Data security in medical information systems using a generic model

P. Sanders and S. Furnell

University of Plymouth, Plymouth, U.K.

Abstract

The content of this paper is based upon work currently being carried out as part of the Commission of European Communities SEISMED (Secure Environment for Information Systems in MEDicine) project, the aim of which is to provide recommendations on security for existing systems in European Health Care Establishments (HCEs).

1. Introduction

The need for adequate data security in the medical environment is obvious, given that the maintenance of patient confidentiality and safety are of paramount importance to retaining a relationship of trust between patients and the HCE. In addition, the transition to the purchaser-provider system of funding now present in parts of the European Community means that more traditional business-type data also require protection.

A number of methods of protection may be suitable for adoption in the medical field, ranging from technical measures (achieved either via software or hardware) on the systems themselves to procedures implemented across the HCE [1]. In broad terms the methods fall into 3 main categories, as below:

- **External control mechanisms**
  Safeguards against fire, flood, theft, equipment or power failure and such like. Emphasis of security through staff awareness programmes.
- **User interface control mechanisms**
  Provision of authentication / access control features (e.g. the use of passwords, tokens, and related issues).
- **Internal control mechanisms**
  Including such concepts as data encryption, virus prevention, system auditing.

These general ideas have been explored in detail in previous publications in a piecemeal approach. What is now required is a set of guidelines on where, what and how to put security into HCE systems in general. It would then be possible for individual system administrators to select solutions appropriate for their own particular arrangements.

The provision of security for medical data on a large scale is a complex issue, given that a myriad of different computer systems (in terms of hardware, networking and actual applications) may be identified within a single country, let alone in the full European scenario. The issue is further complicated by the variety of information that may be held, and the fact that several different levels of sensitivity may exist. As the desired protection will depend upon the risks associated with the information, it is impossible to assert a single level of security that will be appropriate for all data.

In order to address these problems there is a requirement for a flexible system which is able to integrate security into the multiple networks and databases in an open systems type environment. In addition, a method is needed to simplify the identification of security requirements for individual systems.

2. Method of implementation

In consultation with a number of Health Care Establishments (HCEs) within Europe, the general care activities carried out by hospitals, general practitioners, community health care centres, and various other support services have been examined. This has enabled a generic model of the medical

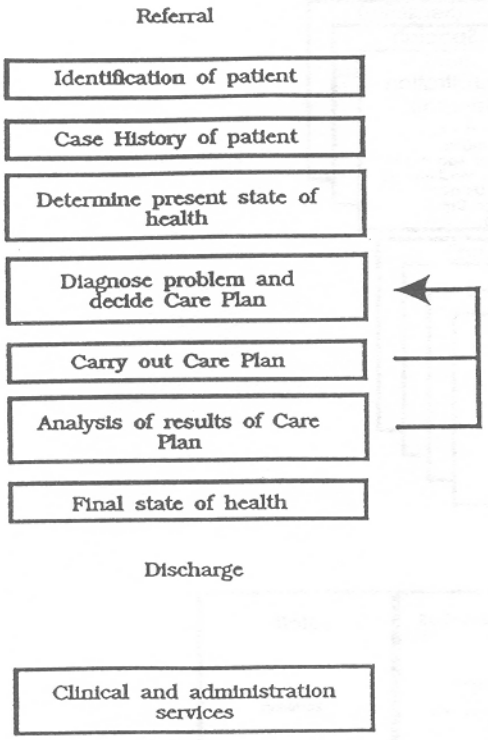

Fig. 1: General patient care activity

environment to be produced that can be used as the basis for further investigation [2].

The analysis established that, at a high level, all medical environments are of a similar nature (i.e. their aim is to provide a very similar set of services, albeit in slightly different ways, with differing levels of sophistication). The activities involved in the provision of health care can be seen to fall into the basic sequence of operations shown in Fig. 1.

At each stage of this sequence a variety of patient care or administration data may be generated or utilised from existing knowledge (i.e. medical or organisational). The type and quantity of information involved will be dependant upon the problems and requirements of the individual patients. In addition, the support services that surround the main care activities may also produce or use further data of their own.

This information may be of varying levels of sensitivity, and this will again be highly dependent upon the cases involved. Data relating to the clinical side of care delivery may be considered to fall into four main classifications in terms of sensitivity:

Operational:
Information used directly to make / govern patient care decisions. Can be subdivided into:
- **General** (the vast majority of patients)
- **Special** (e.g. HCE staff or special groups in the community)
- **Sensitive** (e.g. patients with sensitive problems such as AIDS or psychological disorders).

Non-Operational :
Information that does not directly govern patient decisions but is used for planning and resourcing purposes (e.g. analysis of workloads).

An overall view of the data involved is given by grouping them into the categories shown in Fig. 2. Obviously the categories shown are of a (necessarily) broad nature, but they may be broken down into further levels of detail as required. For example:

Patient Care
This group would contain the medical history, diagnosis, care decisions and treatment information that relate to individual patients. Data examples could be:

Episode information	Specific needs
Dates of admissions / discharges	Health care delivered
Staff involved	Drug therapy
Diagnosis including clinical coding/s	Outcome of the treatment
Care plan	Consultant and anaesthetist reports

The above groups now provide a generic framework encompassing all data required by a HCE. Specific medical applications may utilise information from all of the data groups, or simply a subset of them. It is consequently possible to map such applications onto the model, indicating the data groups that are involved. This can be used to highlight any weaknesses in the systems, and hence suggest the security services that may be required.

To illustrate how this mapping may be achieved,

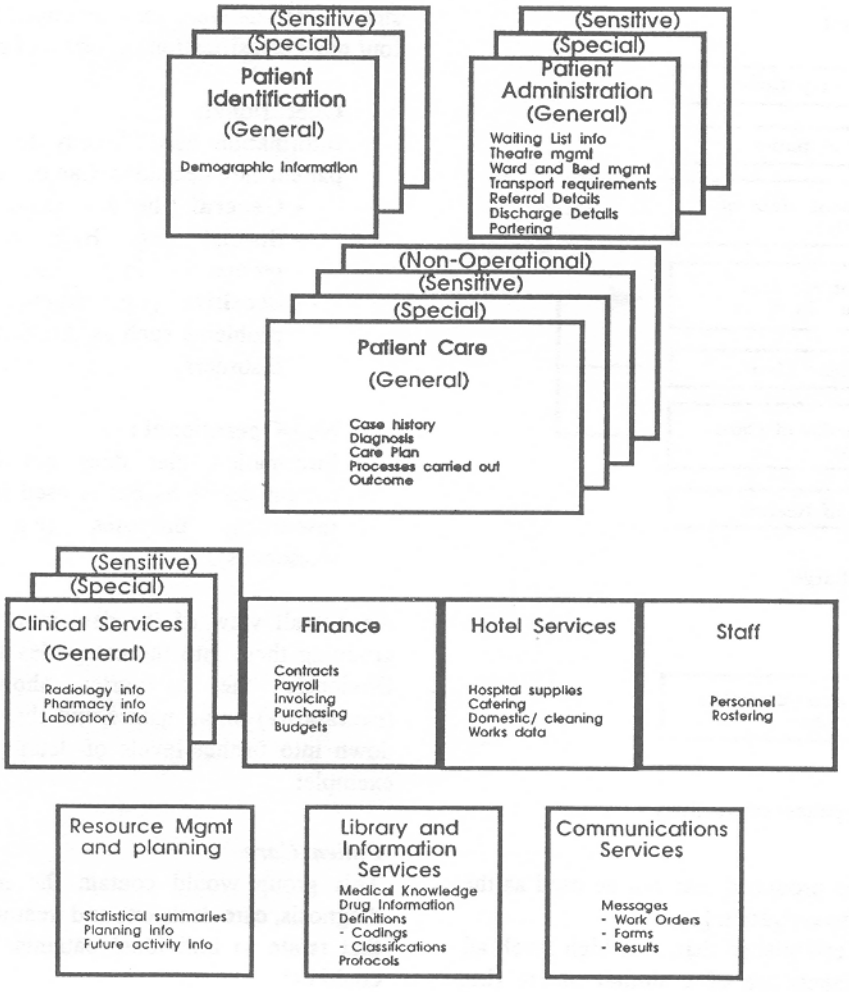

Fig. 2: General health care data groups

Fig. 3 shows how the Patient Administration System (PAS), as used by the Plymouth Health Authority, can be incorporated into such an arrangement.

At this stage the risks or threats that may be associated with each type of data in the system may be considered in terms of the core elements of security: disclosure of the information to either HCE staff or outsiders (confidentiality), denial of access to the information over various periods (availability) and modification or destruction of data (integrity) and user authentification. Several categories of risk can be identified, all of which must be considered in order to determine how serious their impact would be in each case:

- Commercial confidentiality
- Disruption
- Embarrassment
- Financial Loss
- Legal
- Personal privacy
- Safety

For example, the disclosure of sensitive patient care information to HCE outsiders could be seen as a serious risk in terms of legal action, patient personal privacy and embarrassment to both the patient and the HCE.

Each category of risk suggests certain protection

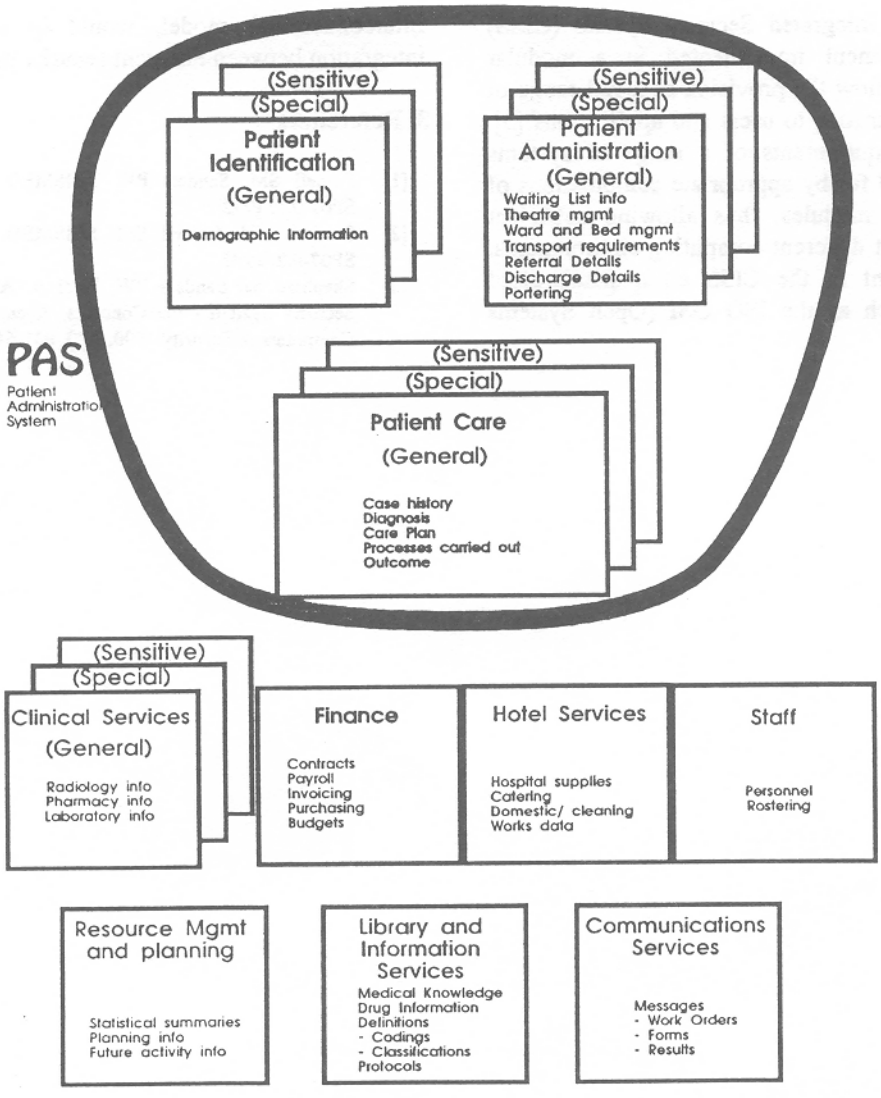

Fig. 3: Plymouth PAS mapping

measures that should be incorporated into a system. For example, in the cases of Embarrassment and Safety the following security services are suggested:

Embarrassment:
This requires a low to medium confidentiality service to be provided. In a low level system, standard password authentification with access limitation may be appropariate. For medium confidentiality the addition of card identification and audit may be more practical.

Safety:
This is the most important aspect from the patient care viewpoint, and warrants the highest possible levels of integrity as well as a strong backup source. Use of check codes and encryption, as well as full auditing and a high level of user authentification seems necessary.

A practical method of realising these security services in existing or new systems is to incorporate them as an add-on service. The use of a

Comprehensive Integrated Security System (CISS) overlay arrangement implemented in a modular fashion would allow the provision of a full range of services / mechanisms to users and applications [3]. The security requirements of a range of systems could be catered for by appropriate combinations of the generalised modules, thus allowing sufficient flexibility to suit different computing environments. The development of the CISS on a standardised architecture, such as the ISO OSI (Open Systems Interconnection) model, would in turn facilitate integration between different security domains.

3. References

[1] Furnell SM, Sanders PW. SEISMED Internal Report SP07-0.1, 1992.

[2] Sanders PW, Furnell SM. SEISMED Internal Report SP07-0.2, 1992.

[3] Shepherd SJ, Sanders PW, Patel A. A Comprehensive Security System - the Concepts, Agents and Protocols. Computers & Security 1990; 9(7): 631-643.