IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB8518

Chapter III

Information Security Framework for Health Information Systems

Lech J. Janczewski
The University of Auckland, New Zealand

This chapter outlines the major issues related to the security of medical information systems. Medical information systems are unique in this sense that integrity of the records and privacy issues are dominant. The presentation includes the formulation of the basic medical information security tenets as well as the discussion of the major components of the security subsystem: patient identification, access mechanism, reference monitor, communication subsystem and database subsystem. Also examples of privacy law are quoted and discussed.

Security is about the protection of assets. Information security deals with the protection of information within a given domain. In this context it is usually expanded into three different directions:

- **Confidentiality**
  Assurance that particular information is accessible (read, write, or execute) by authorised personnel only.
- **Integrity**
  Assurance that during processing no unauthorised changes of information are possible.
- **Availability**
  Assurance that information can be used at will.

The security of information within a medical information system is extremely important for a number of reasons:

- **Welfare of patients**
  An innocent typing error: entering "+" instead of "-" (resulting in wrong information about an individual's blood group) could have deadly consequences! To say nothing of the social consequences, the financial cost of such errors could be devastating. Multimillion dollar court verdicts are not uncommon. The speed of accessing vital patient records is also important. In the emergency ward the surgery team could not afford a long wait for information about a patient's allergies.
- **Law enforced protection of patients' privacy**
  In the majority of business world's disclosures of organisation secrets could have serious financial consequences, like lost transactions or clients. In the medical domain the situation is far more serious. Most countries have introduced law aimed at the protection of patients' privacy. Violations could lead to criminal court cases, usually being costly and lengthy.
- **Medical research requirements**
  The law should protect the publication of case details, as was mentioned before, but medical information should be also available for researchers in the medical arena. Also, a significant number of medical personnel need to have access to patients files. Hence the characteristic dilemma of medical information: simultaneous needs for protection of data against disclosures with needs for its wide distribution.

The requirements of security of medical information systems could be contrasted with the security of military and banking systems as follows:

- In the military system confidentiality is usually the most important aspect of the security mechanisms (under no circumstances should our enemy know our plans).
- In the banking system, integrity of the data is usually most important (balance of the account reflects the reality of the performed transactions). Recent trends in banking indicate that availability is also becoming quite important. Twenty years ago cashing a cheque in a bank required many hours of waiting for