

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

ICS 35.240.80; 35.080

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

National foreword

This Published Document reproduces verbatim CR 13694:1999.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health Informatics, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the CR title page, pages 2 to 53 and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

This Published Document, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 November 1999

© BSI 04-2000

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
National foreword	Inside front cover
Foreword	ii
Text of CR 13694	5

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.

CEN

European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

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

© 1999 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

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>

Contents

	Page	Page		Page
Foreword	2	A.8 Standards Australia/Standards New Zealand	40	
Introduction	5	Annex B Non-Healthcare and Security Related Standards	41	
1 Scope	5	B.1 British Standards Institution (BSI) (UK)	41	
2 References	5	B.2 ITSEC (UK)	41	
3 Definitions	6	B.3 Central Computer and Telecommunications Agency (CCTA) (UK)	41	
4 Acronyms	6	B.4 Accredited Standards Committee (ASC) X12. (USA)	41	
5 Clarification of issues in HISs	7	B.5 ISO/IEC (International)	42	
5.1 Definitions of Safety, Security and Dependability	7	Annex C Healthcare and Safety Related Standards	44	
5.1.1 Safety	7	C.1 CEN TC/251 (Euro)	44	
5.1.2 Security	8	C.2 Medical Devices Agency (UK)	45	
5.1.3 Dependability	9	C.3 British Standards Institution (UK)	46	
5.2 Medical Devices versus HISs	9	C.4 IEC (International)	46	
5.3 Procurement Process	10	C.5 IEEE (USA)	47	
5.4 Risk Assessment	10	C.6 American Society for Testing and Materials (ASTM) (USA)	48	
5.5 Certification of Systems and In-service Feedback	10	Annex D Non-Healthcare and Security Related Standards	48	
5.6 The Year 2000 (Y2K) Problem	10	D.1 IEC (International)	48	
6 Summary of existing and emerging standards/guidelines	11	D.2 Ministry of Defence (UK)	49	
7 Discussion of the reviewed documents	22	D.3 Requirements and Technical Concepts for Aviation (RTCA) Inc. (USA)	49	
7.1 Review of Security Documents	22	Annex E Standards in Quality Management and Quality Assurance	50	
7.2 Review of Safety Documents	24	Annex F Projects Related to the Security of HISs	50	
8 Issues to be considered by future work	28	F.1 SEMRIC	50	
8.1 Determining the Criticality and Type of HISs	29	F.2 MEDSEC	51	
8.1.1 Criticality of HISs	29	F.3 SEISMED	51	
8.1.2 Types of HISs	30	F.4 ISHTAR	51	
8.2 Development of HISs	30	F.5 G7 ENABLE	52	
8.3 Clinical Testing	31	F.6 TEAC — HEALTH	52	
8.4 Incident Reporting Mechanism	31	Table 1 — Summary of Standards Work in the Healthcare Environment	12	
8.5 Clinician/Supplier Involvement in the Standardization Process	31	Table 2 — Summary of Projects Investigating Security in Healthcare Information Systems	20	
9 Recommendations	32	Table 3 — Summary of Standards Addressing Security	25	
Annex A Healthcare and Security Related Standards	34	Table 4 — Summary of the Most Relevant Security Documents	27	
A.1 CEN/TC251 (Euro)	34	Table 5 — Summary of Standards Addressing Safety	28	
A.2 NHS Executive (UK)	35			
A.3 American Society for Testing and Materials (ASTM) (USA)	36			
A.4 Computer-based Patient Record Institute (CPRI) (USA)	39			
A.5 HL7 Inc (Canada)	40			
A.6 Privacy Commissioner (New Zealand)	40			
A.7 Standards Australia (SA) (Australia)	40			

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 7799-1, *Information Security Management — Code of Practice*.

BS 7799-2, *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.

3 Definitions

accountability	the property that ensures that the actions of an entity can be traced [ISO 7498-2]
authentication	the provision of assurance of the claimed identity of an entity (ISO/IEC 10181-2:1996)
availability	the prevention of the unauthorised withholding of information or resources [ITSEC]
confidentiality	the prevention of the unauthorised disclosure of information [ITSEC]
dependability	the property of a system in which reliance can justifiably be placed on the service that it delivers [3], [4]
integrity	the prevention of the unauthorised modification of information [ITSEC]
safety	the freedom from unacceptable risk of harm (or damage) that may be done to human life (or an environment) by a system. [IEC 61508]. This is further defined in Section 5.1.1
security	the preservation of the confidentiality and integrity of data as well as ensuring the accountability and availability of data. [ENV 12924]. This is further defined in Section 5.1.2
quality	the totality of features and characteristics of a product, process or service that bear on its ability to satisfy its stated or intended needs

4 Acronyms

ALARP — As Low As is Reasonably Practicable.
 AIM — Advanced Informatics in Medicine.
 ASC — Accredited Standards Committee.
 ASTM — American Society for Testing and Materials.
 BSI — British Standards Institution.
 Can — Canada.
 CCTA — Central Computer and Telecommunications Agency.

CEN — Comité Européen de Normalisation.
 CORBA — Common Object Request Broker Architecture.
 CPRI — Computer-based Patient Record Institute.
 CPRS — Computer-based Patient Record System.
 CRAMM — CCTA Risk Analysis and Management Methodology.
 CR — CEN Report.
 D — Germany.
 DC — Draft Copy.
 DERA — Defence Evaluation & Research Agency.
 DHE — Distributed Healthcare Environment.
 EEC — European Economic Community.
 EDIFACT — Electronic Data Interchange For Administration, Commerce and Transport.
 ENV — European Pre-standard.
 EWICS — European Workshop on Industrial Computer Systems.
 Euro — European
 FM-HSP/FR — Framework for Formal Modelling of Healthcare Security Policies.
 GISA — German Information Security Agency.
 HC — Health Care.
 HDLC — High Level Data Link Control.
 HIS — Healthcare Information System.
 HL7 — Health Level 7.
 I — Issued.
 IEC — International Electrotechnical Commission.
 IEEE — Institute of Electrical and Electronic Engineers.
 ICD — Intermittently Connected Devices.
 ICT — Information and Communications Technologies.
 ISHTAR — Implementing Secure Health Telematics Application in Europe
 ISIS — Information Society Initiatives in Standardization.
 ISO — International Organisation for Standards.
 IT — Information Technology.
 ITSEC — Information Technology Security Evaluation Criteria.
 ITSEM — Information Technology Security Evaluation Manual.

MEDSEC — Health Care Security and Privacy in the Information Society.

N — No.

NHS — National Health Service.

NHS IM&T — National Health Service Information Management and Technology.

NR — Not Ready.

NZ — New Zealand.

OII — EC Open Information Interchange.

PES — Programmable Electronic System.

prENV — A European Pre-standard.

PT — Project Team.

RICHE — Réseau d'Information et de Communication Hospitalier Européen.

RTCA — Requirements and Technical Concepts for Aviation.

SA — Standards Australia.

SAFE-ID — Safety Procedures for Identification of Patients and Related Objects.

SEC-COM — Security for Healthcare Communication.

SEC-COM/FR — Framework for Security Protection of Healthcare Communication.

SEC-ICD — Security Requirements for Intermittently Connected Devices.

SECREQ-ICD/FR — Framework for Security Requirements for Intermittently Connected Devices

SEC-ID/CARDS — Secure User Identification for Healthcare Strong Authentication using Microprocessor Cards.

SRS — Safety Related Systems.

SNZ — Standards New Zealand.

Saf. — Safety.

SDO — Standards Developing Organisation.

Sec. — Security.

SEISMED — Secure Environment for Information Systems in Medicine.

SEMRIC — Secure Medical Record Information Communication.

SIREN — Security in Regional Networks.

STEP — Standards Enforcement in Procurement Process.

TC — Technical Committee.

THIS — Trusted Health Information Systems.

TR — Technical Report.

UHID — Universal Healthcare Identifier.

UK — United Kingdom.

USA — United States of America.

WG — Working Group.

Y — Yes.

5 Clarification of issues in HIS's

Due to the increasing use of computer-based systems within the Healthcare sector, information systems are becoming more intimately involved in patient care and Healthcare professionals are becoming more dependant upon their use. For example, information systems are being used to assist in the diagnosis and treatment of patients and to form centralised and distributed databases of patient medical records.

Although, currently, HISs generally only form part of an overall process, any malfunction or vulnerability of these systems can be a threat to patients. Such incidents can result in damage to the health of patients, claims for legal compensation or penalties, and loss of public confidence. This is exemplified by systems used in areas such as drug prescription, radiation treatment, the design of linear accelerator software, and the control of ambulance services [1], [2]. Therefore, while the importance of integrity in HISs is recognised, it is usually the overall system that causes harm rather than the software within the system. Standards that evaluate the whole system involving the software help to reduce risks to patients and to give confidence to purchasers.

This CR reviews standards addressing the complete life cycle of a HIS. It considers the pre-purchasing needs of a customer; the requirements that should be met by a supplier; the maintenance and servicing of systems; and incident reporting mechanisms.

When reviewing the standards regarding HISs, the following issues need to be clarified:

5.1 Definitions of safety, security and dependability

5.1.1 Safety

The notion of safety is usually associated with the prevention of the harm (or damage) that may be done to human life (or an environment) by a system. In the context of safety standards for computer-based systems [IEC 61508; EN 1441; EN 60601-1-4; Medical Devices Directive 93/42/EEC], safety is defined as the freedom from unacceptable risk of harm. In this definition, the terms harm and risk have particular interpretations, and these are:

- i) harm is the physical injury, or the damage to health or property, that may be caused by the system;

ii) risk is the probable rate of occurrence of a hazard causing harm and the degree of severity of the harm. Thus, the concept of risk has two elements:

- a) the frequency with which a hazard occurs, and
- b) the consequences of the hazardous event.

A hazard is understood to be a situation in which there is a potential for human injury.

Thus, the concept of risk forms an integral part of the notion of safety.

The implications of the failure of a safety-related system can vary greatly between applications, and this leads to concepts such as the “level of safety” and the “safety integrity” of a system. IEC 61508 describes these terms as follows:

i) the level of safety of a system is defined as a level of how far safety should be pursued in a given context, assessed to an acceptable level of risk, based on the values of society. In order to achieve an acceptable level of risk, it needs to be determined whether:

- a) the risk is so great that it must be refused altogether; or
- b) the risk is, or has been made, so small as to be insignificant, or
- c) the risk falls between a) and b), and that it has been reduced to the lowest level practicable (bearing in mind the benefits flowing from its acceptance and taking into account the costs of any further reduction).

With respect to c) the ALARP principle requires that any risk must be reduced as far as is reasonably practicable or to a level which is “as low as reasonably practicable”. If a risk falls between the two extremes [i.e. the unacceptable region a) and the broadly acceptable region c)] and the ALARP principle has been applied, then the resulting risk is the tolerable risk for that specific application;

ii) safety integrity denotes the probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a period of time. This definition focuses on the reliability of the safety-related system to perform the safety functions. In determining safety integrity, all causes of failure (both random hardware failures and systematic failures) which lead to an unsafe state must be considered. Some types of failures may be quantified whereas others can depend on factors that cannot be quantified but considered qualitatively. The IEC 61508 defines four types of discrete safety integrity levels, and these specify the safety integrity requirements of the safety functions to be allocated to the safety-related system.

5.1.2 Security

The term security, when applied to information systems, is commonly understood to mean the protection of a system’s assets such as the information and information processing resources. Specifically, security has been defined [ITSEC, ENV 12924, MEDSEC, BS 7799] as the preservation of the confidentiality and integrity of data as well as ensuring the accountability and availability of data. These terms have the follows interpretation:

i) *confidentiality* ensures that information is not made available or disclosed to unauthorized individuals, entities or processes. Thus, the protection of personal medical data is a vital component of medical treatment; in some cases the anonymity of a patient may need to be preserved;

ii) *integrity* denotes that the data has not been altered or destroyed in an unauthorized manner. The subtlety associated with this notion is that unauthorized actions are not only restricted to unauthorized persons but may be performed by authorized users. This situation introduces further difficulties in the health care domain, where professionals are personally responsible and mostly liable for their decisions in favour of a particular action or against it;

iii) *accountability* is concerned with ensuring the actions performed by an entity on a system can be traced uniquely to that entity. This property can be supported by mechanisms such as authentication and non-repudiation of an entity, as well as maintaining audit logs. Authentication is concerned with the verification of the identity of a user, and non-repudiation provide the assurance that a seemingly authentic but possibly forged message cannot subsequently be claimed to be a forgery;

iv) *availability* is concerned with ensuring that data is accessible and useable upon demand by an authorised entity.

Although the notions of confidentiality, integrity, accountability, and availability have been presented separately, they are related. For instance, mechanisms must be implemented in a system that make it possible to provide the correct service to authorised, or trusted, users.

To ensure that a system's assets are adequately protected, and to provide a level of assurance in the operation of a system, risk analysis must be performed. In the context of security, a risk is defined as the aggregate effect of the likelihood of occurrence of a particular threat with the degree of vulnerability to that threat and the potential consequences of the impact to the organisation, if the threat did occur. A threat is defined as an action or event that might prejudice the security of a system. The security assessment of a system includes analysis that considers the assets of a system, the threats that can cause a security breach, the vulnerabilities and weaknesses that results from these threats, and the countermeasures that can be applied to protect the system.

The notions of safety and security may appear to be different, but they are similar in the sense that:

- i) they concerned with freedom from different types of undesirable incidents. Safety is predominantly concerned with preventing the occurrence of harm to human life, and security prevents unauthorised access to information;
- ii) both define a concept of a risk. The risks to a system are either eliminated or made as low as reasonable practicable using the ALARP principle.

In the context of HISs, the notions of safety and security are inter-related and thus an overlap exists. For instance, a scenario can easily arise in which damage to the information in a system could lead to a consequential hazardous situation for patient treatment.

5.1.3 Dependability

When a system is developed to incorporate the notions of both safety and security, the main aim is to ensure that the system becomes more dependable. Hence, the term dependability can be used to describe the type of systems considered in this CR. This term is often used to describe a system in which reliance can justifiably be placed on the service that it delivers to its users. Dependability is considered to be a generic term because it has been defined as comprising the factors of: reliability, safety, maintainability, availability and security [3], [4]. Thus dependability is quantified in terms of various factors that combine to produce a dependable systems. However, the importance of the these factors will vary between applications. Hence, if this term is to be used within the healthcare domain, then an appropriate technical committee should decide on its exact definition.

5.2 Medical Devices versus HIS's

A wide range of information systems exist in the Healthcare sector. A number of these systems are explicitly covered by existing European directives, such as: Active Implantable Medical Devices Directive 90/385/EEC, Medical Devices Directive 93/42/EEC, and the *In-Vitro* Medical Devices Directive.

Most medical devices are covered by the Medical Devices Directive 93/42/EEC. This directive states that it is applicable to: "all devices (including any electronic apparatus such as personal computers and their software) which are used for human beings for the purposes of:

- diagnosis, prevention, monitoring, treatment or alleviation of disease;
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap;
- investigation, replacement or modification of the anatomy or of a physiological process;
- control of conception.

Other types of system include Information Systems that are used in diagnostic support, therapeutic support, and those used to store patient records (such as a patient's medical condition, personal details and diagnosis information). This CR primarily considers the standards that are applicable to the latter type of system which is referred to as a Healthcare Information System.

However, it is regarded as important that there should be a “smooth” transition between the various standards. That is, where a system could be considered as being of one class or another, the decision as to which type it actually is shall not radically alter the controls needed for its development. To this end, this CR will also examine a range of medical/information standards, with a view to assessing their suitability for HISs.

5.3 Procurement Process

In the Healthcare environment, the relationship between the Customer and Supplier of HISs needs to be considered, as well as the process of procuring these systems. The Customer is usually an individual health authority or hospital, who may not have the technical resource or finances necessary to perform procedures such as detailed risk analysis when procuring an information system. Repeated assessment of systems by end customers is inefficient. However, suppliers need to ensure compliance with the relevant standards — this requires either a certification body to assess a system on behalf of the Customer, ensuring that conformance to standards will be assessed after an accident/incident has occurred.

5.4 Risk Assessment

The level of criticality of a HIS needs to be established. In particular, it is necessary to define the criteria for grading the criticality of a system, and to identify the techniques needed to perform system assessment. This work needs to take into consideration the functionality of the system, the system’s environment, and the way in which the system is used.

In the avionics sector, the approach taken is to apply risk assessment techniques to systems that are considered to be potentially safety critical. The task of performing risk assessment determines the level of criticality of the system. Hence, if the system is classified to be critical then rigorous techniques are used for its development. A similar approach should be considered in order to determine the criticality of HISs, and standards such as the IEC 61508, Medical Devices Directive 93/42/EEC and CRAMM provide a useful guide to the classification of systems based on the level of risk. Although rigorous techniques, such as those used in the avionics area, may not be needed for the development of systems in the Healthcare sector, appropriate and specific techniques should be identified.

5.5 Certification of Systems and In Service Feedback

The activity of certification is performed in areas such as military systems and civil avionics systems. Within the context of military systems, the Customer performs the certification on systems, and in civil avionics systems, an external body such as the Civil Aviation Authorities performs the certification of a product.

In the Healthcare sector, as discussed in 3.3, these types of certification activities may not be practical. However, the Customer has a need to be assured that the product is actually safe. Hence, the possibility of some form of a certification mechanism should be considered within the Healthcare sector. Projects such as G7 ENABLE recommend that healthcare systems that can cause harm to an individual should be categorised and brought under the control of regulations. Also frameworks for the certification and regulation of products do exist, and an example of which is provided by the Medical Devices Directive 93/42/EEC.

The notion of providing an incident reporting service when a system is operational is desirable and essential for safety-related systems. This type of service is provided by organisations such as the UK Civil Aviation Authority for the avionics industry and in areas such as the introduction of new medicines (where controlled field trials are performed). Within the healthcare sector, the reporting of unusual events or incidents is mandatory in most organisations. Moreover, documents such as the Medical Devices Directive 93/42/EEC stipulates the setting-up of report back services for medical devices. Hence, a similar reporting service should be considered for HISs; this would allow the failures or comments about an Information System to be registered, compiled into a database and disseminated to other users.

5.6 The Year 2000 (Y2K) Problem

A significant threat to patient safety is expected to arise from the Y2K problem — the fact that many systems use a 2-digit date and may break down when first confronted with a date after the turn of the millennium. According to a recent report, many types of Healthcare equipment such as transfusion pumps used in the UK National Health Service (NHS) will fail; they are set to become inactive if more than six months has passed since they were last serviced, and the date used to measure this is only two digits [5], [6]. This CR does not specifically consider the Y2K problem, or standards related to it, but it recognises this problem in HISs and refers to the following websites for further information;

- i) <http://www.open.gov.uk/hse/year2000.pdf> and

ii) <http://www.rx2000.org/Pubs.html>.

6 Summary of existing and emerging standards/guidelines

This review considers the current and emerging standards and pre-standards, as well as guidelines and projects that are applicable to the Healthcare sector. The approach taken in this review is to consider a broad range of de jure standards, de facto standards and any relevant documents without considering each in depth. The main motivation for adopting this approach was to understand and record the main principles involved in a standard and then to consider how these principles could be applicable to HISs. This review was initiated by identifying the standards organisations and any technical committees that considered the safety or security aspects of HISs, or general computer-based systems.

The meaning of the terms safety and security can change from one domain to another, however, this CR uses CEN's terminology. Specifically, safety denotes freedom from unacceptable risk of harm, and security denotes the control of threats made to the integrity of a system.

The services provided by the Internet, Journals, Healthcare databases and domain experts were used to gather information on relevant Healthcare documents. The criteria for selecting a standard, or document, was based on whether it considered the safety or security aspects of computer-based systems, or HISs. Moreover, each standard was further examined to ascertain whether it:

- i) provided a classification of a system based on its level of risk;
- ii) provided quality procedures for producing the system;
- iii) stipulated any form of risk analysis;
- iv) stipulated any form of certification activity or feedback service;
- v) stipulated any form of incident reporting mechanism.

The review is not intended to be an all inclusive list of all standards and it is inevitable that further standards and projects will be developed and made available following the issue of this report. To address this it is suggested that the author visit the following EC Open Information Interchange (OII) website which provides a useful list of relevant standards;

<http://www2.echo.lu/oii/en/oii-home.html>

In addition, the following CEN/TC 251 website provides a list of useful links to other sites such as the OII (via "Important Links") and a list of CEN/TC 251 documents, reports and standards;

<http://www.centc251.org>

Table 1 provides a summary of the reviewed standards and guidelines, and, where information was available, these documents are discussed in detail in the Annex A of this CR. In Table 1, the standards, and documents, that have been produced within Europe are shown before those that have been produced by non-European countries, because they are deemed to be most applicable in a European context. Also, this table groups the standards into several categories; these categories describe the domain of application of the standard and the issue addressed by the standard. The following shows the order in which these categories appear on Table 1:

- i) Healthcare and Security related standards;
- ii) non-Healthcare and Security related standards;
- iii) Healthcare and Safety related standards;
- iv) non-Healthcare and Safety related standards;
- v) Software quality related standards.

The columns of Table 1 are organised in the following manner:

- i) the title of the standard, or guideline, which includes its reference code;
- ii) the standards developing organisation (SDO) or the organisation responsible for producing the standard or guideline;
- iii) the applicability of the standard to the Healthcare (HC) domain; the options used in this field are: yes ("Y") or no ("N");
- iv) the issue addressed by the standard, i.e. safety ("Saf.") or security ("Sec.");
- v) the status of the standard. This field is labelled as "Status" and has the following options:
 - a) Issued ("I") — this denotes standards that are issued (or guidelines that are published),
 - b) Draft Copy ("DC") — this denotes standards that are available as draft copies (or unpublished guidelines),
 - c) Not Ready ("NR") — this denotes standards (or guidelines) that are under development, or not issued.
- vi) the comments field provides a brief description of the standard/guideline in the form of bullet points. This field is labelled as "Comments".

Table 2 provides a summary of projects that have investigated the security aspects of HISs.

Table 1 — Summary of Standards Work in the Healthcare Environment

Title of Standard/Guideline	SDO	H C	Saf./Sec.	Status	Comments
Medical Informatics: Algorithm and Digital Signature Services in Healthcare (ENV 12388)	CEN/TC 251 (Euro)	Y	Sec.	I	● Defines a digital algorithm for use in European Healthcare. ● Standard is based on the RSA-algorithm. ● See Annex A.1.1
Medical Informatics: Security Categorisation and Protection for Healthcare Information (ENV 12924)	CEN/TC 251 (Euro)	Y	Sec.	I	● Specifies a model and method of categorising automated Healthcare systems based on security. ● A set of protection requirements and recommendations are provided for each category. ● See Annex A.1.2.
Secure User Identification for Healthcare: Identification and Authentication by Passwords- Management and Security (prENV 12251)	CEN/TC 251 (Euro)	Y	Sec.	DC	● Facilitates the secure use of passwords in Healthcare IT systems. ● Strengthens the software procedures associated with the management of user identifiers and passwords. ● See Annex A.1.3.
Health Informatics: Secure User Identification for Healthcare Strong Authentication using Microprocessor Cards [SEC-ID/CARDS (6.4)]	CEN/TC 251 (Euro)	Y	Sec.	NR	● This work is undertaken by PT 37. ● Defines a method for secure user identification by using cryptographic protocols to ensure authentication. ● See Annex A.1.4.
Health informatics: Safety and Security related Software standard for Healthcare [SSQS (6.5)]	CEN/TC 251 (Euro)	Y	Saf./Sec	NR	● This work is undertaken by PT 38.
Health Informatics: Security for Healthcare Communication [SEC-COM (6.10)]	CEN/TC 251 (Euro)	Y	Sec.	NR	● This work is undertaken by PT 39. ● Provides interoperability and implementation standards for the provision of security in Healthcare communication. ● See Annex A.1.5.
Health Informatics: Security Requirements for Intermittently Connected Devices [SEC-ICD (6.12)]	CEN/TC 251 (Euro)	Y	Sec.	NR	● Defines the security requirements of ICDs such as patient cards, which carry important clinical information. ● See Annex A.1.6.

Table 1 — Summary of Standards Work in the Healthcare Environment

Title of Standard/Guideline	SDO	H C	Saf./Sec.	Status	Comments
Health Informatics: Framework for Security Protection of Healthcare Communication [SEC-COM/FR (6.14)]	CEN/TC 251 (Euro)	Y	Sec.	NR	● Defines the framework description of the structures and relations communications and security ● See Annex A.1.7.
Health Informatics: Framework for Security Requirements for Intermittently Connected Devices [SECREQ-ICD/FR (6.15)]	CEN/TC 251 (Euro)	Y	Sec.	NR	● See Annex A.1.8.
Health Informatics: Framework for Formal Modelling of Healthcare Security Policies (FM-HSP/FR)	CEN/TC 251 (Euro)	Y	Sec.	NR	● See Annex A.1.9.
Secure Healthcare Information Systems: A Directory of Information and Communications Technologies (ICT) Security Standards	NHS, (UK)	Y	Sec.	I	● Assesses the status of emerging standardised technologies and methodologies for information and communications system security. ● Summarises the availability of standards for secure ICT. ● See Annex A.2.1.
NHS IM&T Security Manual	NHS, (UK)	Y	Sec.	I	● A range of issues is considered relating to the security of aspects of health information. ● See Annex A.2.2.
Standards Enforcement in Procurement Process (STEP).	NHS (UK)	Y	Sec.	I	● Developed to ensure that IT systems within the NHS conform to IT standards. ● See Annex A.2.3
Report on the Review of Patient Identifiable Information	NHS (UK)	Y	Sec.	I	● Report generated by the Caldicott Committee. ● Report concerns the issues related to Patient-Identifiable information.
Guide for confidentiality, privacy, access & data security principles for health information including computer-based patient records. (E1869)	ASTM/E31.17 (USA)	Y	Sec.	I	● Provides the basic principles for handling confidentiality, access and security of health information. ● See Annex A.3.1.1.
Guide for amendments to health information (PS105)	ASTM/E31.17 (USA)	Y	Sec.	DC	● Provides the basic principles for handling confidentiality, access and security of health information. ● See Annex A.3.1.2.

Table 1 — Summary of Standards Work in the Healthcare Environment

Title of Standard/Guideline	SDO	H C	Saf./Sec.	Status	Comments
Specification for security audit and disclosure logs for use in Health Information Systems. (PS106)	ASTM/E31.17 (USA)	Y	Sec.	DC	● This is a provisional standard. ● Identifies the data to be recorded; the management and use of audit logs. ● See Annex A.3.1.3.
Standard for information access privileges to health information (PS107)	ASTM/E31.17 (USA)	Y	Sec.	DC	● This is a provisional standard. ● Addresses the process of granting and maintaining access privileges to health information. ● See Annex A.3.1.4.
Guide for individual rights regarding health information (PS108)	ASTM/E31.17 (USA)	Y	Sec.	DC	● This is a provisional standard. ● Ensures that legitimate users have access to relevant health information. ● See Annex A.3.1.5.
Guide for the training persons who have access to health information (PS109)	ASTM/E31.17 (USA)	Y	Sec.	DC	● This is a provisional standard. ● Addresses the privacy, confidentiality, and security issues by training persons who have access to health information. ● See Annex A.3.1.6.
Guide for properties of a Universal Healthcare Identifier (UHID) (E1714)	ASTM/E31.20 (USA)	Y	Sec.	I	● Lists the requirements of the person identifier UHID. ● Recommends encryption of identifiers to ensure Confidentiality. ● See Annex A.3.2.1.
Guide for electronic authentication of Healthcare information (E1762)	ASTM/E31.20 (USA)	Y	Sec.	I	● Describes a range of issues concerning the use of electronic signatures. ● Discusses the security requirements for electronic signatures. ● See Annex A.3.2.2.
Specification for authentication of Healthcare information using digital signatures (PS100)	ASTM/E31.20 (USA)	Y	Sec.	DC	● This is a provisional standard. ● Describes the use of digital signatures to provide authentication of Healthcare information. ● See Annex A.3.2.3.
Guidelines for a technical security framework for transmission and storage of Healthcare information (PS101)	ASTM/E31.20 (USA)	Y	Sec.	DC	● This is a provisional standard. ● Presents a framework that describes existing and future standards for the security of Healthcare information. ● See Annex A.3.2.4.