Addressing the problem of data security in healthcare information systems

S M Furnell,* P W Sanders* and M J Warren†

*Network Research Group, School of Electronic, Communication and Electrical Engineering, University of Plymouth, Plymouth PL4 8AA

†Innovation and Technology Research Group, Plymouth Business School, University of Plymouth, Plymouth PL4 8AA

Keywords: SECURITY, GUIDELINES, AWARENESS, WORLD WIDE WEB

Summary

With the increasing use of information technology at all levels of the healthcare environment, this paper identifies the need for appropriate security guidance and awareness to protect the various information systems involved. An overview of two European projects (AIM SEISMED and Health Telematics ISHTAR) is given, describing the work that has been done to develop and promote healthcare security issues. This has specifically included the development of a range of security guidelines and the establishment of a World Wide Web service to support dissemination and awareness activities.

The discussion also identifies that any security mechanisms adopted must be workable within the financial and operational constraints of the healthcare environment. It is concluded that information security will be increasingly vital to ensure the peace of mind of healthcare staff and patients. However, while the work described provides a solid foundation for building protection, the co-operation of individual establishments will ultimately be required to achieve success.

Introduction

The increasing use of information technology (IT) in healthcare has now come to affect virtually all aspects of operation, ranging from direct care delivery to various support and administration functions. While the technology has many advantages, the whole issue of IT introduction presents problems of implementing change and enabling staff to adapt to new systems.

One particular problem area that arises is the need to address information system security. In short, the transition to computer-based systems opens up a whole new range of considerations in terms of maintaining the confidentiality, integrity and availability of healthcare data. Staff at all levels will be affected by these issues and the preservation of security should be an ever-present requirement in day-to-day activities.

The significance of the issue is illustrated by the recent high-profile disagreements between the UK National Health Service (NHS) and the British Medical Association (BMA) over the absence of encryption in the NHS network.[1] However, security comes down to much more than just encryption, and a range of issues must be considered in the healthcare environment. Unfortunately, there has been little detailed guidance in this area, due to the absence of specific security recommendations for the medical environment and the fact that many healthcare establishments (HCEs) do not have access to appropriate expertise. Steps have been taken to rectify these problems in recent years and the next sections will discuss the work of two European Union projects (AIM SEISMED and Health Telematics ISHTAR) which have specifically targeted the issue of HCE security.

The SEISMED project

The SEISMED (Secure Environment for Information Systems in MEDicine) project was a three-and-a-half year initiative, established under the European Commission's Advanced Informatics in Medicine (AIM) programme. The stated objective of the work was to provide practical security advice and guidance to all members of the healthcare community who are involved in the management, development, operation, and maintenance of information systems. The eventual aim was to establish a consistent, harmonised framework for the protection of healthcare systems and data at a European level.

The project began by assessing current security practices, by means of a general survey of European HCEs and by mounting detailed risk-analysis investigations at four participating reference centres. These activities fed into the development of a range of security guidelines, covering the following key areas:

1. high level security policy;
2. guidelines for healthcare risk analysis;
3. guidelines for system design and implementation;
4. guidelines for security in existing operational systems;
5. guidelines for data encryption;
6. guidelines for healthcare network security; and
7. health informatics deontology / code of ethics.

Each set is further subdivided into specific sections targeting HCE management, technical staff, and general users.[2–4] All the guidelines that were developed (with the exception of the legal framework) were implemented and tested within the reference centres, leading to further revisions in light of practical experiences. A simplified diagram showing the interrelationships between the various workpackages is given in figure 1.

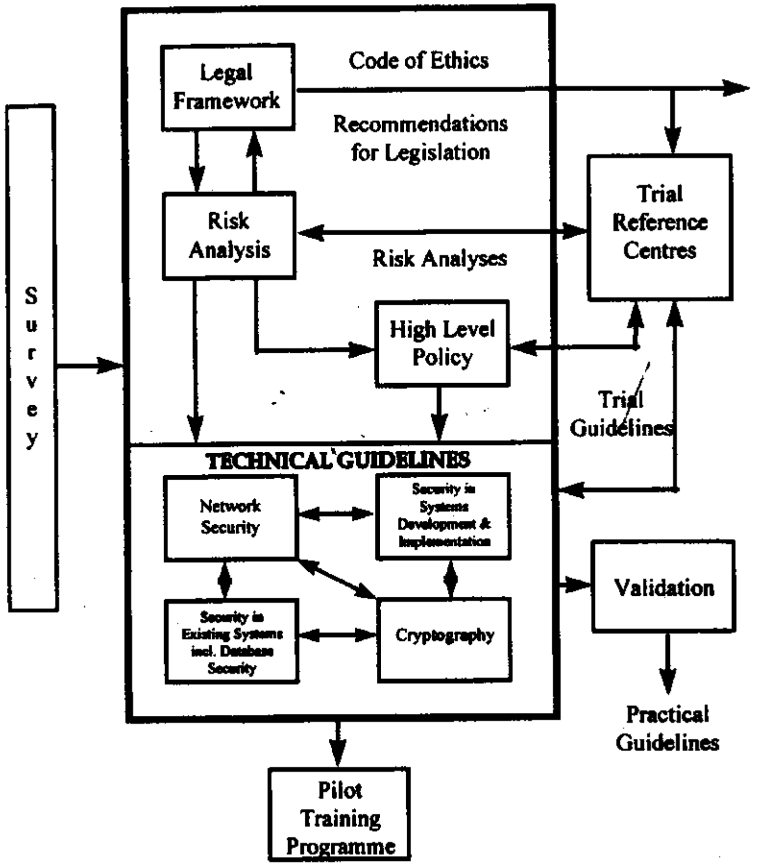


Figure 1 SEISMED workpackage interrelationships

As an illustration of how the guidelines were realised, the discussion will now consider the example of the guidelines for security in existing systems, with which the authors were specifically involved. A suggested baseline level is defined, with recommendations tailored to the addition or enhancement of security in cases where appropriate safeguards are currently lacking. A total of 138 guidelines (grouped under ten protection principles) were identified, covering all of the key aspects that should be considered. The principles are listed in table 1,

Table 1a Principles of security for existing systems

Title	Main issues
Security policy and administration	– the need for a security policy; – policy awareness issues; – co-ordination and administration of security; – use of specialist security personnel.

Physical and environmental security	– physical access control;
	– security of HCE equipment;
	– protection against natural disasters;
	– environmental controls;
	– various procedural measures.

Disaster planning and recovery	– continuity plans (development, testing and update); – fallback arrangements; – post-disaster procedures and controls.
Personnel security	– staff recruitment; – contractual agreements; – security of working practices; – staff appraisals and monitoring; – termination of employment.
Training and awareness	– the need for security awareness; – specific areas that must be addressed (job training, use of information systems); – recommendations for internal/HCE training and awareness initiatives; – use of specialist training courses; – assignment of training responsibilities.

Table 1b Principles of security for existing systems (continued)

Title	Main issues
Information technology facilities management	– system planning and control; – the importance of maintaining back-ups; – media controls; – auditing and system monitoring; – virus controls; – documentation issues.
Authentication and access control	– requirements for user identification and authentication; – password issues; – system and object access restrictions; – methods of control; – access in special cases (eg system management, third parties, temporary staff).
Database security	– control of medical database software; – database organisation and administration; – database operation issues.
System maintenance	– controls to prevent unauthorised changes to and upgrades of HCE software, vendor software and operating systems; – requirements for testing and acceptance.
Legislation compliance	– data protection; – abuse of information systems; – prohibition of 'pirated software'; – compliance with internal security standards; – retention and protection of business records.

along with an indication of the main issues that are encompassed in each case.

It should be evident that the overall set of guidelines provides very comprehensive coverage of the security issues that pertain to healthcare establishments. However, the problem does not end here and (at least) two further issues must be considered:

1. the guidelines must be promoted to the healthcare community;
2. the guidelines must be regularly reviewed and updated to maintain their relevance.

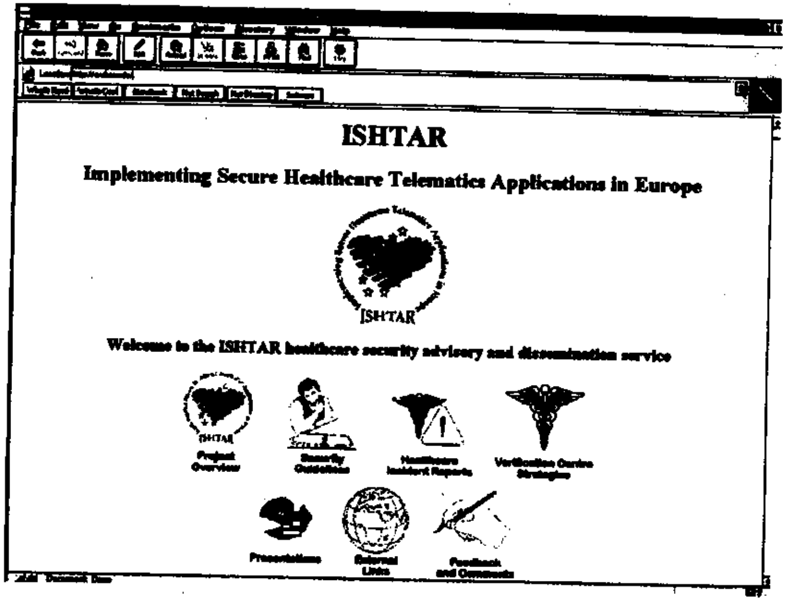
Aspects of this work are being undertaken in a successor project to SEISMED, as described in the next section.

The ISHTAR project

The work on the promotion and maintenance of the guidelines is now continuing as part of the Health Telematics ISHTAR (Implementing Secure Health Telematics Application in euRope) project — a three-year initiative that commenced at the beginning of 1996. The project aims to address a range of issues to support healthcare security, with the outputs from SEISMED providing a general basis for the work. In addition to the enhancement of existing material, some of the main activities include the establishment of an expert advisory panel, a healthcare incident reporting scheme, and security training programmes. A total of ten HCEs from across the European Union are involved as verification centres, providing practical advice and feedback on the work.

Another key aspect of this work, and the area with which the authors are principally involved, is the establishment of a World Wide Web (WWW) service to allow the dissemination of the guidelines and other relevant healthcare security publications in electronic format. A number of potentially useful services will be offered, including:

1. provision of online access to 'highlights' from the security guidelines, with search and feedback options;
2. descriptions of example healthcare protection scenarios/'roadmaps' for providing security;
3. anonymised results from the ISHTAR incident reporting scheme;



ISHTAR

Implementing Secure Healthcare Telematics Applications in Europe

Welcome to the ISHTAR healthcare security advisory and dissemination service

Figure 2 Prototype ISHTAR home page

4. project information and external links to other relevant WWW sites; and
5. other occasional supporting services (eg online presentations).

The high-level options are illustrated in figure 2, which depicts the (prototype) home page for the service.

It is considered that the provision of security advice in this manner will offer a number of advantages in that it will:

1. facilitate the promotion of security to a wider audience;
2. help to ensure that consistent advice is given to different HCEs on similar issues;
3. enable the provision of basic advice that will be appropriate to many scenarios;
4. enable savings on external consultancy costs; and
5. help to reduce the burden on any local security expertise.

Whilst the web service will not totally remove the need for localised security promotion and training (eg the need for staff to be familiar with HCE-specific procedures), it is considered to represent a significant step towards general security awareness.

Other considerations

Even with the successful promotion of comprehensive guidelines, there are other potential problems to be addressed in terms of both the financial and organisational impacts of security. The nature of the healthcare environment is such that it will not tolerate security measures if they are too expensive to implement or have too great an impact on existing practices.

In financial terms, security represents an overhead that does not directly contribute to the primary objectives of the HCE. Expenditure is normally prioritised so that clinical services (ie those in direct contact with patients and advantageous to a large population) will generally obtain funding more easily than support services. The frequent reports of shortages in healthcare (eg in terms of waiting lists for beds and treatment) indicate the level to which even these resources are often restricted. Hence investments to improve security may be considered somewhat secondary and will normally only be approved if the benefits to the HCE can be demonstrated to be of greater importance than if the money was directed at the addition or enhancement of clinical services. As an illustration of the financial constraints, European Commission[5] statistics indicate that expenditure on informatics overall represents only 0.4% of the yearly running costs of a hospital (the majority being taken up by supplies (26%) and personnel (68%) costs).

Another consideration in determining appropriate security is that of convenience. It has been identified[6] that getting healthcare professionals (HCPs) to use information systems in the first place can often be a problem, as system designers frequently do not take into account the clinical environment and the ways in which users are motivated. It is considered that the addition of cumbersome or restrictive protection measures could only worsen this situation (with possible effects including demotivation of staff and reduced efficiency). In some contexts this significantly limits the possible approaches, as it is generally difficult to implement strong security while still maintaining a convenient and user-friendly environment. However, the general requirement that comes through is that non-intrusive mechanisms should be employed whenever possible, so as not to interfere significantly with HCE operations and the ability to deliver care effectively.

Conclusions

With the continuing advancement of IT in healthcare, the issue of ensuring adequate security will become increasingly important for maintaining the peace of mind of both HCPs and their patients.

The current guidelines provide a solid foundation upon which a secure healthcare environment may be realised. However, it is likely that many HCEs will currently be operating with security measures below the baseline levels that are advocated. As such, conformance to the recommendations may involve considerable effort.

It will also be important that HCEs are actually aware of the guidelines and other relevant security issues. The WWW service will be a valuable resource in this respect, providing an easily accessible source for day-to-day reference.

SEISMED and ISHTAR are only two examples of projects that have addressed healthcare security, and various other initiatives are also in progress at both national and European levels. However, it must be remembered that these efforts will come to nothing without the co-operation of individual HCEs. The responsibility for implementing the recommendations and maintaining awareness will ultimately be theirs. Consequently, the promotion of sensible advice which considers the practical constraints of the healthcare environment will be important in ensuring that this can occur.

Acknowledgements and further information

This paper has arisen from the authors' involvement in the ISHTAR Project (Implementing Secure Healthcare Telematics Applications in Europe). A Telematics Applications for Health Project (HC1028) of CEC DGXIII C.

Further information about both the SEISMED and ISHTAR projects can be obtained from: Alison Treacher, PO Box 231, Burton upon Trent DE13 8ZX, UK; or Prof Sokratis Katsikas, University of the Aegean, 30 Voulgaroktonou Street, Athens 114 72, Greece.

References

1. Jones R. Doctors condemn NHS data security. *Computing* 1996; March 28: 1.
2. SEISMED Consortium. *Data security for health care. Vol 1: Management guidelines*. Amsterdam: IOS Press, 1996.
3. SEISMED Consortium. *Data security for health care. Vol 2: Technical guidelines*. Amsterdam: IOS Press, 1996.
4. SEISMED Consortium. *Data security for health care. Vol 3: User guidelines.* Amsterdam: IOS Press, 1996.
5. De Moor G, Lacombe J, Noothoven van Goor J, Thayer C. *Telematics for health care: Its impact? Its future?*. Produced by ACOSTA for the Commission of the European Union AIM programme, 1994.
6. Young D. Can we get doctors to use computers? *Health Services Management* 1996; 6: 116–18.