
- May be required after the entry of an access code or user name
- Assigned after successful system training
- Inexpensive but not the most effective means of verification

Do:

- Choose passwords that are 8-12 characters long.
- Avoid obvious passwords.
- Keep your password private- ie, do not share.
- Change password frequently.

- Do not:
  - Post or write down passwords.
  - Leave computers or applications running when not in use.
  - Re-use the same password for different systems.
  - Use the “browser save” feature.

Biometrics

- Identification based on a unique biological trait, such as:
  - a fingerprint
  - voice or iris pattern
  - retinal scan
  - hand geometry
  - face recognition
  - ear pattern
  - smell
  - blood vessels in the palm
  - gait recognition

Antivirus Software

- Computer programs that can locate and eradicate viruses and other malicious programs from scanned memory sticks, storage devices, individual computers, and networks

Spyware Detection Software

- **Spyware**
  - a type of software that installs itself without the user's permission, collects passwords, PIN numbers, and account numbers and sends them to another party
- **Spyware Detection Software**
  - Detects and eliminates spyware

The Impact of the Internet

Introduces new threats

- E-mail and instant messages may carry personal health information that can be intercepted
- Unapproved use of messages or Web sites can introduce malicious programs
- Web sites used for personal health information may be inappropriately accessed
- Verify wireless networks before use.
- Responsibility for information and information system security is shared

Implications for Mobile Computing

- Devices are easily stolen.
- Devices should require authentication and encryption to safeguard information security.
- Devices should never be left where information may be seen by unauthorized viewers.


Challenging compliance
Accountability for information
Identifying purposes
Individual access
Consent
The ten security principles
Openness
Limiting collection
Safeguards
Accuracy
Limiting use

1. Accountability for information :

- Organizations that collect, use or disclose PHI are responsible for the personal health information in their custody or care.
- A named individual within the organization should be responsible for facilitating organizational compliance with applicable data protection legislation and organizational privacy policies.

2. Identifying purposes for collection , use and disclosure of information :

To allow patients to make appropriate decisions about their PHI, it is important that they be made aware of the purposes for which this information is being collected, used, and disclosed.

There are many legitimate purposes for collecting personal health information; indeed, an international standard classification of such purposes has been developed

These purposes include:

- providing clinical care to an individual
- providing emergency care to an individual
- supporting care activities for the individual within the healthcare organization.
- enabling medical billing (and/or permissions from a funding party for providing health care services to the patient)
- health service management and quality assurance
- education for health care professionals
- public health surveillance and disease control

3. Consent :

An organization should be able to demonstrate that it is in compliance with applicable laws and that the patient can reasonably be expected to know that information about them was going to be collected and used for defined purposes.

4. Limiting collection :

- Organizations should limit collection of personal health information to that which is necessary for the identified purposes; i.e. personal health information should not be collected indiscriminately
- Historically, many fields of data (e.g., religion and race) were collected in patient records, even in cases where they had little or no bearing on treatment and care.

5. Limiting use , disclosure and retention :

Once organizations identify the purposes for which they collect personal and seek consent

6. Accuracy :

The need for accuracy as a fair information practice is particularly relevant in the delivery of healthcare.

7. Safeguards :

By implementing information security safeguards, organizations protect personal health information against loss and theft, as well as unauthorized access, disclosure, copying, use, and modification.

8. Openness :

It should be possible for concerned patients to know the purposes for which information about them is collected, used, and disclosed.

9. Individual access :

Patients should have the right to access their own personal health information so that they can assure its accuracy, and amend inaccurate or incomplete information

10. Challenging compliance :
The right of a patient to lodge a privacy complaint against an organization

Write your opinion as 150 words report to answer…

Reprinted with permission from Harley L. Schwardron.

How can ethics be of use to health or nursing informatics?

Thank You