CEN REPORT

RAPPORT CEN

CEN BERICHT

CR 13694

August 1999

ICS

English version

Health Informatics - Safety and Security Related Software Quality Standards for Healthcare (SSQS)

This CEN Report was approved by CEN on 16 June 1999. It has been drawn up by the Technical Committee CEN/TC 251.

CEN members are the national standards bodies of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Central Secretariat: rue de Stassart, 36 B-1050 Brussels

Ref. No. CR 13694:1999 E

CONTENTS

FOREWORD

INTRODUCTION

1. SCOPE

2. REFERENCES

3. DEFINITIONS

4. ACRONYMS

5. CLARIFICATION OF ISSUES IN HISs
5.1 Definitions of Safety, Security and Dependability
5.1.1 Safety
5.1.2 Security
5.1.3 Dependability
5.2 Medical Devices versus HISs
5.3 Procurement Process
5.4 Risk Assessment
5.5 Certification of Systems and In-service Feedback
5.6 The Year 2000 (Y2K) Problem

6. SUMMARY OF EXISTING AND EMERGING STANDARDS/GUIDELINES

7. DISCUSSION OF THE REVIEWED DOCUMENTS
7.1 Review of Security Documents
7.2 Review of Safety Documents

8. ISSUES TO BE CONSIDERED BY FUTURE WORK
8.1 Determining the Criticality and Type of HISs
8.1.1 Criticality of HISs
8.1.2 Types of HISs
8.2 Development of HISs
8.3 Clinical Testing
8.4 Incident Reporting Mechanism
8.5 Clinician/Supplier Involvement in the Standardization Process

9. RECOMMENDATIONS

ANNEX A: Healthcare and Security Related Standards
A1 CEN/TC251 (Euro)
A2 NHS Executive (UK)

A3 American Society for Testing and Materials (ASTM) (USA)
A4 Computer-based Patient Record Institute (CPRI) (USA)
A5 HL7 Inc (Canada)
A6 Privacy Commissioner (New Zealand)
A7 Standards Australia (SA) (Australia)
A8 Standards Australia/Standards New Zealand

ANNEX B: Non-Healthcare and Security Related Standards

B1 British Standards Institution (BSI) (UK)
B2 ITSEC (UK)
B3 Central Computer and Telecommunications Agency (CCTA) (UK)
B4 Accredited Standards Committee (ASC) X12. (USA)
B5 ISO/IEC (International)

ANNEX C: Healthcare and Safety Related Standards

C1 CEN TC/251 (Euro)
C2 Medical Devices Agency (UK)
C3 British Standards Institution (UK)
C4 IEC (International)
C5 IEEE (USA)
C6 American Society for Testing and Materials (ASTM) (USA)

ANNEX D: Non-Healthcare and Security Related Standards

D1 IEC (International)
D2 Ministry of Defence (UK)
D3 Requirements and Technical Concepts for Aviation (RTCA) Inc. (USA)

ANNEX E: Standards in Quality Management and Quality Assurance

ANNEX F: Projects Related to the Security of HISs

F1 SEMRIC
F2 MEDSEC
F3 SEISMED
F4 ISHTAR
F5 G7 ENABLE
F6 TEAC – HEALTH

FOREWORD

This CEN Report has been prepared under the direction of the European Committee for Standardization (CEN). The preparation of this CEN Report was undertaken by PT 38 under the direction of Working Group III of CEN/TC 251 under Work Item: SSQS.

This CEN Report has undergone a review under the CEN Request for Comments Procedure and subsequently approved by WGIII during the WGIII meeting held in London, UK on 1999-02-01/02.

TC 251 is requested to approve this CEN Report as the final deliverable fo PT38.

An electronic copy of this CEN Report is available from the CEN/TC 251/WGIII website on;

http://forum.afnor.fr/WORK/AFNOR/GPN2/S95I/PRIVATE/WEB/ENGLISH

INTRODUCTION

Healthcare Information Systems (HISs) are increasingly being used within the healthcare sector, and, as a consequence, they are coming closer to the patient and clinicians are becoming much more dependent on their use. For instance, these systems can range from simple databases that are used to record and store medical data, to medical expert systems that are used to assist in the process of diagnosis of an illness. Hence, any malfunction of HISs can have implications for patient safety. Also, unauthorised access to medical data can lead to a breach in patient confidentiality or more seriously unauthorised changes to medical data can lead to incorrect diagnosis which can have an impact on patient safety.

Due to the nature of HISs and the environment in which they must operate, these systems must be developed to ensure that the issues of safety and security are pursued to a level that is considered to be acceptable for the application. Thus, there is a need for standards and documents which ensure that;

- HISs are developed using appropriate techniques;
- HISs are certified to be safe and secure;
- HISs are used in the appropriate manner;
- HISs are adequately maintained;
- incidents concerning HISs are monitored.

1. SCOPE

This CR presents a review of the existing and emerging standards that are, or may be, applicable to HISs. The type of standards that are considered are those that focus on the issues of software safety, security, confidentiality, and integrity. This CR also provides a discussion of the issues that need to be addressed in compiling a guidance for purchasers and developers of HISs.

This CR also examines some standards which do not necessarily concern HISs but instead refer to general computer-based systems. These standards are examined because it is considered that they may be applicable, or adapted, to Healthcare Systems. The standardising organisations examined in this review include: IEC, CEN, BSI, ASC X12, ASTM, CPRI and IEEE.

The discussion in this CR highlights that many standards and guidelines have been developed to address the security of HISs, but few standards address the safety issues. However, several safety standards do exist that address medical devices, medical equipment or general safety related systems. These standards may be adapted or used to develop safety standards for HISs.

From the review presented in this CR, it is concluded that future standardization work in HISs should give greater consideration to the safety aspects of these systems. Specifically, the areas that should be addressed are: determining the criticality of HISs, defining the approaches and methods for developing HISs, providing facilities for performing clinical testing of HIS and the setting of an incident reporting mechanisms to monitor the in-service operation of HISs.

2. REFERENCES

This CR cites the following key references at appropriate places in the text. A fuller description of reference documents and projects is provided in the appendices;

BS 7799 (Part 1)	Information Security Management – Code of Practice
BS 7799 (Part 2)	Information Security Management – Accreditation Process
EN 1441	Medical Devices – Risk Analysis.
EN 60601-1-4	Medical Electrical Equipment – Part 1: General Requirements for Safety – 4. Collateral Standard: Programmable Electrical Medical Systems.
ENV 12924	Medical Informatics – Security Categorisation and Protection for Healthcare Information.
IEC 61508	Functional Safety – Safety Related Systems.
ITSEC	Information Technology Security Evaluation Criteria.

[1] I. Peterson, “Fatal Defects“, Vintage Books, ISBN 0-0991-9742-1, 1996.
[2] P.G. Neumann, “Computer Related Risks“, Addison Wesley, ISBN: 0-201-55805-x, 1995.
[3] J.C. Laprie, ‘Dependability: A unifying concept for reliable computing and fault tolerances’, In T. Anderson (Ed.), ‘Dependability of Resilient Computers’ Blackwell Sciences Publications, Oxford, 1989, pp 1-28.
[4] J.A. McDermid, ‘On dependability, its measurement and its management’, High Integrity Systems, Vol. 1, No. 1, 1994, pp 17 -26.
[5] R.J. Anderson, “Safety and Privacy in Clinical Information Systems“,
[6] J. Vowler, “Patient care at risk from millennium bug“, Computer Weekly, May 1997, p. 3.
[7] R.S. Pressman, “Software Engineering: a practitioner’s approach“, McGraw-Hill International, 1994.
[8] C. Mazza, J. Fairclough, B. Melton, D. De Pablo, A. Scheffer, and R. Stevens, “Software Engineering Standards“, Prentice Hall, 1994.