TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN ISO/TS 14441

December 2013

ICS 35.240.80

English Version

Health informatics - Security and privacy requirements of EHR systems for use in conformity assessment (ISO/TS 14441:2013)

Informatique de santé - Sécurité et exigences d'intimité des systèmes de EHR pour l'évaluation de la conformité (ISO/TS 14441:2013)

Medizinische Informatik - Sicherheits- und Datenschutzanforderungen für die Konformitätsprüfung von EGA-Systemen (ISO/TS 14441:2013)

This Technical Specification (CEN/TS) was approved by CEN on 7 April 2013 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN ISO/TS 14441:2013 E

Foreword

This document (CEN ISO/TS 14441:2013) has been prepared by Technical Committee ISO/TC 215 “Health informatics” in collaboration with Technical Committee CEN/TC 251 “Health informatics” the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/TS 14441:2013 has been approved by CEN as CEN ISO/TS 14441:2013 without any modification.

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviations **9**
5 Security and privacy requirements **9**
5.1 General 9
5.2 Theoretical foundation 9
5.3 Privacy and security requirements 12
5.4 Common Criteria 28
6 Best practice and guidance for establishing and maintaining conformity assessment programs **30**
6.1 Concepts 31
6.2 Conformity assessment processes 33
Annex A (informative) **Conformity assessment programs — Design considerations and illustrative examples from member countries as of 2010** **36**
Annex B (informative) **Comparison of jurisdictional requirements** **54**
Bibliography **112**

Introduction

As local, regional and national EHR infostructures develop, electronic patient record systems are being implemented at the many points of care where patients are seen [point-of-service (POS) clinical systems]. In addition to institutional settings like hospitals, where the systems in various departments (e.g. nursing units) are typically integrated into a single patient record, smaller single purpose systems such as electronic medical records (EMRs) are also being implemented in physician offices and other non-institutional settings such as public health where the sophistication of the systems and the local IT support infrastructure is much less. As countries begin to connect these POS clinical systems to EHR infostructures (or directly exchange clinical information with other POS clinical systems through system-to-system communications), the security and privacy of these systems becomes much more critical and complex than when the systems operated in a disconnected or 'stand-alone' state. To ensure the required standards are implemented correctly into these systems, so that they will securely interact with EHR infostructures and maintain the privacy of patient information, many countries are implementing certification and conformance testing programs to provide objective evidence of conformity with these requirements.

This Technical Specification identifies the security and privacy requirements, harvested from the above mentioned standards and international experiences, which should be in place for conformance testing for interoperable POS clinical (electronic patient record) systems interfacing with EHRs.

The POS clinical systems profiled receive, store, process, display and communicate clinical data and administrative actions, as well as information related to system users (demographics, personal).

The systems are always accessed by authorized and authenticated users. These users are:

— health professionals that input, access and use patient data, clinical procedures, and statistics;

— administrative users that input and read patient's personal and demographics data, administrative and statistical information;

— administrators that control users power, perform backups, provide system configuration, including security ones;

— auditors that read audit trails;

— other EHR systems that input and receive data;

— subjects of care and their substitute decision makers, who may have restricted access to input and retrieve authorized data.

Key assumptions that apply for compliant POS clinical systems are as follows:

— the Target of Evaluation (TOE) comprises commercial off the shelf (COTS), governmental, proprietary and free and open source software;

— authenticated users recognize the need for a secure IT environment;

— authenticated users can be trusted to comply with the organization's security policy;

— business security processes are implemented with due regard for what can (and cannot) be reasonably accomplished in a clinical setting;

— competent security administration is carried out in relation to the system's installation and ongoing operations.

This Technical Specification draws from international standards, which have been developed by ISO/TC 215 for EHRs, as well as other ISO standards such as such as ISO/IEC 27001 and the ISO/IEC 17000 series of standards developed by the ISO Committee on conformity assessment (CASCO). This Technical Specification also reflects the experience that various countries have had to date in implementing certification and conformance testing programs in addressing privacy and security requirements in the

context where electronic patient record (clinical) systems at the point of care are interoperable with regional and national EHRs.

This Technical Specification includes:

— security and privacy requirements that should be met to ensure that information is protected as well as the main categories of attack;

— discussion of the theoretical foundations underpinning the requirements;

— guidance on best practice for establishing and maintaining conformity assessment programs;

— description of the conformity assessment process, including the key concepts and processes.

Annex A provides more detailed information on conformity assessment models and processes, plus examples of conformity assessment programs in four example countries at a point in time (2010).

Annex B provides a detailed examination of the privacy and security requirements in place in five jurisdictions at the time that this Technical Specification was written. This analysis was used to derive the security and privacy requirements in Clause 5.

This Technical Specification is to be used by agencies which accredit or operate programs for certifying health software products through conformity assessment against privacy and security standards, software suppliers demonstrating their compliance with those requirements, and purchasers of those systems who want assurance that the requirements have been met.

Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment

1 Scope

This Technical Specification examines electronic patient record systems at the clinical point of care that are also interoperable with EHRs. Hardware and process controls are out of the scope. This Technical Specification addresses their security and privacy protections by providing a set of security and privacy requirements, along with guidelines and best practice for conformity assessment.

ISO/IEC 15408 (all parts) defines "targets of evaluation" for security evaluation of IT products. This Technical Specification includes a cross-mapping of 82 security and privacy requirements against the Common Criteria categories in ISO/IEC 15408 (all parts). The point-of-service (POS) clinical software is typically part of a larger system, for example, running on top of an operating system, so it must work in concert with other components to provide proper security and privacy. While a Protection Profile (PP) includes requirements for component security functions to support system security services, it does not specify protocols or standards for conformity assessment, and does not address privacy requirements.

This Technical Specification focuses on two main topics:

a) Security and privacy requirements (Clause 5). Clause 5 is technical and provides a comprehensive set of 82 requirements necessary to protect (information, patients) against the main categories of risks, addressing the broad scope of security and privacy concerns for point of care, interoperable clinical (electronic patient record) systems. These requirements are suitable for conformity assessment purposes.

b) Best practice and guidance for establishing and maintaining conformity assessment programs (Clause 6). Clause 6 provides an overview of conformity assessment concepts and processes that can be used by governments, local authorities, professional associations, software developers, health informatics societies, patients' representatives and others, to improve conformity with health software security and privacy requirements. Annex A provides complementary information useful to countries in designing conformity assessment programs such as further material on conformity assessment business models, processes and other considerations, along with illustrative examples of conformity assessment activities in four countries.

Policies that apply to a local, regional or national implementation environment, and procedural, administrative or physical (including hardware) aspects of privacy and security management are outside the scope of this Technical Specification. Security management is included in the scope of ISO 27799.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17000, *Conformity assessment — Vocabulary and general principles*

ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.