Chapter II
Security Health Information Systems

Christina Ilioudi
University of Piraeus, Greece

Athina Lazakidou
University of Piraeus, Greece

ABSTRACT

Please provide an abstract.

INTRODUCTION

Before the computer age, healthcare information was typically stored in the physician's office. All information specific to a patient was generally kept in a medical record and filed in the office filing cabinet. The introduction of technology changed how physicians and other health organizations keep personal health information. Nowadays medical data are being kept in a computer, so we talk about an electronic patient record (EPR) and not about a printed medical record. Thus, health information systems rely upon a computerised infrastructure. The development of Internet technology and Web-based applications made health information more accessible than ever before from many locations by multiple health providers and

health plans. In the near future, the Internet will probably be the platform of choice for processing health transactions and communicating information and data. But along with this accessibility come increased threats to the security of health information, and those who would steal, divert, alter, or misuse your information are becoming even more skilled at finding what they want and covering their tracks.

In healthcare, it is very important to develop secure systems because we want to ensure that the medical data that contain the personal information of patients will not be violated by anyone. Thus, what is under question is the availability of the right data to the right user at the right time (availability). Information technology deeply affects the confidential relationship between patient and doctor since it increasingly surrounds and mediates it. Hence, the protection of personal medical data (confidentiality) is a necessity without which medical treatment will hardly be successful. This will sometimes include the anonymity of a patient. In addition to the protection of data from unauthorized reading, data also have to be protected against unauthorized modification (integrity). Also, healthcare professionals are personally responsible and mostly liable for their decisions in favour of a particular action or against it. This raises the need for health information systems that are capable of providing an individual with undoubted proof that he or she took a certain action or did not (accountability). Below we will explain how exactly the information flow takes place in medical systems, which security model we used in the past, what the threats are, which mechanisms are usually being used to prevent the violence of those systems, and finally we will present some examples of security deficiency and what impacts have been recorded.

INFORMATION-FLOW CONTROL

In security engineering, there are two approaches to information-flow control. The first approach (Figure 1) is multilevel security (top-down approach), in which lower level information may move up in the hierarchy, but higher level information may not move down. The main representative of this approach is the Bell-LaPadula policy. The second approach (Figure 2) is multilateral security, in which information is prevented from flowing across departments. One representative of this approach is the BMA model developed by the British Medical Association to describe the information flows permitted by medical ethics. This kind of security applys very well in healthcare systems as it covers the use of techniques such as anonymity. However, we will not make further analysis of it here because this is not our goal.

THREATS TO HEALTH INFORMATION SYSTEMS

One question of vital importance for health information systems could be “What are the threats that could have a major impact on health information?” If we try to answer the question, we would count some of the potential threats. A threat can be an agent who either accidentally or intentionally gains unauthorized access to the protected IT systems. Threats may be physical or logical. Physical threats include the following.

- employees (common threat)
- ex-employees
- hackers
- terrorists
- criminals
- customers