PD CEN/TS 16850:2015

BSI Standards Publication

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

...making excellence a habit.™

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.

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

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

Ref. No. CEN/TS 16850:2015 E

Contents

Page

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.

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.

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).

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;

- 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:

- 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:

- 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:

- 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.

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;

- The process to identify HCF staff and others (fire, law enforcement, public health) that require access;
- Communication methods for supplemental and on duty personnel;
- Methods for managing internal and external communications;
- Establishing and maintaining perimeters and visitor protocols;
- Obtaining additional security and or law enforcement staff;
- Establishing secure passage routes and shuttle transportation for HCF staff;
- Management of the internal environment during lockdown; and
- Reversing the lockdown and opening areas.

Controlled access plans should be tested and evaluated as part of disaster drills and exercises with other HCFs and other community agencies with patient representatives. The inclusion of patient representatives included in these exercises should be considered.

4.1.5 Car park and vehicle control

A program for the control and space allocation of vehicles should be developed and maintained by the HCF.

Measures for identification of authorized vehicles and access control should be implemented.

EXAMPLES A label, decal or access card system may be used.

Traffic flow and numbers should be investigated and road usage should be optimized with directional movement restrictions, thereby encouraging separate entry and exit points where possible. Car park layout and allocations should always consider the relevance of shift-work on parking.

Parking areas should be regularly patrolled by security, and a security escort should be offered between the workplace and parking areas.

Road use and design shall also make provisions for emergency vehicles and restricted parking spaces should only be allocated for emergency services vehicles or staff on call for emergency procedures.

Where the risk to personnel is high, security measures such as CCTV and out-door security technologies and alarms should be used to improve security and safety. Staff and visitor parking should be separate.

4.2 People

4.2.1 Staff

4.2.1.1 Staff selection & screening

The HCF should have a documented program for pre-employment background screening, which consists of, but is not limited to practice and procedures.

The HCF should uphold legal compliance with law and regulations with regards to screening.

The HCF should appoint the departments/positions who conduct the pre-employment background screening.

The HCF should repeat the background screening periodically.

The HCF should involve at least the following departments:

- human resources;

- security;
- business or process owners and managers; and
- legal departments.

The HCF should appoint a position, which is responsible for the overall pre-employment background screening program.

The HCF should appoint positions and departments for whom pre-employment background screening is mandatory.

The structure of a pre-employment background screening should consist of, but should not be limited to, a standard employment application form. This application form should contain at least:

- current employment;
- residence address history;
- date of birth;
- employment history;
- prior criminal history (in line with national privacy regulations);
- educational history;
- inquiry as to whether applicant has legal right to work in specific country; and
- disclosure and authorization for background screening.

Applications should be reviewed for completeness and if minimum requirements of the position are met.

The HCF should perform job interviews. Job interviews are needed to:

- convey critical information to the applicant in order to discourage inappropriate applicants;
- allow for the transfer of missing information from the applicant to the employer;
- permit an assessment of the candidate.

The HCF should maintain several levels of background screening in accordance to the position and/or department. The HCF should periodically review the screening of persons working on behalf of the organization.

4.2.1.2 Wearing of identity cards

The HCF should consider the benefits of having staff conspicuously wear their identity cards at all times whilst in the area for which the identity card is valid. The benefits include the following:

- positive identification of authorized people;
- raising of security consciousness amongst staff;
- assistance in quickly identifying a person who has illegally entered the area;
- clear identification of visitors (i.e. not wearing an authorized identity card);

- stopping unauthorized people appearing as authorized by the simple removal of a visitor's identity card, or not wearing an identity card at all.

Those who cannot wear identity card because of the requirements of their duties should carry them and be able to produce them on request.

NOTE Identity cards need to be clearly legible.

4.2.1.3 Workplace violence

The HCF is advised to implement a protocol addressing workplace violence prevention and response.

The protocol should be elaborated based on the following components of an effective safety and security program, which also apply to prevent workplace violence:

- management commitment and employee involvement;
- worksite analysis;
- hazard reduction and response;
- training;
- record keeping and program evaluation.

A multidisciplinary team should be appointed to develop and maintain the workplace violence program. The team should have support by the HCF's top management.

Security should have a clearly defined role in assisting in the HCF's workplace violence program. The team should receive orientation and training in evaluating and responding.

The HCF should establish a system such as patient record flags, electronic warnings, chart tags, log books, or verbal census reports that identify patients and clients who may present assaultive or threatening behavioural challenges.

The HCF should establish policies and procedures prohibiting the carrying of firearms and other weapons onto the facility with the exception of authorized law enforcement personnel, weapons carried by the facility's security and others specifically authorized, such as armoured car personnel.

The HCF is encouraged to post warnings at entrances to the facility as to how violence against staff or other patients/visitors will be dealt with.

The HCF should incorporate targeted Violence protocols into its Violence in the Workplace policy or create a separate policy for preventing and responding to targeted violence (including domestic violence).

4.2.1.4 Contracting

Specific security requirements should be taken into account in contract documents, purchase agreements and service contracts.

4.2.1.5 Home health security

HCFs providing home health services will develop a security plan to protect staff travelling into the community to perform their job duties.

HCFs should have a risk assessment process in place, which would allow home health staff to determine appropriate safeguards associated with a community visit. The risk assessment process may include a community crime assessment, previous history of the client and use of a location based threat assessment.

Home health staff should be provided with education and training regarding risk identification and preventive safeguards. Training should include information and guidelines on security awareness, crime prevention and defensive measures. Training records should be maintained.

HCFs should develop a communication process to protect home health staff. This should include proactive check-in and check-out procedures, which would allow staff to make contact during the shift to help ensure their safety. Cell phones, automated check-in procedures or GPS devices may be considered as appropriate to facilitate this process.

Security or other appropriate escorts should be available to home health staff providing services in areas or situations deemed high risk, or as individual situations warrant.

Procedures should be in place for home health staff to follow in the event of a security incident or a situation in which they have a concern for their security.

HCFs should have a process in place how to respond to missed check-ins.

4.2.1.6 Role of security personnel in patient management

The HCF will develop policies and procedures that identify the responsibilities and scope of activities of security personnel in performing patient intervention activities. Patient intervention activities include performing patient watches, holds, restraints and seclusions relative to the medical evaluation or treatment of patients.

Management of patient care from the time of admission to care to the time of discharge is the responsibility of clinical care staff.

When security is involved in patient intervention activities, such intervention will be under the direction and supervision of clinical care staff. Security may take independent action when presented with circumstances involving a clear and present danger of bodily harm or danger to property.

The long-term use of security as observers or in patient watch situations should be avoided unless dedicated security-staffing resources have been allocated for this specific purpose. If other security resources are used, significant efforts should be made to maintain the overall quality of safety on the campus. Placing patients in restraint or seclusion should also include appropriate clinical staff monitoring. If security is used to support this monitoring, the appropriate training should be provided. In general, security should be used to supplement and not replace clinical staff members. The primary role of security should be to assist in situations where help is needed to gain control of the patient.

4.2.1.7 Restraining by staff

Security personnel may be requested to assist medical staff in physically restraining a patient. Under these circumstances, written security procedures and concept should specifically cover the circumstances, authority and procedures as agreed with the HCF top management or management of medical services.

Restraining procedures shall meet the law and regulatory requirements.

In cases where security personnel assists in restraining or the seclusion of a patient within the facility, where physical force and/or restraint devices are required, the following will apply:

— There will be continuous supervision, direction and monitoring of security actions by qualified facility clinical care staff who will be present at all times;

— Restraint devices will be those devices commonly used in the medical care environment which have been approved by the HCF. Handcuffs and similar law enforcement restraint devices will not be used unless such medical restraint devices are not readily available, and there is an immediate and clear danger that the patient may harm himself or others;

NOTE It is recognized that law enforcement restraint devices may not be used in any case in specific jurisdictions. The use of weapons by security is considered as law enforcement use and not a healthcare intervention. The use of a weapon by security to protect people or hospital property from harm would be handled as a criminal activity.

- Security will receive training for their role with established protocols relevant to the patient;
- Watches, holds and restraining patients. Collaborative training with clinical staff should include de-escalation and proper patient restraint techniques, mental health holds, Against Medical Advice (AMA) discharges as well as accreditation and regulatory agencies;
- Security's patient intervention activities should be documented and should include the name of the requested carer, time of request, instructions given, patient name, time, nature, duration of service rendered and the identity of all security involved in providing the support service;
- Any action taken by security personnel such as restraining or use of any weapon shall meet regulatory and legislative requirements, and the HCF should pay special attention to all procedures described above.

4.2.1.8 Training of personnel

The HCF will ensure that any individuals performing security services are trained to meet regulatory or legislatively required standards for security training and standard practices within the healthcare security industry. Security staff are also trained to meet the requirements set by the outcomes of the risk assessment.

HCFs should develop a continual training and education plan, execute this and evaluate it.

This plan should contain, but not be limited to:

- a continuous, cyclic description based on the PDCA-cycle;
- alignment with general security policy and risk assessment;
- the goals of the training and education plan;
- the management sign off;
- the involvement of HR department;
- the staff member responsible for development and execution of the plan;
- the selection of security requirements, competency and skills (in relation to either individual or department needs);
- the evaluation, testing and maintaining skills and knowledge methods;
- a periodic evaluation of the plan.

Training should include a method to verify that the training received resulted in an acceptable level of competency for each person trained.

Training records for each individual should be maintained by the HCF and archived in the file of each individual staff member, in accordance with the HCF Record Retention Policy. Due to different national legislation and standards, each HCF should determine for how long staff records are kept before they are destroyed or deleted according to local law, legislation and/or standards.

Training records should include the subject matter, time, duration of training, instructor's name and affiliation and competency verification.

If a local entity with jurisdiction prescribes mandatory training for contract officers, but not proprietary officers, the HCF should at least provide or demand an equivalent level of training for proprietary officers.

Initial training in critical tasks with demonstrated competency should be provided prior to a security officer's unsupervised assignment.

4.2.1.9 Security Awareness Program (SAP)

The HCF should define the organizational levels for SAP, but not limit it to:

— executive management and middle management;

— first-line supervision;

— individual employees;

— non-employees (patients, visitors).

The HCF should develop an SAP policy, procedures, instructions and a purpose for the SAP.

The SAP should address the following topics, but not limit it to:

— Why the organization requires SAP?

— The added value of SAP to the organization.

— What actions are needed in SAP for specific assets?

— What are the employees' responsibilities?

— How can employees meet those responsibilities?

— How can employees report SAP violations?

— How can employees identify indicators of risk and danger and how they should react?

The HCF may use techniques and resources such as:

— written material;

— audio-visual material;

— formal security briefings;

— integration into line operations inside experts;

— outside experts;

— liaison employees.

The HCF should use techniques which objectively measure the effectiveness of SAP.

4.2.2 Visitors

The HCF should identify restricted areas, where control of entry/exit is necessary for visitor identification. Written instructions regarding visitors should be given to staff.

To be effective, measures for the control of visitors should include a register which is to be signed by all visitors and the representatives authorizing such visits and which will show the following information:

- name of the visitor;
- facility or firm the visitor represents or, in the case of private individuals, their private address;
- name of the person to be visited; and
- date and times of the visitor's arrival and departure.

Numbered identity cards or visitor passes should be issued. At the end of each designated day/period all visitor passes should be checked and action taken to recover or cancel any that are not returned. The HCF staff should have a contingency plan to deal with possible security compromise originating from the misuse of non-returned passes.

This register should be a protected document.

4.2.3 Patients

4.2.3.1 Searching patients and patient area for dangerous items

Search of persons should be performed in accordance with legislation, The HCF should establish procedures to reduce the likelihood of dangerous items entering the HCF. Patients and visitors should be warned about those items which they are not permitted to in. Searches of patients, patient belongings and patient areas should be conducted as needed with patient agreement.

These searches are undertaken to reduce the likelihood of potentially dangerous, illegal, or other items, which may be contrary to the patient's treatment plan from being brought into the HCF.

Dangerous items include, but are not limited to, any type of weapon, illegal or unauthorized drugs, intoxicants, flammable items and sharp edged objects. Other items may be prohibited based on patient needs as determined by medical staff.

A room search and a personal search protocol, which respects the dignity of the patient should be established. The protocol should include:

- When a search is justified;
- Who may initiate a search (usually medical or nursing staff);
- Who conducts the search;
- Which role and responsibility has the local security personnel;
- How a search should be conducted, both of a person and an area;
- Who shall be informed internally;
- How search results are to be documented?
- How seized items are to be handled, safeguarded, and ultimately disposed of, allowing for, as appropriate:
  - destroying and discarding;
  - turning over to law enforcement; or
  - returning the item(s) to the owner or a responsible family member.

These searches and inspections are administrative in nature, and are not law enforcement searches. It is not the intent of this Technical Specification (TS) to provide law enforcement with evidence to criminally prosecute or otherwise act on the basis of items seized during such inspections. Nor is it the intent of this TS to prohibit the turning over of such dangerous items to the appropriate law enforcement. The HCF's search protocol should address who may, and under what circumstances a determination will be made to involve law enforcement.

4.2.3.2 Paediatric security

Paediatric patients present unique security challenges for HCFs. Paediatric patients can present risks of, abduction, parental custody issues, being physically assaulted, wandering off, elopement and other issues. The older paediatric patient may even introduce issues involving contraband, gang related activity and other problematic behaviours.

HCFs should implement protective measures (a program) that identifies and minimizes the risks and vulnerabilities of its paediatric patient population. Proactive steps and available HCF resources should be documented in a format that paediatric staff can readily access when they have questions on paediatric security practices. The program should:

— be based on identified risks at the HCF as well as current professional literature on infant/child abduction;

— include policies, procedures and protocols to deter infant/child abduction and to respond to suspected or actual abduction for both non-family and family related abduction incidents;

— include training of multidisciplinary healthcare staff in both deterring and responding to abductions;

— include applicable education of parents/guardians in their role of safeguarding their infant/child. Parental education should be conducted initially upon admission and include periodic refreshers throughout the duration of the infants/child's stay in the HCF or during home visits; and

— include the use of physical and electronic security measures, such as access control, based on the HCF's ongoing risk assessment.

HCFs should establish security related procedures for the intake of paediatric patients to include assessing patient history for problematic behaviours and victimization, the need for visitor control; probing for current and past restraining orders and identifying issues related to possible child abuse, custodial disputes, gang involvement, elopement concerns and contraband possession.

Admissions and Triage staff should be trained in probing for issues relative to paediatric safety and security. Inpatient clinical staff working with paediatric patients should receive similar training, as well as instruction in the indicators of when a family, visitor, staff member or another may be involved in abuse or neglect of the patient. Procedures in legally-required reporting suspicions of the same should be developed and included in this training.

Custodial parents and guardians should receive guidance, both verbally and in writing, regarding their vital role in providing safety and security for their paediatric patient.

Paediatric patient visitation privileges should be set out in a written policy and procedure that provides for a controlled and welcoming environment.

Authorized visitors should be readily identifiable. Consideration should be given to identifying persons who are authorized for 'after-hour' or 'over-night' visitations.

Timely campus-wide communication procedures should be established which include the use of distinct emergency codes and procedures to respond to paediatric abductions and elopements.

Inpatient areas providing paediatric care, including the Paediatric Care Unit (PEDS), Neonatal Intensive Care Unit (NICU), Paediatric Intensive Care Unit (PICU), Adolescent Psychiatric Unit (APU), and any adult unit which may be used from time to time for paediatric care, should be evaluated against the special risks associated with the paediatric patient.

4.2.3.3 Wandering patients search

The HCF should establish protocols and security orders for dealing with wandering or missing patients. Departments and wards should first establish that the patient is not in the immediate area. Security should be notified immediately if the patient is not found, and proceed with well-rehearsed plans for locating the patient.

Law enforcement should be notified as soon as it is suspected that the patient is not within the HCF.

4.2.3.4 Patients with protective status

In developing the protective security measures, the HCF should consider and, where necessary, include plans for security arrangements required for patients with protective status. These patients may include VIPs, victims of crime or potential victims of crime.

The measures should also include procedures to protect visitors and staff of such patients. When dealing with a patient under protective status following actions should be taken to ensure:

— a coordinated involvement of key HCF personnel responsible for security;

— the implementation of an organized security plan to protect the patient, which may involve various levels of protection and an effective contingency plan involving additional services such as the police; and

— proof of identification of visitors.

The HCF should consider special security measures for prisoners, to protect other persons inside the HCF. Such measures may include, but are not limited to:

— special entry points for the prisoner and its escort;

— security measures to protect corridors along which prisoners are escorted;

— securing of all equipment, which could be used as a weapon or tool for escape for the prisoner;

— denial of access to other patients, staff and visitors, who are not directly involved in healthcare of the prisoner, to rooms or corridors where the prisoner is escorted;

— implementation of special security measures when weapons are used by law enforcement to escort the prisoner.

4.2.3.5 Patient property security

The loss of property can put such stress on patients that it affects their recovery. It is not only the loss of valuable items and currency which causes stress, but also the loss of spectacles, slippers, dentures, books, hearing aids.

A first step should be to persuade patients not to bring with them items that are valuable or attractive to thieves.

It is important to ensure that the handing over of currency and valuables is witnessed and strictly accounted for with appropriate documentation.

Procedures should be set out in detail in staff training programs. They should include the following:

— staff responsibilities;

— recording procedures for all property handed over to staff;

— disclaimers for use when patients refuse to hand over valuables for safe keeping;

— procedures for use when patients leave wards for treatment, X- rays or operations;

— procedures for use when patients are unconscious, confused or under the influence of drugs or alcohol;

— procedures for the removal, safe custody and disposal of offensive or illegal items, including checks that staff themselves do not retain or remove such items;

— procedures for use in accident and emergency unit and on patient transfer to other departments;

— procedures for use when patients die, are discharged or wish to have their property disposed of differently; and

— particularly valuable items or large amounts of currency should be transferred immediately to a suitable safe, or the currency banked and a trust account receipt issued.

The transfer of responsibility for valuables from one organization or location to another should be recorded.

Signs should be prominently displayed in buildings and grounds disclaiming liability for loss or damage to property, although this will not necessarily protect the organization in the event of negligence by staff.

4.3 Facilities and technology (infrastructure and access system)

4.3.1 Design and construction

Security technologies and alarm systems for new buildings and reconstruction projects should be considered as early as possible, preferably during the concept and design stage.

The HCF should complete a security risk assessment prior to design and construction.

Cabling for security technologies and alarm systems often requires access conduit through floors and walls which are fire rated accordingly. Installers shall ensure that the installation of the cabling meets all applicable installation and design standards or legal requirements.

NOTE The location and proximity of some departments such as emergency units may warrant special consideration in the furniture design and access/exit requirements. Placement of windows, doors, furniture and fittings can influence the level of security within a healthcare facility. Grounds design and vegetation can impact on both personal and property security.

The HCF should consider use of security technologies and alarm systems in which classified information, drugs, CBRN materials, currency, vital and attractive property are stored or handled, so that these areas are given appropriate protection.

The HCF should consider that the design stage includes:

— floor loadings for security equipment and containers;

— space for secure storage;

— space for security personnel;

— special features for staff protection such as heavy barriers ;

— needs for security technologies and alarm systems including mechanical security systems;

— secure storage facilities;

— location and design of parking areas; and

- specific needs of specialized departments of HCF such as emergency units, surgery rooms etc. for quick access.

The HCF should identify the preferred locations for burglar and intruder resistant areas, as well as perimeter protection, security technology and structural requirements.

The HCF should carefully evaluate the alternatives and determine things such as:

- cost-effectiveness;
- user-friendliness;
- effect on the general administration of the facility; and
- risk analysis outputs.

The HCF occupies buildings and areas that house people, classified information, or vital or attractive property. The HCF shall take into account buildings or areas, and provide a level of protection appropriate to the local risk. This provision is necessary for all periods within and outside of working hours.

4.3.2 Physical security

Physical security includes the measures taken to protect patients, staff, and the infrastructure from intentional human threats, and to prevent unauthorized disclosure or loss of information and loss of or damage to assets. Such measures include the control of the movement of people, and the use of physical measures and monitoring arrangements to control security risks.

The organization shall establish, implement, maintain, monitor and document such measures in order to continually improve them. These measures shall be consistent with respect to human rights (typically privacy of personal information).

Such measures should include the following:

- physical barriers designed to deter and minimize the possibility, or show evidence of unauthorized entry/exit;
- entry/exit control measures designed to minimize the possibility of unauthorized access;
- monitoring systems designed to detect unauthorized entry/exit or other emergency situations;
- adequate responses to deal with security incidents.

The HCF should take into account security measures and equipment (typically electronic systems connections, police cooperation etc.) provided by governmental or municipal authorities.

4.3.3 Fences and walls

If they are properly designed and installed, fences and walls, provide a physical barrier around an area or entire HCF. To provide the maximum benefit they may need to be used in conjunction with other measures such as lighting and CCTV. This benefit can be achieved by the protection-in-depth principle.

Reliability of fences and walls should be determined by risk assessment and risk analysis.

4.3.4 Closed circuit TV (CCTV)

CCTV systems may be used to provide surveillance of entrances, passages and other areas. They may be used in conjunction with a security alarm system to assist organization in assessing activation of the system, or with an access control system to facilitate personal identification for remote entry/exit control. For the safety of personnel and for maximum effectiveness CCTV systems should be monitored by a competent person able to respond to incident or report the incident to a responsible person for response.

All CCTV systems, especially video recording, shall meet all legal obligations and regulations.

The information stating that CCTV is in use should be visibly posted.

4.3.5 Identity cards

Where control by recognition is not feasible, identity cards should be used. These cards should be used as an aid to staff to identify and verify authority to enter. They may include the necessary features to allow operation of automated electronic access control systems.

The identity cards should bear the following information:

- the serial number;
- a photograph and description of the holder;
- the signatures of the holder and the issuer;
- conditions of issue;
- instructions to finder in case of loss; and
- the expiry date.

The identity card may be colour-coded to assist in identifying the user or the areas to which the holder has access.

All identity cards have the potential to become compromised. The identity card should be tamper and forgery resistant to allow for the identification of compromised identity cards.

4.3.6 Technologies and alarm systems

The HCF should ensure that all applied security technologies are designed and used with respect to:

- the legal and normative requirements;
- privacy of patients, visitors and staff;
- information security of all information related to security technologies and alarm systems;
- identified risks and threats; and
- the healthcare procedures and processes (non-security).

The following aspects should be considered during the planning and installation of security technologies. The solutions should be:

- easy to operate and should clearly indicate their status in all protected sectors;
- protected against tampering;
- highly resistant to nuisance and false alarms;
- periodically tested.

Maintenance procedures should be such that they ensure the system is reliable and continually operational.

NOTE Installation, testing and maintenance is often regulated by national legislation, e.g. for fire alarm systems.

Mimic panels should be used with caution as they can be set to intercept panic alarms preventing them being responded to by an effective security patrol or law enforcement. This can be critical if the entire facility is under threat. Accordingly, mimic panels should time out and call an outside agency if the alarm is not acknowledged within a prescribed period (e.g. a few minutes).

4.3.7 Control rooms

Where staff are required to undertake security control activities such as monitoring CCTV images or managing a radio network, their operational needs shall be addressed. This will include the setting aside of suitable spaces, environmental design and systems specification considerations. Whilst the recommendations which follow related primarily to purpose-designed control rooms, many of the considerations will also be applicable to other areas where security control is exercised, such as reception areas.

Space provision should be based on the ergonomic arrangement of workstations so that monitor screens can be easily viewed, and primary equipment is within easy reach. The needs of temporary visitors during incidents should be considered, which may include the provision of temporary seating or work surfaces. Circulation routes and access for maintenance need also to be considered when suitable space is set aside for a control room. Additionally, floor-to-ceiling heights are an important consideration when wall mounted overview displays are likely to be used or display screens suspended from ceilings. There may also be minimum height restrictions for ergonomically suitable lighting schemes to be achieved.

A key feature of many security control environments is 24 hour operation which impacts on the environmental specification of the rooms.

EXAMPLE The design of the heating and ventilation system should consider the diurnal rhythms of the operators and compensate for the natural drop in body temperature in the early hours of the morning.

The environment should be designed to take account of the visual demands placed on the operators. Natural and artificial lighting should be such that strong contrasts are avoided and reflections on screens minimized. Where voice communication is likely to take place - whether by radio, telephone or direct - the acoustic environment should be such as to minimize interference with this activity.

The limitations of the human operator, and the tasks they are expected to undertake, should inform the specification and selection of the equipment to be used in the control room. It is recommended that specialist guidance is sought on the optimum ways of structuring and presenting information, including CCTV images and the general design and layout of points of control (ISO 11064).

4.3.8 Accommodation for patients with protective status or prisoners

The HCF may designate a room(s) for patients with protective status. Preparing such accommodation may require a special risk analysis and assessment in order to find the right design, furniture and fittings.

The HCF should consider for security measures if law enforcement should be available within the room(s). The external appearance of the room(s) should where possible not draw attention to the importance of the patient within or to the security measures.

4.3.9 Security signage

Areas maintaining access control or imposed restricted access should be signposted accordingly. The sign should indicate a partially open door and a person at the opening.

4.3.10 Alternative entries

Where entry/exit is controlled, it is essential that other potential entry/exit points (e.g. back doors, windows, fire escapes, ceiling space and under-floor areas) are properly secured. It may be necessary for intrusion detection devices to be fitted at such points.

4.3.11 Operating (surgery) rooms security

Special consideration should be given to the security of the operating suite, particularly during quiet periods when staff attendance is low or non-existent. Operating rooms require open access to stores and supplies (including drugs) and it is often not possible to lock away and secure these supplies. Access control measures and the supervision of non-operating room staff will assist in reducing the opportunity for theft.

The access control measures should be considered during the design stage if possible.

The security of the operating suite should be supported by suitable measures and procedures including after-hours access and the supervision of contractors. A sound protective security program including a security risk assessment should be conducted.

4.3.12 Emergency unit security

HCFs with an emergency unit should conduct a security risk assessment with respect to determining the security risks, and apply the necessary security measures which will mitigate identified risks.

The security of the emergency unit area should be supported by suitable measures and procedures to provide guidance to emergency unit staff and the protective security employees, in order to effectively deal with security incidents.

The emergency unit is not independent from the rest of the healthcare facility. However, the number of patients, type of patients, visitors, the risk environment in which the facility is located and the emergency unit design will affect the security situation (volume, types of patients treated, probability of incidents and community demographics).

The security administrator should be involved in the planning and building phases of emergency department construction and renovation as a resource relative to the following security design issues:

- Access control — ambulatory and ambulance entrances should be separate, with automatically-operated locks. Waiting areas and treatment areas should be suitably separated and movement through/access to them controlled. There should be a concept limiting the number of people accompanying a patient. There should be restricted access from emergency unit to the rest of the HCF.

- The design of the emergency unit — the design of the emergency unit, including waiting and the reception/nurses' station, will have a considerable impact on security. Counters should be constructed to reduce the probability of being jumped over or reached over to grab or strike staff. The reception area should have an unobstructed view of the entire waiting area.

- Panic alarms — the need for a panic alarm system or a static protective security staff member should be based on the security risk assessment.

- The emergency department waiting area should be separated from the emergency department treatment area and be self-contained, but include independent access to restrooms, telephones and vending machines.

- Access controls should be in place to control and limit access of emergency department visitors into the Emergency Department (ED) treatment area and into the main hospital.

- A quiet room should be available adjacent to the waiting room to provide security or emergency unit staff with an area to calm down concerned or anxious persons without disturbing others, and to provide an interview room for law enforcement if required. This may go together with the following room.
- A room or area within the emergency department, separate from other patients, should be available for the treatment of behavioural/mental health or other high risk patients. Considerations for this room should include visibility by staff and the removal or securing of items that could be used by the patient to injure themselves or others,
- The ambulance entrance should be separate from the walk-in entrance and waiting room.

Organizational means may be the following:

- Security staff provides support services in the care and control of ED. These services are to be provided at the request and under the direction and supervision of clinical staff unless circumstances require immediate action to prevent injury or destruction of property.
- Security equipment and systems to protect staff and patients should be in place. These may include electronic access control, video surveillance and duress alarms. The emergency department should be capable of a rapid lockdown down in event of an emergency. Drills should be conducted to exercise the lockdown process.
- Physical measures and/or procedures should be in place to deter the elopement or removal of patients at risk of harming themselves, others or of being harmed themselves.
- Emergency department staff (including security) should receive on-going training in workplace violence, aggressive/violent patient management to recognize, avoid, diffuse and respond to potentially violent situations. This training should include the management of aggressive behaviour and anxiety.
- Some larger HCFs may identify a need to position uniformed security staff in the emergency unit area. Emergency unit security measures should include visitor control, patient restraint and security assistance to staff.
- Periodic meetings (at a minimum annually), with multidisciplinary staff should be conducted to review security protocols and resolve security issues within the emergency care setting.
- Policies, procedures and training programs should be established for security’s role in managing high-risk patients including patient watches, holds, searches and application of patient restraints.

4.3.13 Burglar and intruder resistant areas

Burglar and intruder resistant areas are in general used to protect people, classified information, and vital or attractive property.

These areas, which may be a single room, building, or a complex consisting of a number of buildings, are areas with security measures in place for the secure handling and storage of classified matter and valuable/vital assets.

Burglar resistant areas are those which are secured in a manner suitable for the handling of currency, patients' valuables, drugs, CBRN materials and other vital/valuable assets. The physical security features of a burglar resistant area should include the following:

- Tamper-evident barriers - highly resistant unsecured openings to unauthorized entry/exit,

- A security alarm system with a reliable response providing after-hours coverage communications link to an effective of all areas where classified and vital/valuable assets are handled or stored.

Intruder resistant areas are those which are secured in a manner suitable for the handling and storage of assets of value to the healthcare facility and hazardous materials. An intruder resistant area should include tamper evident barriers, resistant to unauthorized entry/exit, with no unsecured openings.

4.3.14 Personal attack alarms (Panic alarms)

Alarms may be necessary for the personal security of those people who may, because of their duties, be subjected to violent acts. However, critical to the effectiveness of any duress alarm is a speedy, reliable and competent response.

HCFs should have a plan for an overall alarm system which uses unique, clearly distinguishable signals for different situations.

The nature of the response to panic alarm activation should be determined locally. Whoever responds should be quickly on the scene, and capable of assessing the situation they may be confronted with (e.g. an assault) in a competent manner. They should be able to do this discreetly so as not to further panic the person threatening violence and to determine whether they have the ability to deal with the incident, or whether to seek back-up. There is little to be gained by the response personnel becoming unwitting victims.

Employees should be trained in how, when and when not to activate panic alarms and should be informed about the nature of the response they can expect to such an activation. The design and position of alarms is also critical. In most cases they should be out of sight, yet easily able to be activated discreetly so as not to panic the person threatening to cause harm. The alarm itself should be discreet but be able to alert other staff that a problem exists, without panicking the person threatening violence. There is little use in having the alarm monitored at a remote location unless there is a means of communicating quickly with an appropriate response such as a mobile security patrol or the local police.

Where several panic alarm points are installed or mobile panic transmitters are used, it is imperative to the successful operation of the system that there be a means of quickly communicating the precise location of the alarm to the response agency.

Panic alarms shall be tested at regular intervals to ensure that they operate effectively and that the response persons perform as required.

Alarm switches should be designed to minimize unintentional (or false intentional) activation of the alarm system.

Where a fault exists with the panic alarm system servicing, the organization should immediately put into place measures which are consistent with the function of the panic system and ensure rectification of the fault.

4.3.15 Cash and other monetary processing systems

The HCF should establish cash, check/cheque and card processing systems designed to reduce the likelihood of loss or fraud, identity theft, and to enhance the safety of staff involved in accepting monetary transactions. Management of receipts should be based upon a cost benefit and risk analysis.

The design, audit and maintenance of the collection and accounting system should be the responsibility of the HCF’s Internal Auditor, in consultation with the HCF’s designated security representative.

One primary collection point [i.e. a ‘Main Cashier’s Office’] should be established to receive, account for and process all funds received by secondary collection points.

Secondary collection points [for patient co-pays, garage receipts, pharmacy payments, gift shop monies, food area receipts, employee replacement ID payments etc.] should be as limited in number as practicable.

The amount of cash kept anywhere on the HCF's premises should be kept to a minimum.

All collection points and Automated Teller Machines (ATM) should be indoors, in high visibility areas.

Collection points and ATMs should be equipped with duress alarms and recorded video surveillance.

The HCF should establish written collection and reconciliation procedures and a records retention policy for cash collection that is followed by all collection points.

Receipt of all funds should be recorded immediately via:

- on-line electronic processing;
- on-line cash register which displays the amount charged; or
- contemporaneously maintained HCF designed 'Cash and Cheque Log'.

A 'For-Deposit-Only' stamp should be used to immediately endorse each cheque. All cheques should be made in the name of the HCF.

To discourage fraud, a separation of duties is encouraged amongst the collecting, depositing, reconciling, and reporting functions within each collection area.

HCF procedures should prohibit departments from receiving external funds directly and depositing funds into any bank account except the HCF's.

Each time a different person assumes control over a cash/ check draw, a count and reconciliation should be completed.

Secondary collection points should be scheduled to deposit their receipts and processing forms into central collection office, according to the risks associated with the amount of monies involved. If a deposit is not immediately reconciled by the central collection office, a locked bag system should be used and a receipt obtained.

If daily deposits are not required, then fund and related reconciliation documents should be secured separately.

A secure 'drop-safe', requiring dual person access, should be considered for deposits made when the central collection office is closed. Locked bags should be used. 'Drop-safes' should be in an area monitored by recorded video surveillance with consideration for entry recording and audit capability.

Staff receiving funds should receive training in the HCF's collection handling systems. Training should include:

- documentation and reconciliation requirements;
- counterfeit identification;
- protection of personal information;
- reporting of suspected fraudulent activity; and
- response to an attempted robbery.

Reconciliation of all receipts should be completed at least daily at all collection points.

Discrepancies should be immediately reported. A system for determining the need for further investigative follow-up should be established that is based on discrepancy amounts and patterns.

All collection points should retain a copy of their own collection and reconciliation documents.

The physical transfer or transportation of cash or receipts should be conducted using risk appropriate protection measures and include consideration for bonded and insured armored car service.

4.4 Security incident response

4.4.1 General

The HCF will develop procedures for responding to internal security incidents.

Internal security incidents generally refer to manmade incidents (intentional) vs. natural occurrences. Procedures may include initial response to, and the securing of, an incident scene, providing necessary assistance, law enforcement contacts, appropriate investigation and documentation. The procedure should be as follows:

- Proceed quickly and safely to the scene. Observe people or vehicles leaving the vicinity. Upon arrival identify key staff and obtain additional available information.
- Quickly and carefully assess the scene, gathering facts about who, what, when, where and how. Evaluate the nature and extent of the problem to determine an initial course of action. Utilize personal protection equipment (PPE) if warranted.
- Alert other parties or agencies which may include other security officers, security supervisor, hospital supervisor/administrator, police/fire department, and those potentially affected by the incident.
- Secure the scene to mitigate further damage or injury and to preserve evidence.
- Direct security related actions at the scene by exhibiting leadership to mitigate damage and injuries. Transfer leadership once designated authorities or administrative staff have arrived.
- Take notes and obtain verbal/written statements which may be used in preparing the security incident report. Complete required documentation and provide information to assist authorities.

4.4.2 Criteria

A security incident is deemed to have occurred when there is:

- actual harm to a person within a healthcare facility or its grounds;
- a threat to harm or frighten a person within a healthcare facility or its grounds;
- loss of or damage to valuable, vital or hazardous property owned or in the possession of the organization, or belonging to any person to whom it owes a duty of care; or
- loss, compromise or misuse of sensitive or vital information.

When a security incident has occurred, the main objectives of the investigation are as follows:

- establish exactly what happened, and why, how and when it happened;
- assess the degree of compromise, damage or harm;
- recommend measures to contain the problem; and
- make recommendations to minimize the possibility of a recurrence.

The most important step is immediate investigation. Therefore, it should be impressed on all employees and others that they shall report any incident or suspected incident.

Responsibility for the immediate preliminary investigation should be placed on a particular individual who would normally be responsible of the organization security.

An incident should not be considered in isolation. It may be possible to draw conclusions from an examination of all the incidents which have occurred over a period of time. Details of all incidents and the inquiries into them should be maintained within the organization.

Security incidents and their evidence should be used for security risk assessment and analysis.

4.4.3 Minimizing possibility of recurrence

Each incident should provide data for the future.

An incident could reveal where the security arrangements of an HCF are deficient, or point to a failure by an individual (e.g. staff carelessness. Conclusions drawn may have wider implications beyond the particular facility and, if necessary, should be taken up with other relevant facilities.

Whatever the circumstances, no incident should be allowed to pass without its impact being made known to those responsible.

The HCF should also consider recording incidents on offenders' individual personal files. There may be a need to review the suitability of persistent offenders to continue their employment.

4.4.4 Reports and statistics

Investigations into security incidents provide a valuable insight into whether the protective security arrangements are proving effective. Investigations are also useful in the risk management process.

The HCF should compile and maintain incident reports, occurrence logs, shift reports and any other documentation relevant to the performance.

Reports provide a medium for translating data and information into statistics as well as providing relevant information to other stakeholders in a timely and orderly manner.

4.4.5 Incident report

Considerations should be given to the requirements of both the HCF and external services, such as the law enforcement, in compiling the information to be included in this report.

Incident reports should include type of incident(s), time of incident, location of incident, description of offender and victim (if any), i.e. patient, staff or others, and allow for the inclusion of written narrative of the incident, including outcomes.

4.4.6 Interfacing with first responders and emergency management

Based on the risk assessment the HCF should develop and maintain plans for interfacing with first responders and emergency management to address threats, hazards and emergencies that may impact the facility and its operations.

A multidisciplinary team should be appointed to develop, maintain and approve the emergency management program. The team should have express support of the facility's CEO along with authority for the program.

Security should have a clearly defined role in the HCF's emergency management program. The emergency management program should be based on the four phases of mitigation, preparedness, response and recovery. The recovery phase should take into account that security is addressed within the business continuity approach of the HCF.

The facility should conduct a comprehensive risk assessment to identify and prioritize events that may impact facility operations. Risk assessments should be reviewed periodically and whenever conditions change.

Multidisciplinary emergency response plans should be developed to address the potential threats identified by the HCF.

Emergency response plans should have an all-hazards Incident Command System (ICS).

Emergency response plans should address not only immediate and short term response by the HCF but the possibility of emergency operations lasting for days, weeks or even longer.

HCF staff should receive education and training in emergency management consistent with their most likely role in responding to the event, which should be followed up with relevant corrective action.

Emergency response plans should be exercised both for training purposes – so staff understands their roles and responsibilities and feel comfortable in those roles – and to identify and document the plans' strengths, weaknesses and areas for improvement.

Emergency plans should include community involvement – other HCFs, emergency responders and government agencies.

Emergency plans should include provision for the care and wellbeing of HCF staff and their families.

Emergency plans should include also plans for CBRNE incidents as described in 4.5.2.

4.4.7 Targeted violence

HCFs will provide a response to manage targeted violence.

The three major functions of a threat assessment are:

- identification of the perpetrator(s);
- assessment of the risks of violence posed by a given perpetrator at any given time; and
- management of both the subject and the risks that he or she presents to a given target.

The level of threat will determine the scope and timing of the response.

The HCF policy should identify responsibility of staff to report a risk of targeted violence as quickly as possible so the threat can be assessed and preventative measures can be initiated.

Mechanisms should be in place to require reporting of threats where personal safety may be at risk.

All identified threats of targeted violence should be treated seriously and assessed through a process that analyses the threat and recommends the appropriate level or type of intervention to be initiated.

Security should play a lead role in the threat assessment process and design of any safety plan. HCF staff involved in the process of assessing the threat to determine the appropriate level and type of intervention required should receive training for this role.

Where warranted by risk in specific circumstances, HCFs should employ preventative measures to protect the potential target. Measures should include:

- Placing a no information/privacy block on the patient information system or, if an employee, protecting information related to work location;
- Communication with security to provide updated information;
- Information to be shared with workers or other individuals in the area as appropriate;
- Involvement of staff or family members for support as necessary;
- Consideration of moving the person at risk to another care area or another site;
- Consideration for work and parking space and transportation alternatives;
- Restriction on visitors or access to the potential target, including lockdown of the area if required;
- In appropriate circumstances notification of law enforcement; and

- Documentation of risk and preventative measures initiated.

The safety of the potential victim should be of paramount concern at all times.

4.5 Plans for special cases

4.5.1 Child abduction

The HCF providing medical services for infants and children should develop procedures to respond to an abduction incident.

The use of a standard code to institute a response to an infant/child abduction, or suspected abduction, is encouraged.

Abduction drills should be conducted to exercise the HCF abduction response plan.

Consideration should be given to conducting the exercise in all areas housing infants or pediatric patients.

4.5.2 CBRN incident response

The HCF should have a response plan for incidents with chemical, biological, radioactive and/or nuclear substances. The plan should enclose:

- legal responsibilities;
- decontamination infrastructure;
- alignment with overall HCF response plans;
- personal protective equipment such as: Radiation Detection Equipment, Suits, hand protection and/or respiratory protection;
- role, tasks and responsibilities of (security) staff;
- communication (equipment);
- incident training/education, preparation and response;
- post incident;
- triage system;
- patient care by security staff;
- dealing with media, bystanders, and families of victims; and
- escorting of media, bystanders, families, etc. to their own designated collection point.

4.5.3 Prisoner patients

Prisoner patients presented by prisoner staff should be restrained by the prison-supplied devices, which may include handcuffs, shackles, manacles or similar devices.

The HCF should develop a plan for situation, when prisoner and prisoner staff (such as law enforcement) are present in the HCF (for example prisoner is escorted for medical treatment) to prevent any security incident which may put in a risk all other staff, patients or visitors.

4.5.4 Offensive weapons and other dangerous equipment

The HCF should establish a security measures for the control of weapons or other dangerous items or goods coming into the healthcare facility (see 4.2.3.1 and 4.2.3.4).

EXAMPLES Security, and other equipment carried by law enforcement, emergency services, corrective services, payroll contractors and military personnel, visitors or patients, all of whom may legally carry weapons.

4.5.5 Active shooter

Workplace violence is a serious threat for all healthcare facilities and requires proactive steps to be taken to prevent and mitigate risks associated with violence. A situation involving a person who has or is threatening to use a firearm, and may be moving from one location to another, requires a specific response protocol.

A multidisciplinary team should be appointed by the HCF to designate its plan for responding to an active shooter, in coordination with law enforcement.

Communication procedures should be established that include the creation of a specific announcement (emergency code or plain language) and procedure to institute a response to an active shooter situation.

The HCF should have a timely HCF-wide notification system to alert staff to the threat of an active shooter. The mechanisms should include multiple modes of notification intended to reach all persons inside the facility and on its grounds. These may include overhead pages, text (SMS) messaging, digital displays, e-mails, intercoms, call boxes, popup messages, or other notification methods.

Employees and staff should be educated on their awareness, reporting of and response to an active shooter. Specific procedures should be established for the initial response of staff or anyone in the immediate vicinity of an active shooter. Actions may include:

— to seek cover and protection;

— to leave the area if possible;

— to evacuate safely as many patients, visitors and staff as practical from the area (if it is possible to leave the aera);

— to shut and lock doors or otherwise shelter in place in a secured area until law enforcement authorities arrive (if it is impossible to leave the area); and

All electronic devices should be silenced.

— to avoid entering or moving towards the area where an active shooter is reported or believed to be in.

The activation of the active shooter response plan should include immediate notification of the law enforcement. The communication with law enforcement should be maintained and may include:

— All known and developing information on the incident, including the description and background of the suspect(s);

— A description of the weapons used;

— Known information on any victims or hostages; and

— Location(s) impacted by the event and current location involved. Responding law enforcement officials should be provided facility maps, access codes, keys or other requirements.

The activation of the active shooter response plan may include these actions at the HCF:

— Establishing an incident command post and Emergency Operations Centre as circumstances warrant;

— Restricting access to the facility;

— Re-routing or diverting incoming patients; and

- Disabling utilities, news and public Wi-Fi systems when appropriate and in consultation with law enforcement guidance.

Upon conclusion of an active shooter event, the HCF should announce an "all clear" only after law enforcement has indicated the environment is safe. Additional measures may include:

- Accounting for all patients and all staff members (physicians and contract) listed in the census;
- Responding to the medical needs of victims;
- Assessing damage to the building, equipment and sterile environments;
- Arranging for employee assistance programs for staff members;
- Providing additional security or law enforcement presence; and
- Debriefing, evaluating, and reviewing the incident and the effectiveness of the emergency plan and response. Change or update the response plan as needed.

Active shooter drills should be conducted periodically to exercise the plan and the response of law enforcement.

4.5.6 Drug diversion and security of CBRNE substances

Drug diversion is a concern for all HCFs. Implementation of proper safeguards and administration of drug control methodologies, and subsequent investigation of controlled substance diversion or theft, is a responsibility of all HCFs.

These mechanisms can also be used to secure high risk chemical, biological, radioactive or nuclear substances. 'Controlled substances' can also mean CBRNE substances.

Drug/CBRNE diversion or tampering can take many forms such as:

- Simple theft – controlled substance/high risk CBRNE substances taken from a cabinet, dispensing mechanism or other area where controlled substances are stored;
- Theft by substitution – controlled substance is removed from its container and replaced with another substance;
- Theft by documentation – the medical chart, records, or logs manipulated to show controlled substance was administered and dosage given, however small an amount;
- No medication was actually given; or
- Under-medicating the patient – a specific amount of controlled substance is ordered and only partially administered.

The HCF should designate, in writing, the person (by title) responsible for the security of controlled substances. Security should work in collaboration with these individuals and others delegated with the responsibility for the protection of controlled substances.

Staff working with controlled substance distribution, administration, and disposal should be active in the safeguarding of controlled substances and educated on this responsibility.

All staff, including contract staff, should be required to report suspicious behavior or activity involving controlled substance handling, or a suspected unfitness for duty or a substance abuse problem.

The HCF should have a system in place to monitor and audit controlled substances. This includes examining practices for storage, handling, administering, and disposal of controlled substances. HCFs should conduct random reviews of all controlled substance transactions. Auditing software may be used and can provide evidence should the audit reveal a drug diversion.

The HCF should develop and periodically review controlled substance policies and procedures, e.g. handling and dispensing, wasting practices, discrepancy investigation and violation reporting. The HCF should have a written policy stating no prescription drug, non-prescription drug, or controlled substance may be sold, transferred or otherwise distributed unless authorized in writing by the appropriate individual charged with such responsibility.

Procedures for immediate follow-up and reporting of a suspected violation of drug diversion or other incidents associated with the mishandling or misuse of controlled substances should be developed. Actions should include:

- initiate a timely and confidential inquiry;
- maintain patient and staff safety;
- conduct a drug audit for purposes of determining if a discrepancy exists;
- maintain the integrity of investigation; and
- respond to potential impairment.

Security should engage in or support investigative activity as part of the follow-up of a suspected violation.

A program for drug testing of staff who handle controlled substances should be considered as a proactive element of drug control and may provide information that suggests the need for further investigation.

Notifications of suspected drug diversion received from external reporting sources, such as local law enforcement personnel or a regulatory board, should be referred to the HCFs Pharmacy authority or other designated official.

The HCF should establish clear responsibilities for reporting drug diversion or theft/misuse of controlled substances to internal and external authorities.

4.5.7 Vehicle and aircraft security

The HCF that uses emergency vehicles or aircraft should provide adequate security for parking vehicles whilst not in use. Unattended ambulances parked on the facility grounds should always be locked, the keys and vehicle remain the responsibility of the vehicle driver or attendant and provisions should be in place to ensure that ambulances are not obstructed by other parked vehicles.

Accident response or triage vehicles, when not in use, should be parked in a conspicuous position in clear view. A vehicle alarm system should be fitted to these vehicles.

Aircraft used for medical evacuation should not be left unattended or unsecured when not in use. Aircraft security remains the responsibility of the pilot concerned. However, the security personnel should assist with short-term security when requested.

4.5.8 Media

If permission is granted for visits by the media, the following security principles should be observed:

- a responsible person should accompany representatives throughout the visit, and
- classified material should be protected from access by members of the media.

Script and photographs to be released to the media should be vetted by the organization prior to release.

5 Performance evaluation

5.1 General

The performance review should take into account reports and statistics explained in 4.4.4 and 4.4.5. This review should take into account results from performed exercises and tests.

5.2 Management review

Top management should review the organization's healthcare facility security management at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review should include consideration of:

- information on the security performance, including trends;
- feedback of interested parties;
- opportunities for continual improvement and possible demand on changes to the healthcare facility security management system;
- update of risk assessment, risk analysis, incident management and prevention;
- healthcare and operational requirements;
- risk reduction and security requirements;
- regulatory, legal and other requirements (requirements of other standards which the organization decide to comply or implement);
- contractual obligations;
- resources need; and
- improvement to how the effectiveness of control is measured.

6 Exercise and testing

The organization should test and evaluate the appropriateness and efficiency of its healthcare facility security management system, its objectives, targets, processes and procedures (including partnership, outsourcers and supply chain relationships).

An annual exercise for security personnel and other staff (high risk) should be performed, preferably including interaction with external parties (law enforcement) based on selected security scenarios.

The organization should validate its healthcare facility security management system using exercises and tests that:

- are consistent with the scope of the healthcare facility security management system and objectives of the organization;
- are based on realistic scenarios that are well planned with clearly defined aims and objectives;
- minimize the risk of disruption to operations and the potential to cause risk to operations assets and patients;
- are respectful of the human right of privacy for patients;

- produce a formalized post-exercise report that contains outcomes, recommendations, and arrangements to implement improvements in a timely fashion;
- are reviewed within the context of continual improvement; and
- are conducted at planned intervals and from time to time on a non-periodic basis as determined by the management of the organization, as well as when significant changes occur within the organization and the environment it operates in.

NOTE Contractual obligations may include contracts between governmental bodies on healthcare services provided by organization in healthcare facility, which may refer to legal and regulatory obligations. These obligations depend on national healthcare systems, which may vary in each European member state.

Bibliography

EN ISO 9001:2008, *Quality management systems - Requirements (ISO 9001:2008)*

EN ISO 11064 (all parts), *Ergonomic design of control centres (ISO 11064)*

EN 13940-1:2007, *Health informatics - System of concepts to support continuity of care - Part 1: Basic concepts*

ISO 22398:2013, *Societal security — Guidelines for exercises*

ISO/IEC 27000:2014, *Information technology —Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

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

ISO 31000:2009, *Risk management — Principles and guidelines*

IEC 31010:2009, *Risk management — Risk assessment techniques*

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™