MED. INFORM. (1994), VOL. 19, NO. 3, 229–245

A generic methodology for health care data security

S. M. FURNELL†, P. N. GAUNT‡, G. PANGALOS§,
P. W. SANDERS† and M. J. WARREN†

† Security Research Group, Faculty of Technology,
University of Plymouth, UK
‡ Department of Health Care Informatics,
University of Plymouth/Derriford Hospital, UK
§ Informatics Laboratory, Faculty of Technology,
Aristotelian University of Thessaloniki, Greece

(*Received November 1993*)

Abstract. The aim is to outline the framework of a generic methodology for specifying countermeasures in health care environments. The method is specifically aimed at the enhancement of security in existing health care systems, and a key element is the use of predetermined 'profiles' by which these may be classified. Example scenarios are presented to illustrate how the concept could be applied in practice. The paper is based upon work that was initially 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 security recommendations for European health care establishments (HCEs).

Keywords: Risk analysis; System profiling.

1. Introduction

During the past few decades the use of information technology (IT) has become more widespread in all areas of society, and the types of activities that it performs or supports have become increasingly more important. As a result, information systems are now heavily utilized by all levels of staff, and relied upon to the extent that it would be difficult to manage without them.

The health care field has been no exception to the trend, as witnessed by the wide variety of applications that now handle many types of health data [1]. These systems contain vast amounts of information, much of it relating to individuals and of a sensitive nature. In addition to direct care applications, some parts of the European Community are now making the transition to a purchaser–provider funding system, meaning that an increasing volume of traditional business type data must also be maintained.

The combination of these points serves to make the protection of health information systems a vital concern, and necessitates that security is now considered as an essential aspect of the information technology field.

At a high level, information security is defined as being the combination of the following key factors [2]:

(1) *Confidentiality.* This refers to the prevention of unauthorized disclosure of information. All access to data must be restricted to authorized users who have a legitimate 'need to know'. Confidentiality is fundamental in health care since certain categories of data may be of a particularly sensitive nature,

0307–7640/94 $10·00 © 1994 Taylor & Francis Ltd.

and disclosure could result in significant embarrassment or prejudice to the individual concerned.

(2) *Integrity*. The prevention of unauthorized modification of information. There is a requirement to be able to trust the system and be confident that the same information can be retrieved as was originally entered. For example, the accidental or deliberate alteration of patient-related data could have serious implications for care delivery.

(3) *Availability*. Data and systems should be accessible and usable (by authorized users) when and where they are required. This requirement necessitates both prevention of the unauthorized withholding of information or resources, and adequate safeguards against system failure. In some medical environments, for example, critical systems may be required to be in operation 24 h a day, 7 days a week.

Security breaches may result from a variety of accidental or deliberate acts, with potential threats being posed by outsiders and from staff within the organization. Deliberate acts may include activities such as fraud, theft, hacking and virus infection. The health care field has certainly not been immune to these threats, with the most recent UK survey [3] showing that 10% of *reported* security incidents were related to health care systems (with roughly an even split between the above categories).

The introduction of information security seeks to eliminate or, more realistically, reduce the vulnerability to any risks that may be present. Protection must encompass the computer system and everything associated with it (e.g. from the computer unit itself to the building in which it is housed). Most important, however, is the protection of the information stored in the systems. These goals may be realized via a variety of measures [4], of both a technical and non-technical nature (e.g. physical, personnel and administrative controls).

In a health care establishment (HCE), any part of the computing system could provide the basis for a security breach, and this multiplicity of targets makes medical security a difficult issue. Large-scale introduction is complicated by the myriad of different system configurations (in terms of hardware, networking and actual applications) that may be identified within a single country, let alone within the full European scenario [5]. The issue is further complicated by the variety of information that may be held, and the fact that several different levels of data sensitivity may exist. The desired protection will depend upon several factors including the computer configuration, the operational environment and the information itself. As such it is impossible to assert a single level of security that will be appropriate for all cases without it being excessive in some applications.

Introducing security is a balancing process between providing the desirable level of protection against the maintenance of an adequate level of availability and performance (so that legitimate users have easy access to the data). Specifying the level of security that should be included involves some judgement about the dangers associated with the system, the required level of availability and the resource implications of various means of avoiding or minimizing those dangers.

Guidelines are therefore required on the selection of appropriate security measures, as well as on where and how to put them into HCE systems in general. The commonly accepted means of achieving this is to conduct a risk analysis investigation. However, this can be a time-consuming and costly proposition, and

may consequently be prohibitive in many cases. It would obviously be undesirable for security to be overlooked when this occurs. Given that many of the threats and vulnerabilities of individual HCEs are not unique, a full risk analysis in each case may also be largely unnecessary.

This paper proposes the framework of a methodology that is able to simplify the identification of security requirements for individual systems. This provides a straightforward means by which system administrators/security officers can select solutions appropriate for their own particular arrangements.

2. A conceptual overview of the generic methodology

Security should be examined from the perspective of the whole system, with all factors that influence protection requirements being considered. In general terms the security-relevant elements of existing systems are characterized as follows:

$$\text{Information system} = \text{Computer configuration} + \text{Operational environment} + \text{Data sensitivity}$$

These elements have been incorporated into the framework of a system protection methodology as shown in figure 1. This illustrates (at a high level) the steps involved in profiling existing systems to determine their requirements and select appropriate countermeasures.

The rationale of the methodology is that similar organizations/systems will have similar security requirements and a key factor in the approach was to devise a number of predetermined security 'profiles' for each element of existing systems. What the methodology proposes is a 'mix-and-match' approach to countermeasure selection, based upon a comparison of existing systems against general profiles. Using appropriate combinations it is possible, at a high level, to generate existing system profiles/categorizations that could then account for the majority of health care IT scenarios. From these it should be feasible to specify appropriate protection measures to meet the security requirements in each case.

The main elements of the methodology are now considered in more detail.

2.1. *Computer configuration*

This refers to the IT assets (both hardware and software) of the organization. At a high level it is possible to identify a relatively small number of elements which may be included in any given computer configuration, as shown in figure 2. Individual systems would be considered to determine which elements are applicable, and countermeasures selected accordingly. Examples of associated baseline countermeasures have been identified for each configuration, and are grouped as shown in table 1.

2.2. *Operational environment*

This considers the nature of the environment in which the IT assets are actually located and used, which may also affect the type and level of protection that is required. Table 2 indicates the main environmental considerations that may have security bearing. Appropriate combinations of these factors can be used to describe the majority of health care establishments (i.e. from GPs to general hospitals). Again, appropriate baseline countermeasures can be specified for each type of environment, and the key issues are indicated in table 3.

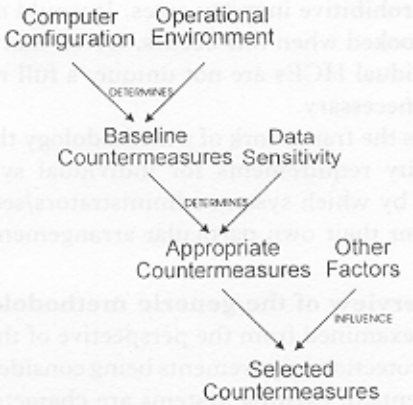

Figure 1. Existing system protection methodology overview.

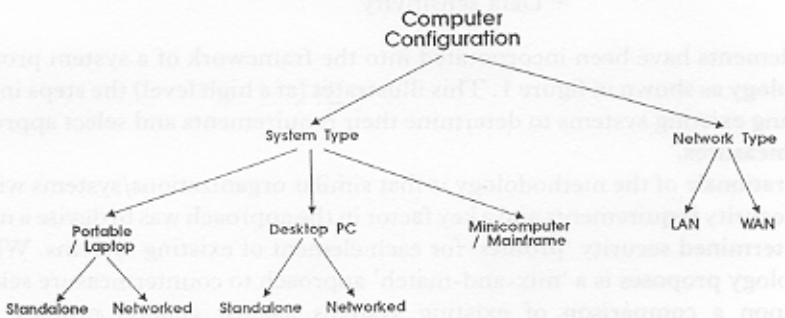

Figure 2. Computer configuration groups.

Table 1. Computer configuration countermeasure categories.

Category	Example issues
Physical	Physical access, theft prevention
Disaster planning	Maintenance contracts, alternative systems, backup arrangements
System	Authentication, logical access controls
Procedural	Backup/recovery policy, software usage, hardcopy control
Personnel	Operational training, computer-related awareness

2.3. *Data sensitivity*

The sensitivity of data is determined by two major factors, as shown in figure 3. These factors, and the means of rating sensitivity, will now be considered in more detail.

2.3.1. *Data type.* In consultation with a number of HCEs within Europe, the general care activities carried out by hospitals, general practitioners, community health care centres, and various other support services were examined. This enabled a generic model of medical data to be developed as the basis for further investigation [6]. The model is composed of 12 main data groups, as described in table 4. The purpose is to allow a simple means of specifying what data are available within

Table 2. Operational environment categories.

Factor	Options	Comments
Location	Fixed/mobile	Variable environment (e.g. portable computer system) limits environmental measures
	Rural/urban/city	Local environment is an indicator of local population density, crime potential and likelihood of natural disasters
Buildings	Single/multiple	Number of buildings will determine access control, site security requirements
	Old/modern	Age of building may indicate risk of fire, natural damage, etc.
People	Number (low, medium, high)	Number and mixture of people influences access controls and personnel-related measures
	Staff/contract/public	

Table 3. Operational environment countermeasure categories.

Category	Example issues
Site security	Building/site access, theft prevention
Disaster planning	Fire, flood, natural disasters
Procedural	Control of visitors, controls on smoking, eating/drinking
Personnel	Job recruitment/termination, awareness

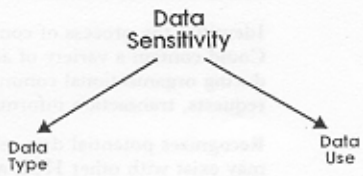

Figure 3. Factors of data sensitivity.

a system and help in the allocation of appropriate sensitivities, thus simplifying the process of identifying how and where data are located in different computer systems and networks. The information used by the HCE may be of varying levels of sensitivity, and this will again be highly dependent upon the cases involved.

The models groups are of a (necessarily) broad nature, but they may be broken down into further levels of detail as required. For example:

> *Patient care*: Episode information, Dates of admissions/discharges, Staff involved, Diagnosis including clinical codings(s), Care plan, Specific needs, Health care delivered, Drug therapy, Outcome of the treatment, Consultants' and anaesthetists' reports.

The model provides a generic framework that should encompass all data required by a HCE. Specific medical applications may store and communicate information from all of the data groups, or a particular subset of them. It is consequently possible to map such applications on to the model, indicating the data groups that are

Table 4. Generic data group descriptions.

Data group	Description
Patient identification	General information held regarding individual patients referred to the health care service. Often utilized by a number of different systems/applications
Patient administration	Information used in the day-to-day scheduling of various non-clinical care activities related to patients (i.e. concerned with the delivery of resources that in turn facilitate clinical care)
Patient care	Contains medical history, diagnosis, care decisions and treatment information relating to individual patients
Clinical services	Information related to the functioning of service departments of the HCE. Data are for the department's internal use (not patient-related)
Finance	Information covering all aspects of finance that are involved in the operation of HCEs
Hotel services	Information stored on all the basic 'housekeeping' functions of health care systems
Staff	Personnel information relating to all grades of HCE staff
Resource management and planning	Information used in the management, monitoring and planning of health care organizations
Library and information services	Encompasses the existing medical knowledge that is referenced by clinical staff, and national/local protocols for clinical management
Expert systems	Information utilized by decision support tools and/or neural networks within the HCE
Communication services	Identifies the process of communication within the HCE. Could contain a variety of additional data generated during organizational communication (e.g. activity requests, transaction information
External systems	Recognizes potential data relationships (interfaces) that may exist with other HCE applications/systems

Table 5. General categories of medical data usage.

Data use	Description
Operational clinical	Planning, delivery and monitoring of health care
Emergency care	Provision of care in a clinical emergency, where optimal conditions/information cannot be guaranteed
Critical clinical	Control of instrumentation/systems in direct feedback loops
Expert systems	Use in decision support tools or neural networks
Operational non-clinical	Supporting HCE infrastructure, but not directly influencing care of individuals
Financial	Contract management, purchasing and billing
Planning and resource managment	Aggregation of data for planning and review purposes
Quality management	Clinical audit, assessment of care efficiency and outcome
Clinical research	Identifiable or anonymized data used for research purposes; usually utilizes aggregated data

involved, and from this derive the basic sensitivity of the information. Examples of such mappings are given later in the text.

2.3.2. *Data use.* Incorporating this factor of data sensitivity into the methodology demands that an appropriate range of general uses can be identified. Related work within the SEISMED project [7] has determined a high-level set of data uses that are appropriate for our purposes. A total of nine categories is considered, as described in table 5.

2.3.3. *Sensitivity ratings.* Sensitivity is quantified in terms of several different types of impact that may relate to the data in the system. Four main types of impact can be identified, with appropriate countermeasures being given in each case.

(1) *Disclosure.* Unauthorized disclosure of information to HCE staff or outsiders.
(2) *Denial.* Denial of access to the information for varying periods.
(3) *Modification.* Accidental or deliberate alteration of the information.
(4) *Destruction.* Destruction of the system or information. An extreme form of unavailability.

The type and use of the data will have different influences over the protection requirements in each of these cases.

Disclosure. Data type is the most significant factor in determining the confidentiality requirement, as data will generally portray the same information in all contexts. The protection afforded should therefore remain constant regardless of which application uses it. However, data usage may still have some effect as it can influence problems arising through data aggregation. It is conceivable that, if certain data elements are combined, then the impact of disclosure may be greater than that of any one element in isolation.

Denial, modification and destruction. The requirements for these are primarily determined by the data usage, as the context will determine the seriousness of the impact.

Impacts are rated low, medium or high (where low indicates that the baseline countermeasure level is satisfactory, and high is the maximum protection that can be provided). The level is determined by considering a number of potential influencing factors: (*a*) confidentality (both personal and commercial), (*b*) disruption, (*c*) embarrassment, (*d*) financial loss, (*e*) legal, (*f*) personal 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. The level of impact will in turn determine the level of countermeasure.

Medical opinion from within various European HCEs was sought in obtaining the impact valuations (using a small survey distributed to appropriate personnel). Nevertheless, it is recognized that, because of the inherent subjectivity in any judgements (based largely on individual roles and/or perceptions of the problems), the resulting figures represent 'reasonable' rather than 'correct' values (i.e. values which the majority of health care professionals would be prepared to accept as an adequate representation of the situation).

2.4. *Other factors*

This element of the methodology highlights the fact that whilst the 'appropriate countermeasures' suggested may be suitable when considering the existing system in isolation, a number of real-world factors are also likely to influence the final selection process. Such factors are principally considered to include the following:

(1) *Cost constraints.* The cost of adopting particular countermeasures may be considered from several angles (e.g. financial, performance, practicality, etc.). The acceptable levels will obviously be highly dependent upon individual environments and their priorities. Financial cost is perceived as being a particularly key factor in security-related decision-making for the majority of health care establishments.
(2) *Operational constraints.* The selection of countermeasures will also be influenced by the nature of the organization itself. Any proposals must fit in with what is likely to be tolerated/accepted within the particular health care environment, and should not conflict too greatly with established practice. This relates to the 'business culture' of the organization.
(3) *Existing countermeasures.* Any security countermeasures that are already in place in relation to the existing system will obviously influence whether some of the suggested countermeasures need to be considered/adopted.

These would obviously be very subjective elements in the application of the methodology, and it is not possible to formalize them further.

2.5. *Countermeasures*

Actual security countermeasures are identified and refined at various stages within the methodology, and it can be seen from figure 1 that they are categorized under three headings. These are distinguished as shown below:

(1) *Baseline countermeasures.* Represents the minimal security considerations for a given computer configuration in a particular environment, and should be considered irrespective of the data held or the purpose(s) the system is used for.
(2) *Appropriate countermeasures.* Represents the overall set of countermeasures that may be appropriate for a given system, considering what data are used and how, but not taking into account any practical constraints that may apply in respect to implementation.
(3) *Selected countermeasures.* Represents the final output of the methodology, namely a set of countermeasures that may be added to the existing system to address the security requirements (having considered any imitations of the individual HCE).

The countermeasures used with the methodology are derived from a representative set that are being developed for use within the SEISMED project [8].

3. Methodology implementation

This section describes the specific steps by which the methodology would be implemented when considering individual existing systems.

In order to apply the method the following factors would need to be identified for the specific system/application being considered: (*a*) computer configuration involved, (*b*) type of operational environment(s), (*c*) data groups involved,

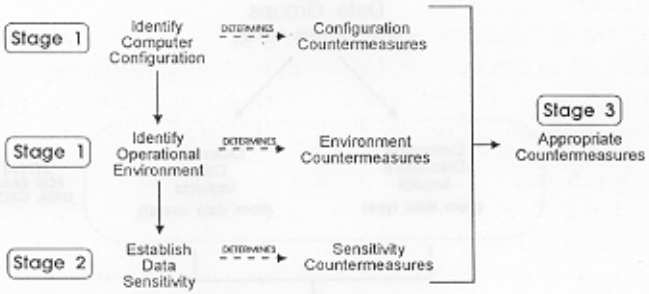

Figure 4. Methodology implementation steps.

(*d*) purpose of application (data use(s)). Countermeasures would then be derived as shown in figure 4. At each stage appropriate countermeasures would be selected from corresponding categories (NB: It is likely that some duplication may occur in terms of the countermeasures suggested within different categories).

The stages of the methodology may be more formally described as follows:

Stage 1: Determine basic system profile
Input: none.
Output: baseline countermeasures.
Description: categorize computer configuration and operational environment of the existing system according to predetermined profile categories. For computer configuration choose appropriate elements from: (*a*) laptop/portable, (*b*) desktop PC, (*c*) mini/mainframe, (*d*) network. For operational environment categorize elements of: (*a*) location, (*b*) buildings, (*c*) people.

Stage 2: Determine data sensitivity
Input: none.
Output: data-related countermeasures.
Description: establish data types and uses. Select countermeasures based upon sensitivities encompassed. Choose appropriate levels from *each* of: (*a*) disclosure countermeasures, (*b*) denial countermeasures, (*c*) modification countermeasures, (*d*) destruction countermeasures. This stage is described in more detail below.

Stage 3: Determine appropriate system countermeasures
Input: baseline countermeasures, data-related countermeasures.
Output: appropriate system countermeasures.
Description: generate countermeasure set that would satisfy the requirements of the existing system.

Stage 4: Select system countermeasures
Input: appropriate countermeasures.
Output: selected (final) system countermeasures.
Description: refine countermeasure set by considering any HCE specific factors/constraints that may apply.

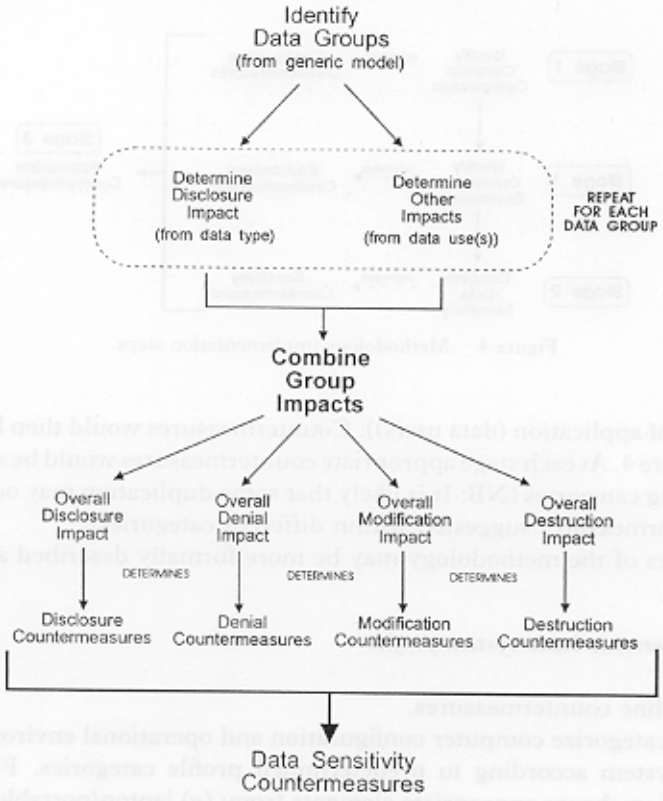

Figure 5. Determining data sensitivity.

3.1. *Determining data sensitivity*

Determining the data sensitivity countermeasures for an existing system is the most complex stage of the methodology, as they will be based upon a variety of impact values derived from the data involved. *All* data groups in the system must be considered to establish: (*a*) impact valuations for disclosure (based on data type only); (*b*) impact valuations for denial, modification, destruction (based on data type and use). The specific procedure involved is illustrated in figure 5. These stages and descriptions are listed below:

2.1. Identify the data groups involved using generic data model.
2.2. Determine disclosure impacts from model group valuations.
2.3. Identify general data usage category(s) that applies to the system.
2.4. Determine denial, modification and destruction impacts from usage valuations for each data group involved.
2.5. Derive overall sensitivity values for application by selecting 'worst-case' values from component groups (four values in total).
2.6. Determine appropriate data sensitivity countermeasures using values from 2.5.

4. Illustrative examples

The following section presents two basic examples to illustrate how the

methodology may be applied in practice. These are based on typical information system scenarios that may be found within the UK health service.

Note that the countermeasures and impact levels given in the examples are selected from predetermined lists. However, listing a full set of countermeasures is outside the scope of this paper, and the examples therefore provide only a small representative selection. It should also be noted that the examples only proceed to stage 3 of the methodology. The reason for this is that stage 4 is very much related to the subjective factors of real-world environments, and imposing artificial constraints would add little to the examples.

4.1. *Example 1*

4.1.1. Scenario. A patient records system maintained by a small GP practice. The system is primarily based upon a standalone PC, although selected data may be transferred to and from this using a portable computer that the GP takes on general visits and emergency call-outs. The practice is based in a single, modern building located in an inner city.

4.1.2. *Methodology implementation*

Stage 1: Determine basic system profile

Computer configuration: Laptop/portable—standalone; Desktop PC—standalone.

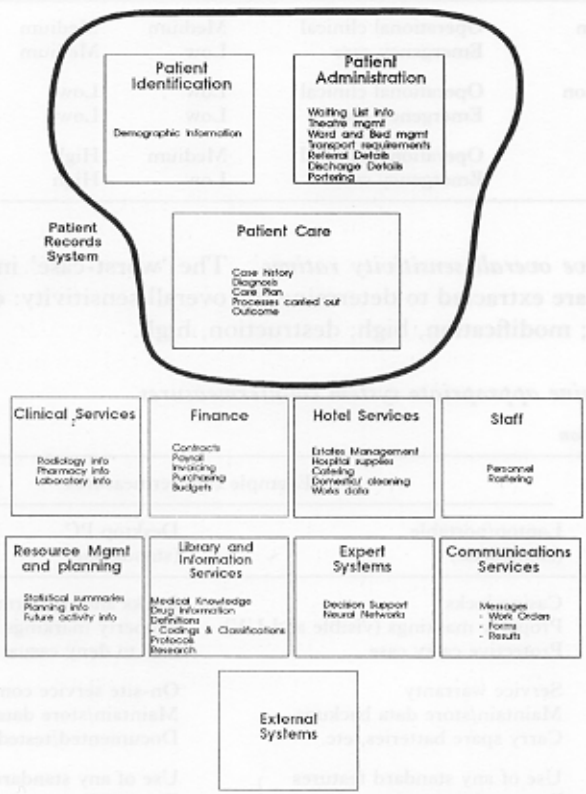

Figure 6. GP records system mapping.

Operational environment: Location—fixed and mobile, city; building—single, modern; People—staff, public, low.

Stage 2: Determine data sensitivity

Stage 2.1: Identify data groups. Three data groups are encompassed, and can be identified from the existing model as shown in figure 6.

Stage 2.2: Determine disclosure impacts

Data group	Impact level
Patient identification	Low
Patient administration	Medium
Patient care	High

Stage 2.3: Identify data uses. Potential data uses are identified as follows: (*a*) operational clinical, (*b*) emergency care.

Stage 2.4: Determine denial, modification and destruction impacts

		Impact levels		
Data group	Use	Denial	Modification	Destruction
Patient identification	Operational clinical	Medium	Medium	Low
	Emergency care	Low	Medium	Low
Patient administration	Operational clinical	Low	Low	Low
	Emergency care	Low	Low	Low
Patient care	Operational clinical	Medium	High	High
	Emergency care	Low	High	Medium

Stage 2.5: Derive overall sensitivity ratings. The 'worst-case' impacts from the previous tables are extracted to determine the overall sensitivity: disclosure, high; denial, medium; modification, high; destruction, high.

Stage 3: Determine appropriate system countermeasures

Computer configuration

	Example countermeasures	
Countermeasure category	Laptop/portable (standalone)	Desktop PC (standalone)
Physical	Casing locks	Locks and/or alarms
	Property markings (visible and UV)	Property markings (visible and UV)
	Protective carry case	Site to deny casual access
Disaster planning	Service warranty	On-site service contract
	Maintain/store data backups	Maintain/store data backups
	Carry spare batteries, etc.	Documented/tested recovery strategy
System	Use of any standard features	Use of any standard security features
	Password protection	Password protection
	Virus checking	Virus checking

	Hard disk encryption	Menu-only access (no DOS) Integrity checksums
Procedural	Store sensitive data on separate media Care of floppy disks Lock away when not in use Regular backup to desktop machine	Ban unauthorized software Control software updates Regular (automatic?) backups Care of floppy disks
Personnel	Stress individual accountability for machine/data when off-site	Provide software training Disciplinary procedures for misuse

Operational environment

	Example countermeasures	
Countermeasure category	Single-building/modern/city	Mobile
Site	Use of staff ID badges Receptionist/guard at main entrance Room access control (locks) Alarm systems	The nature of this environment is, by definition, variable, making it difficult to cite environment-specific countermeasures.
Disaster planning	Smoke and moisture detectors Fire alarm (linked to fire station)	Additional attention should therefore be devoted to the physical countermeasures relating to the computer configuration, with the level of protection being appropriate to account for the 'worst-case' scenario.
Procedural	Visitors escorted (non-public areas) Strangers challenged (non-public areas) Prohibit smoking	
Personnel	Controlled access hours Defined responsibilities Monitor maintenance work	

Data sensitivity

	Example countermeasures		
Countermeasure level	Disclosure	Denial/destruction	Modification
Medium	File-level passwords SMART cards Hard-copy controls	Regular recovery checks Alternative processing arrangements Disk shadowing Resource control	File-level passwords Integrity checksums Auditing
High	Encrypted transmission Encrypted storage Removable storage media Secure disposal of media/paper TEMPEST protection	Backup generators Separation of key assets	Digital signature Data encryption

4.2. *Example 2*

4.1.1. *Scenario.* A pharmacy department serving a large general hospital uses a minicomputer-based system for drug administration. The system may be accessed from a number of locations within the HCE over a local area network.

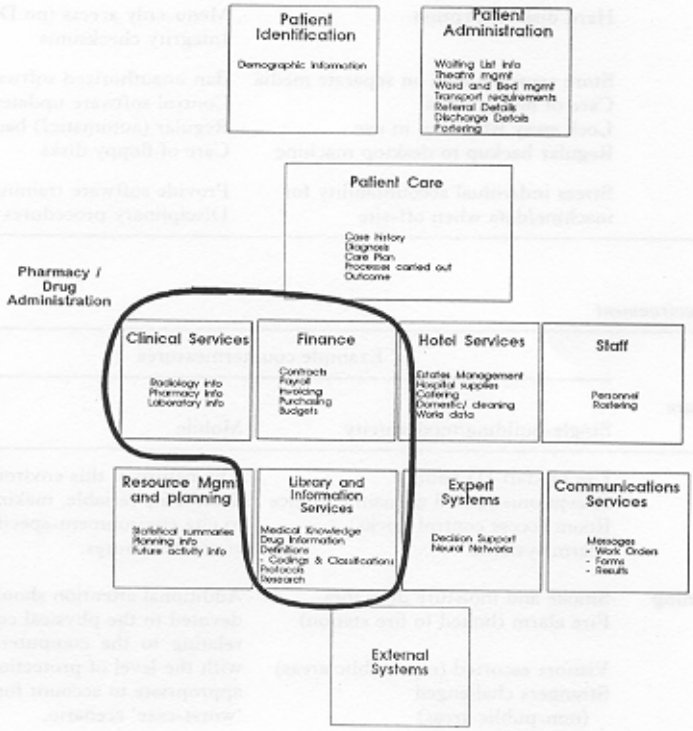

Figure 7. Drug administration system mapping.

4.1.2. *Methodology implementation*

Stage 1: Determine basic system profile

Computer configuration: mini/mainframe; Network—LAN.

Operational environment: location—fixed, urban; building—multiple, modern; people—staff, public, contract, high.

Stage 2: Determine data sensitivity

Stage 2.1. Identify data groups. Three data groups are encompassed, and can be identified from the existing model as shown in figure 7.

Stage 2.2: Determine disclosure impacts

Data group	Impact level
Clinical services	Low
Finance	Medium
Library and information services	High

Stage 2.3: Identify data uses. Potential data uses are identified as follows: (*a*) operational non-clinical, (*b*) financial, (*c*) planning and resource management.

Stage 2.4: Determine denial, modification and destruction impacts

		Impact levels		
Data group	Use	Denial	Modification	Destruction
Clinical Services	Operational non-clinical	Low	Medium	Medium
	Financial	Low	Medium	Medium
	Planning and resource management	Low	Low	Low
Finance	Operational non-clinical	Low	Medium	Medium
	Financial	Medium	Medium	Medium
	Planning and resource management	Low	Medium	Low
Library and information services	Operational non-clinical	Medium	Medium	Medium
	Financial	Low	Low	Low
	Planning and resource management	Low	Medium	Low

Stage 2.5: Derive overall sensitivity ratings. The 'worst case' impacts from the previous tables are extracted to determine the overall sensitivity: disclosure, medium; denial, medium; modification, medium; destruction, medium.

Stage 3: Determine appropriate system countermeasures

Computer configuration

Mini/mainframe		Network (LAN)	
Countermeasure category	Example countermeasures	Countermeasure category	Example countermeasures
Physical	Control access to computer suite	Physical	Protect cabling from interference/tampering (data and power)
	Identifiable marking on terminals		Provide alternate routeing
	Site to deny casual access/viewing		
Disaster planning	24-hour maintenance contract	System	Monitor for overuse/failure
	Duplicate/alternative system		Automatic re-routeing
	Maintain/store data backups		Integrity checking on transmission
	Prioritize recovery options		Secure WAN gateways
	Documented/tested recovery plans		
System	Use OS security features	Procedural	Maintain list of network assets/access points
	Access time/location controls		
	Enforced password criteria		
	Automatic terminal logout		
	Auditing of activity		
Procedural	Log/investigate reported variances		
	Control software development/updates		
	Formal testing of new programs		
Personnel	Provide software training		
	Disciplinary procedures for misuse		
	Avoid reliance on individuals		

Operational environment

Multi-building/modern/urban	
Countermeasure category	Example countermeasures
Site	Security patrols Closed-circuit TV monitoring Use of staff ID badges Receptionists/guards for sensitive areas Room access control (locks) Alarm systems
Disaster planning	Smoke and moisture detectors Fire alarm (linked to fire station) Backup generator
Procedural	Visitors escorted (non-public areas) Strangers challenged (non-public areas) Prohibit smoking
Personnel	Defined responsibilities Controlled access hours Monitor maintenance work

Data sensitivity

	Example countermeasures		
Countermeasure level	Disclosure	Denial/destruction	Modification
Medium	File-level passwords SMART cards	Regular recovery checks Alternative processing arrangements	File-level passwords Integrity checksums
	Hardcopy controls	Resource control Disk shadowing	Auditing

5. Future enhancement

The most significant extension that is planned is to develop an expert system to be used in conjunction with the methodology. This would contain the expert knowledge necessary to apply the methodology, as well as a knowledge base of appropriate countermeasures.

An expert system would contribute further to the user-friendliness and general accessibility of the method, as it would allow the techniques to be used by health care staff who were not necessarily security-trained (e.g. a hospital general manager). A major advantage of this would be cost, as expensive consultancy would not be required to carry out security reviews. If the system was developed for PC environments it could be made available in nearly all HCE environments.

6. Conclusions

The paper should have served to illustrate how high-level categorizations of health care systems may be used to simplify considerably the process of security selection. Such an approach would be valuable in cases where a full security review has been denied on the grounds of budget or inconvenience.

It is envisaged that the overall methodology should be compatible with the majority of systems, catering for a range of general existing system categorizations. Despite this, however, it is still conceivable that systems will be encountered that do not fit comfortably within the profiles suggested. In these cases it will be necessary to perform a more detailed risk analysis to determine the specific requirements of the system/environment. Additionally, in systems where extremely high levels of risk are identified, more detailed study is also advisable.

The methodology itself is at an early stage of development, and requires further refinement before it can be considered practically viable. The next stage of development will be to encompass it within an expert system so that it can be used within various HCE environments. This will serve to test the methodology and allow adjustments to be made accordingly.

Acknowledgements

We would like to acknowledge the various partners and collaborators within the SEISMED project for their contributions to the content of this paper.

References

1. ABBOT, W. (1992) *Information Technology in Health Care—A Handbook* (London: Longman, in association with the Institute of Health Services Management).
2. ITSEC (1991) *Information Technology Security Evaluation Criteria, Provisional Harmonised Criteria* (Commission of European Communities).
3. AUDIT COMMISSION (1990) *Survey of Computer Fraud and Abuse.*
4. MUFTIC, S., PATEL, A., SANDERS, P., COLON, S., HEIJNSDIJK, J., and PULKKINEN, V. (1993) *Security Architecture for Open Distributed Systems* (Chichester: Wiley).
5. TRITECH (1992) *Report of Questionnaire Study 1992—Statistical Tables and Verbal Responses.* SEISMED Internal Report SP03-01.
6. SANDERS, P. W., and FURNELL, S. M. (1993) Data security in medical information systems using a generic model. *Proceedings of MIE 93 Congress*, Jerusalem, 18–22 April.
7. GAUNT, P. N., and FRANCE, R. F. (1993) The need for security in health care information systems—a clinical view. SEISMED Internal Report SP11-02.A08.02.
8. FURNELL, S. M., and SANDERS, P. W. (1993) First draft guidelines for existing systems. SEISMED Internal Report SP07-0.7.