PD CEN/TS 16850:2015

BSI Standards Publication

Societal and Citizen Security — Guidance for managing security in healthcare facilities

bsi.

...making excellence a habit.™

Document Sharing Hub

National foreword

This Published Document is the UK implementation of CEN/TS 16850:2015.

The UK participation in its preparation was entrusted to Technical Committee BCM/1/-/3, Supply Chain Continuity.

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

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2015.
Published by BSI Standards Limited 2015

ISBN 978 0 580 89284 4

ICS 11.020; 13.310; 91.040.10

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 September 2015.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD CEN/TS 16850:2015

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 16850

September 2015

ICS 13.310; 91.040.10; 11.020

English Version

Societal and Citizen Security - Guidance for managing security in healthcare facilities

Sécurité sociétale du citoyen - Lignes directrices pour gérer la sécurité dans les établissements de santé

Schutz und Sicherheit der Bürger - Leitfaden für das Sicherungsmanagement in Gesundheitseinrichtungen

This Technical Specification (CEN/TS) was approved by CEN on 27 July 2015 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

© 2015 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CEN/TS 16850:2015 E

Documents
Document Sharing Hub

Full document details: PD CEN/TS 16850:2015

Contents

Page

European foreword ... 4
Introduction ... 5
1 Scope ... 6
2 Terms and definitions ... 6
3 General guidance ... 6
3.1 Approach ... 6
3.2 Context of the HCF security management ... 6
3.3 Compliance with national legislation ... 7
3.4 Risk management ... 7
3.5 Leadership ... 8
3.5.1 General ... 8
3.5.2 Organization of roles, responsibilities and authority ... 8
3.6 Establishment of a security management policy ... 9
3.7 Security Management Plan (SMP) ... 9
3.8 Interfacing with other management systems ... 10
4 Operational guidance ... 10
4.1 Organization (General procedures) ... 10
4.1.1 Controlled areas ... 10
4.1.2 Access control ... 10
4.1.3 Secure storage ... 12
4.1.4 Facility restricted access (emergency lockdown) ... 12
4.1.5 Car park and vehicle control ... 13
4.2 People ... 13
4.2.1 Staff ... 13
4.2.2 Visitors ... 18
4.2.3 Patients ... 19
4.3 Facilities and technology (infrastructure and access system) ... 22
4.3.1 Design and construction ... 22
4.3.2 Physical security ... 23
4.3.3 Fences and walls ... 23
4.3.4 Closed circuit TV (CCTV) ... 23
4.3.5 Identity cards ... 24
4.3.6 Technologies and alarm systems ... 24
4.3.7 Control rooms ... 25
4.3.8 Accommodation for patients with protective status or prisoners ... 25
4.3.9 Security signage ... 25
4.3.10 Alternative entries ... 26
4.3.11 Operating (surgery) rooms security ... 26
4.3.12 Emergency unit security ... 26
4.3.13 Burglar and intruder resistant areas ... 27
4.3.14 Personal attack alarms (Panic alarms) ... 28
4.3.15 Cash and other monetary processing systems ... 28
4.4 Security incident response ... 30
4.4.1 General ... 30
4.4.2 Criteria ... 30
4.4.3 Minimizing possibility of recurrence ... 31
4.4.4 Reports and statistics ... 31

AVA Documents
Document Sharing Hub
Full document details: PD CEN/TS 16850:2015

4.4.5 Incident report **31**
4.4.6 Interfacing with first responders and emergency management **31**
4.4.7 Targeted violence **32**
4.5 Plans for special cases **33**
4.5.1 Child abduction **33**
4.5.2 CBRN incident response **33**
4.5.3 Prisoner patients **33**
4.5.4 Offensive weapons and other dangerous equipment **33**
4.5.5 Active shooter **34**
4.5.6 Drug diversion and security of CBRNE substances **35**
4.5.7 Vehicle and aircraft security **36**
4.5.8 Media **36**

5 Performance evaluation **37**
5.1 General **37**
5.2 Management review **37**

6 Exercise and testing **37**

Bibliography **39**

Documents
Document Sharing Hub
Full document details: PD CEN/TS 16850:2015

European foreword

This document (CEN/TS 16850:2015) has been prepared by Technical Committee CEN/TC 391 "Societal and Citizen Security", 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.

Documents
Document Sharing Hub
Full document details: PD CEN/TS 16850:2015

Introduction

Security of healthcare facilities is very important for effective and high quality medical treatment. It is a very wide area and the primary objective of this Technical Specification (TS) is to provide all responsible persons, within healthcare facility, with guidelines on how to manage security.

This is not a management system standard. This TS is giving an opportunity to be more specific in proposed security measures, which leads to better security of healthcare facility staff, patient and other people, who are visiting such a facility. There is also an important fact that this TS is not a closed project and we are expecting further development of this document.

Management of security in healthcare facilities is a dynamic process and this TS proposes guidelines, which help responsible persons have a choice from different techniques for how to improve security.

It is important to emphasize that across the European Union there are several regulatory and legislative limitations for use of security techniques and technologies, so it is important to take these limitations into account. Use of the guidelines may vary based on the health care system in each country of the European Union.

Documents
Document Sharing Hub
Full document details: PD CEN/TS 16850:2015

1 Scope

This Technical Specification provides guidance for managing security in healthcare facilities. It covers the protection of people, critical processes, assets and information against security threats.

This Technical Specification applies to hospitals and places that provide healthcare services, such as - but not limited to - psychiatric clinics, homes for the elderly and institutions for the handicapped. It also applies to self-employed practicing healthcare professionals. It does not apply to occupational health and safety and fire safety.

This Technical Specification is not a management system standard. However it can be applied as part of a management system, such as with EN ISO 9001.

2 Terms and definitions

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

2.1
controlled area
area which has specific controls to restrict access to authorized persons only

2.2
targeted violence
situation where an individual, individuals or group are identified at risk of violence, usually from another specific individual such as in cases involving domestic violence

Note 1 to entry: Often, the perpetrator and target are known to each other prior to an incident.

3 General guidance

3.1 Approach

Security management for a healthcare facility (HCF) should:

— be consistent with other policies;

— be documented, implemented and maintained;

— be visibly endorsed by top management;

— provide a framework which enables the specification of security management objectives and targets;

— be consistent with the organization's risk management;

— be communicated to all employees, patients and other stakeholders; and

— respect the rights of patients and visitors.

3.2 Context of the HCF security management

The HCF should determine internal and external issues that are relevant to its purpose and that affect its ability to achieve the intended level of security within the HCF.

The context should be taken into account when establishing, implementing, maintaining and continually improving the HCF security management (system).

Documents
Document Sharing Hub
Full document details: PD CEN/TS 16850:2015

The HCF should identify and document:

— the HCF's activities, functions, services, products, partnerships, supply chains, resources, relationships with interested parties, and their relationship with security management; and

— links between the HCF security management system design and the HCF's other policies, including its other management strategies and implemented management systems.

3.3 Compliance with national legislation

The HCF should establish and maintain procedure(s) to:

— identify legal, regulatory, and other requirements to which the HCF subscribes related to the HCF security management;

— determine legal restrictions on certain security procedures based on jurisdiction; and

— determine how these requirements apply to its HCF security management.

The HCF should document this information and keep it up to date.

The HCF should ensure that applicable legal, regulatory and other requirements to which the organization subscribes are considered in developing, implementing and maintaining its HCF security management.

NOTE 1 These procedures are in most cases an integral part of management system standards, such as quality management systems, e.g. EN ISO 9001:2008. In this case, the organization should ensure that specific requirements for security-related issues, such as requirements for technologies etc. are included.

NOTE 2 The mission of HCF personnel is to provide healthcare and not law enforcement.

3.4 Risk management

Security management is risk management, therefore the security management system should be aligned with other risk management systems within the HCF. The HCF should establish, implement and maintain a formal and documented risk assessment process for security risk identification, analysis and evaluation, in order to:

— identify operational security risks caused by intentional, unintentional and human threats that have a potential for direct or indirect consequences on the HCF's objectives, tangible and intangible assets, and interested parties (threat, vulnerability, and criticality analysis);

— systematically analyse risk likelihood and consequence, and set risk criteria; and

— systematically evaluate and prioritize security risk controls and measures and their related costs.

The HCF should:

— document and keep this information up to date and secure;

— periodically review whether the risk assessment methods are effective for security risk management;

— re-evaluate risks within the context of changes within the HCF, or made to the HCF's operating environment, procedures, functions, services, partnerships, and supply chains;

— evaluate the direct and indirect benefits and costs of options to manage risk and enhance reliability and security;

AVA Documents
Document Sharing Hub

Full document details: PD CEN/TS 16850:2015

— evaluate the actual effectiveness of security risk management measure options;

— ensure that the prioritized risks and impacts are taken into account in establishing, implementing and operating its HCF security management; and

— evaluate the effectiveness of security risk controls and measures.

NOTE For methods of risk assessment and risk analysis see IEC 31010.

The HCF should establish, implement and maintain a formal and documented communication and consultation process, consistent with operational security, with all stakeholders in the risk assessment process to ensure that:

— security risks are adequately identified and communicated;

— interests of other internal and external interested parties are understood;

— dependencies and linkages with subcontractors, third parties providing outsourcing and those within the supply chain are understood;

— the risk assessment process interfaces well with other management disciplines; and

— risk assessment is being conducted within the appropriate internal and external context and parameters relevant to the HCF and its interested parties.

The risk assessment should identify activities, operations and processes that need to be managed. Outputs should include a prioritized risk register identifying measures to mitigate risk and justification for risk acceptance.

3.5 Leadership

3.5.1 General

Top management should demonstrate leadership and commitment with respect to the HCF security management by:

— making security management one of the responsibilities of one of the members of top management;

— appointing a responsible person for the healthcare security management with leadership and technical competence (see 3.5.2);

— supporting relevant management roles to demonstrate their leadership as it applies to their areas of responsibility (see 3.6);

— ensuring that the resources needed for the HCF security management are available (see 3.6);

— supporting the planning of security measures (see 3.7); and

— directing and supporting persons to contribute to the effectiveness of the HCF security management (see 4.2.1.6 and 4.2.1.8).

3.5.2 Organization of roles, responsibilities and authority

Top management should ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management should ensure that:

Documents
Document Sharing Hub
Full document details: PD CEN/TS 16850:2015

— an administrative person, designated by leadership, is charged with primary responsibility for the security function, e.g. a security manager; and

— provision is made for the professional development of the Security manager.

NOTE Membership in at least one professional security organization and participation in security educational programs is strongly encouraged.

The security manager:

— should have demonstrated competence in security risk management and knowledge of the healthcare industry;

— is involved in the planning and building phases of all new facility construction and renovations;

— possesses policy-making authority, and will be in charge of the reviewing and approval process of the HCF;

— plays a critical leadership role in Healthcare Facilities (HCFs) security management; and

— possesses the authority to immediately and independently address any imminent threat that may result in serious bodily injury, death, or significant loss of property. This authority should include standing authorization to deploy and implement timely interim measures.

3.6 Establishment of a security management policy

A security management policy should clearly state the organization's objectives for, and commitment to, security management, and typically addresses the following:

— the organization's rationale for managing security;

— articulate its objectives related to healthcare facility security;

— links between the organization's objectives and policies and the security management policy;

— accountabilities and responsibilities for managing security;

— the way in which conflicting interests are dealt with;

— commitment to make the necessary resources available to assist those accountable and responsible for managing security;

— the way in which security management performance will be measured and reported; and

— commitment to review and improve the security management policy and framework periodically and in response to an event or change in circumstances.

The security management policy should be communicated appropriately.

3.7 Security Management Plan (SMP)

Organizations should develop a Security Management Plan (SMP), based on their risk assessment. The SMP should include preventive, protective, mitigation, response and recovery measures designed to provide a safe and secure environment.

The plan should be based on the risk assessment and needs of the HCF.

The SMP should include, but not be limited to:

Documents
Document Sharing Hub
Full document details: PD CEN/TS 16850:2015

— a security program mission statement;

— a statement of program authority (e.g. a facility organization chart depicting reporting levels);

— the identification of security sensitive areas;

— an overview of security program duties and activities;

— the documentation system in place (i.e. records & reports);

— a training and exercise program for the security staff and all other staff;

— planned liaison activities with local public safety agencies and other HCFs as appropriate;

— a security organizational chart; and

— a copy of the most recent annual program, evaluation report and plan for improvement.

The SMP should be evaluated periodically, and modified as required. Periodical reviews should be documented.

3.8 Interfacing with other management systems

Top management and the security managers should ensure that:

— the HCF security management system operates conforming to the requirements of other implemented management system standards; and

— the performance of the HCF security management is reported to top management.

The HCF should align the security management with other quality, safety and security management systems, such as Information Security Management System (ISMS).

4 Operational guidance

4.1 Organization (General procedures)

4.1.1 Controlled areas

Based on the risk assessment, certain areas of the HCF are determined to be a controlled areas. A controlled area may be part or all of a burglar or intruder resistant area. A controlled area should have means of:

— denying entry to unauthorized persons;

— identifying authorized persons;

— logging entry and - where required - exit of authorized persons; and

— alerting the appropriate authorities in the event of a forced entry or a door opened too long based on the set down criteria.

4.1.2 Access control

4.1.2.1 General

Access control (entry/exit) - using positive personal identification - is essential for controlled areas. The methods actually available to control the access are as follows:

Documents
Document Sharing Hub
Full document details: PD CEN/TS 16850:2015

— key lockable door using a key management which is strictly controlled by limiting the number of authorized users and the means of duplicating the keys;

— visual recognition of authorized people (suitable for access control to small areas which are always occupied, or areas where entry is supervised by a trusted custodian who knows the occupants of the area well enough to identify them, or is able to do so with the assistance of a security pass or ID card);

— mechanical code locks (suitable for access control of small to medium areas which are sometimes left unoccupied);

— electronic access control systems (suitable for larger areas, including several networked areas, whether occupied or not, or where a reliable and secure audit of entry and exit is required. Passes or identity cards authenticate bona fide authorized persons;

  The highest level of security is provided by biometric recognition systems using personal characteristics such as fingerprint, hand geometry or eye retina for recognition. For effective electronic access control, the quality of locking mechanisms, door closers and other peripheral equipment shall be commensurate with the quality of the recognition system and level of control required.

— specific access control systems such as interlocking doors.

NOTE Cards (e.g. identity cards) need to be clearly legible.

For other open areas, consideration should be given to the installation of entry/exit control measures to ensure that:

— only authorized people have unimpeded entry/exit to the building or area;

— visitors are logged and escorted; and

— valuable or vital assets cannot be removed from the controlled area without proper authority.

4.1.2.2 Level of access control

When designing or implementing access control, the HCF should consider:

— the classification or value of material handled or stored;

— the location, size and layout of the area;

— the number of entry/exit points; and

— the number of staff authorized to have access to the area.

4.1.2.3 Access control requirements

Regardless of the entry/exit control method used, persons should only be given the means for entry/exit if they have:

— a legitimate need for unescorted entry/exit to the area; and

— the appropriate security clearance.

AVA Documents
Document Sharing Hub

Full document details: PD CEN/TS 16850:2015

4.1.2.4 Identity cards - receipt and conditions

The issuing process of identity cards should be documented and persons receiving identity cards should be made aware of the need to:

— wear the identification where required;

— safeguard the identity card;

— report its loss to the issuing responsible person immediately;

— return the identity card on cessation of visits or employment; and

— follow the procedures for its use.

4.1.3 Secure storage

The level of secure storage required to adequately protect classified, sensitive and valuable assets can only be determined following a risk assessment.

The following factors for the risk assessment of storage help to select the appropriate security container or secure room:

— the level of classification of information;

— the value and importance of the property to be stored;

— the location (e.g. within a burglar/intruder resistant area);

— the structure and location of the container/building; and

— the entry/exit control system of this area.

4.1.4 Facility restricted access (emergency lockdown)

Emergency situations may require a HCF to immediately or progressively be “locked down" to mitigate possible harm to patients, staff, and visitors and to protect property. Lockdown situations may result from internal or external events such as a hostage incident, active shooter, infant abduction, forensic patient escape, or a man-made or natural disaster.

Restricting movement of individuals into, throughout and out of the HCF during an emergency can be critical to the safety of patients and staff and to the protection of life-saving supplies, equipment and infrastructure.

A security risk assessment should be undertaken whenever a lockdown policy is developed or reviewed. Situations identified by the risk assessment should be evaluated based upon identified emergency scenarios within the HCFs locality.

Restricted access protocols should consider ‘in place’ physical security measures (electronic access control, traffic barriers, etc.), on-duty staff members (security and HCF staff) and the availability of supplemental staff from external resources.

Restricted access protocols should address the following:

— How to limit access for the entire facility. This may be accomplished in progressive stages and may involve the facility incident command structure;

— The persons authorized to implement the restricted access plan;

— Controlling access to security sensitive areas and high risk departments;

Documents
Document Sharing Hub
Full document details: PD CEN/TS 16850:2015