NHS National Services Scotland

Security Management Framework for NHS Boards in Scotland

Health Facilities Scotland
Facilities Management

December 2008

Contents

Disclaimer

The contents of this document are provided by way of general guidance only at the time of its publication. Any party making any use thereof or placing any reliance thereon shall do so only upon exercise of that party's own judgement as to the adequacy of the contents in the particular circumstances of its use and application. No warranty is given as to the accuracy, relevance or completeness of the contents of this document and Health Facilities Scotland, a Division of NHS National Services Scotland, shall have no responsibility for any errors in or omissions therefrom, or any use made of, or reliance placed upon, any of the contents of this document.

1. Introduction

Background

1.1 The Scottish Government Health Directorate (SGHD) is committed to improving the environment within NHS hospitals for patients, staff and all other users of these facilities. A range of standards and initiatives have already been introduced for a number of facilities management staff (FM) and it is well recognised that all areas of FM underpin clinical care and are important elements contributing to patients wellbeing and recovery.

To ensure continuous improvement in all areas of FM, Health Facilities Scotland has established a Strategic Facilities Group to advise the Scottish Government Health Directorate (SGHD) and take other initiatives forward. This Framework aims to address the important issues of safety for staff and patients from physical and non-physical assaults, crime prevention and the related activities of training, reporting and monitoring of performance and continuous improvement.

The delivery of security services

1.2 Generally the management of so-called 'soft' facilities services, which includes security, is split between estates and hotel services. Organisational structures within Boards continue to evolve to reflect the increasing importance being placed on these aspects of FM in supporting the delivery of clinical services.

In the majority of Boards, the responsibility for security is channelled through directorates covering Estates and/or Facilities (hotel services) or Risk Management. Structures below director level generally involve a designated manager with responsibility for security, managing contracted services and/or overseeing the activities of in-house staff, and disseminating policy for these services.

This Security Management Framework requires that Boards nominate a Board member with responsibility for these services.

Purpose of the Framework

1.3 The purpose of this Framework is to introduce revised security standards for NHSScotland and provide guidance on their implementation.

The central part of this document is the requirement for Risk Assessment, (see Appendix A), and this is complemented by additional guidance and examples of best practice.

Reference sources of further information have been provided in Appendix A and Appendix B respectively.

There are many organisations, which have an important part to play in providing Boards with information and support. It is essential that Boards are aware of them, and familiar with their particular area of support and/or expertise. Appendix B: B3 provides examples of such organisations.

2. Risk management

2.1 As with many areas of FM there are examples of good practice in many hospitals in Scotland. It is, however, necessary and desirable for realistic, attainable, and common standards of security to be applied across NHSScotland. The Risk Management Standard set out at Appendix A, provides these common standards whilst leaving adequate scope for Boards to adopt operational processes in respect of specific issues and local needs.

2.2 A major feature of the standard is the need for an appropriate level of knowledge and expertise on security matters to be available throughout the organisation in order to ensure the development of effective security strategies, policies and procedures. In support of this, it is essential to actively engage with all concerned, and establish a culture that allows stakeholders the opportunity to play their part in reducing security risk.

The following notes cover each Area of Assessment in turn:

Area for Assessment 1: Accountability throughout the organisation

2.3 Boards will have a single Executive Director with lead responsibility for management of security across the organisation who will ensure:

- the establishment of appropriate structures, policies and processes necessary for the Board-wide approach to the management of security issues;
- access to appropriate specialist advice;
- central accountability and Board reporting arrangements.

2.4 Boards must ensure that the Board level Director with responsibility for this work has access to competent specialist advice on security related issues. In addition, they will need to ensure that they have attended basic awareness training as a minimum.

2.5 The Board should be aware of the key security issues facing the organisation. Evidence of regular reporting of issues via the Board's formal committee structures, Board meetings or Performance Management arrangement should be demonstrated via formal minutes/agendas etc.

2.6 If not already in place, Boards should establish a multidisciplinary committee that has part, or whole, of its agenda dedicated to the implementation and monitoring of the Board's security strategy/action plans. This forum must include representation from relevant competent person(s) and managers with direct responsibility for security management.

2.7 Boards should ensure that line managers are aware of and understand their responsibilities in relation to the management of security in their areas of control.

Area for Assessment 2: Accountability at operational level

2.8 It is now seen as imperative that each Board has a designated staff member with specific operational responsibility for security, and this has been made an explicit requirement for this 'Area for Assessment'.

2.9 In larger Boards there is an expectation that an appropriately trained Security Manager will be appointed who will normally work for a senior manager reporting directly to the Executive Director with overall accountability for security. The senior manager will need to have a comprehensive understanding of security issues, whereas the Security Manager will be expected to have undergone some form of accredited training. Although not compulsory at this time in NHSScotland, consideration should be given to the four week Local Security Management Specialist (LSMS) training course organised by the Counter Fraud and Security Management Service (CFSMS).

2.10 Smaller Boards may be unable to justify the appointment of a full-time Security Manager, and might wish to consider making a joint appointment with another Board.

2.11 Security should not be an additional responsibility for an existing member of staff unless it is clear that there is the capacity for them to fulfil the role. Time should be given for adequate on-going training and the development of expertise and specialist knowledge. Boards may also have access to a number of other individuals who are also appropriately trained and who have specific expertise in particular areas e.g. police, government officials, and industry specialists.

Area for Assessment 3: Accountability for policy and strategy

2.12 A range of measures should be identified for ensuring adequate exposure and communication of the security policy. It is not sufficient to present staff with a file of all Board policies to read and sign with the expectation that these will be fully understood and supported. Formal lines of communication should be supplemented by less formal ones including video/DVDs, posters, flyers and use of an intranet site.

Area for Assessment 4: Process for crime prevention

2.13 It is important to utilise risk assessment in the development of suitable crime prevention programmes. In addition, there is the expectation that such programmes will incorporate specific crime prevention plans for particular areas and involve relevant staff at all levels with clear lines of communication for them to contribute to the refinement of the plans.

Area for Assessment 5: Process for responding to incidents

2.14 This area is focused on the development and communication of the appropriate response plans and has detailed requirements for what must be included.

Area for Assessment 6: Process for the reporting and analysis of incidents

2.15 Systems for security hazard incident reporting should not be set up in isolation. Some systems whilst appearing robust may have shortcomings, for example, incidents fed into the system during night shift may not be adequately communicated to day staff on handover.

Additionally, it is important that adequate lessons are learnt from each and every incident, and that full account is taken of them with measures including:

- amending security procedures;
- updating risk assessments;
- highlighting hot spots;
- identifying the need for further training;
- improvements in communication to relevant staff;
- improvements in supporting staff;
- improvements in raising awareness;
- identifying shortcomings in systems.

Area for Assessment 7: Process for risk management

2.16 This standard indicates the part that 'Departmental Security Guidelines' may play, and how their development may assist with the risk management of security issues. The guidelines would relate to a particular department and should be read and implemented in conjunction with the Board's overall Security Policy, to ensure a safe environment for staff, patients and visitors alike.

Contents may include, for example:

- a reception process for screening visitors;
- keys, alarms and the use of access systems;
- daily opening and lock downs;
- wearing/carrying identification badges;
- safeguarding patients, child protection and personal safety;
- IT protection and confidentiality;
- protecting staff property.

Area for Assessment 8: Capability and access to information

2.17 In order for the organisation to have access to up-to-date security related legislation and guidance, there is a requirement for the Security

Manager/Specialist with the specific operational responsibility for Board security matters to have a PC with full internet access.

Area for Assessment 9: Capability and providing the necessary training

2.18 This area emphasises the need for security training to be tailored for particular staff groups with respect to the risks involved along with crime prevention and conflict resolution being given specific requirements for assessment. In addition, as indicated under Assessment Area 1, there is an emphasis placed upon an appropriate level of awareness of security issues at all levels with a specific requirement for the Board. Areas of Assessment 1 and 2 also highlight training needs by inclusion of specific requirements for the nominated Executive Director to have specialist advice on security matters readily available, and the importance of specialist training for the security manager or other individual with specific operational responsibility.

Area for Assessment 10: Capability and the competence of security staff

2.19 The standard that should be applied when recruiting security staff is, BS7858 – 'The Code of Practice for Security Screening of Personnel Employed in a Security Environment', which sets out the vetting process to be followed. Procedures for pre and post employment checks for all persons working within NHSScotland should also be observed during the recruitment process.

Boards should be aware that compulsory licensing and regulations of the private security industry in Scotland came into force on the 1st November 2007. From this date it is illegal to operate in Scotland in a designated security role without a Security Industry Authority (SIA) Licence. At a future date, it is expected that the requirements will be extended to cover in-house services.

Area for Assessment 11: Outcomes and the use of key indicators.

2.20 This area has a list of compulsory key indicators for data collection systems and a requirement for Boards to make use of internal performance indicators designed to assist managing security risks.

Area for Assessment 12: Monitoring and review

2.21 Management arrangements should include an internal audit function as well as other quality control and assurance functions. The internal audit function is required to give an indication to the Board of the adequacy and effectiveness of the overall system of internal audit. It is expected that Boards will employ Information Technology to best effect in the monitoring and review process of their security management system, and to ensure that the nominated Executive Director for security issues provides up-to-date management information for the Board on a regular basis.

Area for Assessment 13: Audit

2.22 With a range of independent internal and external assurance available, attention is drawn to making optimum use of these services and the need for vigilance in avoiding duplication and/or omission.

3. Additional guidelines

Co-ordination and communications

3.1 As part of a Board's Security Strategy, a multidisciplinary committee should be established (referred to in Section 2 under Area for Assessment 1). This may include hospital management and staff representation, as well as representatives from public groups, local authorities and those having responsibility for local safety, local police (operational and crime prevention staff), as well as representatives from appropriate contract security companies. The multidisciplinary approach will also provide a valuable opportunity to inform on a wide range of issues such as the requirement for a Board to take into account all security considerations in its Arson Policy and Fire Strategy.

3.2 An example of the main objectives of a Board Security Group is as follows:

Good Practice Example - Board Security Group

Main Objectives

- to develop a community approach to security and crime reduction, working together to ensure that there is a secure healthcare environment that protects patients and staff, visitors and their property, as well as physical assets of the Board;
- for the police, the Board and those having responsibility for community safety and security to work collaboratively to promote an effective security policy;
- to promote good practice across all agencies and develop a common understanding of the issues pertinent to each agency;
- to establish partnership links with crime reduction and community safety groups to help promote security awareness amongst all employees of the Board along with patients and visitors to the Board;
- to contribute legally and effectively to the collection and sharing of information with partners;
- to support Home Office initiatives and contribute to tackling violence in the community;
- to promote operational initiatives, for example the use of anti-social behaviour law that will ensure patients, staff and visitors feel and are indeed, safe in their working environment and during their visits to Board sites;
- to reduce crime (and the fear of crime) on Board sites and through its work within communities across the Board catchment area;
- to introduce and promote a 'Hospital Watch' scheme throughout the community;
- to clearly define any legal responsibilities that affects the Board;
- to monitor and review current practice, feedback from sub-groups and identify operational difficulties;
- to establish effective lines of communication to relevant sub groups and for all staff on matters relating to security;
- to identify resource requirements and potential funding;
- to continually monitor and review the Board's security strategy plans and progress;
- to produce an annual report on the progress on the Board's security strategy, the system of security management in place and its effectiveness and recommend any improvements that may be required.

3.3 Maintaining effective communication channels with staff is essential, not only to ensure that staff can keep colleagues informed of their whereabouts, but also to provide a means of making contact in an emergency and improve an

individual's sense of security. Boards will therefore need to consider carefully the communication needs of their staff and the measures that can be taken to minimise any risk to their safety.

3.4 In the case of lone workers, guidance issued for the NHS in England deals with their protection, and this is to be complemented with more specific guidance for the ambulance and mental health environments. Should Boards consider this guidance, it needs to be stressed that it cannot cater for every situation that may, or could, occur within a particular environment. Indeed, it states that such guidance should be used as a template from which local procedures and systems to protect lone workers should be developed, revised and enhanced.

It is only by Board ownership of procedures developed in this way that the local needs of staff and the environments in which they have to work will be fully reflected and properly addressed. The NHS Security Management Service has also issued an evaluation report on lone worker devices in a healthcare setting that provides a valuable insight into how best to use such technology for a range of applications.

Crime reduction

Personal safety awareness

3.5 Police Force Training departments are usually able to offer presentations to organisations/Boards on Personal Safety Awareness, at very reasonable costs.

Good Practice Example - Personal safety awareness

Police forces across England and Wales have delivered presentations covering a range of issues including the following:

- subject behaviour patterns;
- impact factors;
- reasonable response options;
- tactical communications;
- danger warning signs;
- the five-step appeal – Simple, Reasonable, Personal, and Final – followed by Action.

Car parking

3.6 Schemes such as the 'Safer Parking Scheme' is an initiative of the Association of Chief Police Officers (ACPO) aimed at reducing crime and the fear of crime in parking facilities. Safer parking status, Park Mark, is awarded to parking facilities, which have achieved the requirements of a risk assessment as conducted by the police. The scheme is just one of the ACPO's 'Secured by Design' initiatives and is managed by the British Parking Association on behalf of ACPO, and supported by the Home Office. Full details are provided at: http://www.britishparking.co.uk. See also http://www.securedbydesign.com

CCTV

3.7 The use of CCTV has been well documented as a good disincentive to anti-social behaviour and/or unlawful behaviour and can also provide important

evidence when offenders are prosecuted. When employed in conjunction with other security measures, it can play an essential role in the delivery of a highly effective system that provides benefits far greater than the sum of its parts, as shown in the following case study.

Case Study – Kings College Hospital: Security Control Room

The Security Control Room at Kings College Hospital is the centre of their response to incidents in A&E and across the Trust through the use of Pinpoint CCTV, panic alarms and emergency telephone numbers. Help points and intruder alarms are all responded to from this room. The integration of systems has improved emergency response times and has seen a fall in crime within the Trust grounds. The establishment of a control room and the use of CCTV, security staff and Pinpoint all underline the Trust's commitment to staff safety and have found universal support from staff and their representatives at Kings.

The Kings Security team provides the principal response to incidents in A&E across the Trust. They are recruited through selection days where skills are tested, including interpersonal skills and backgrounds are vetted to British Standard 7858. The security team can deal with 75% of incidents without needing police support. The duration of incidents are shorter, perpetrators are detained and, if appropriate, are arrested by police.

Pinpoint is a proprietary staff safety system that was initially installed in A&E and X-Ray, and since extended into many Outpatient Departments (OPDs) and wards. It comprises of a staff portable alarm which, if triggered, transmits to a receiver in the ceiling which has a unique address such as 'Lift Lobby' or 'Main Reception'. This signals to all A&E staff bases and to the master panel in Security Control. A&E staff will respond and security staff will be instantly despatched to the location with the radio message 'Pinpoint Main Reception'. A&E staff confidence in the system is high and they know assistance will be swift to arrive.

CCTV is a key component in providing for staff safety in A&E and across the Trust. This includes the external campus and car parks where it is integrated with lighting. The aim is to achieve 'Park Mark' Safer Parking Status. The system has a full maintenance contract with higher priority call out for A&E cameras. The systems presence is well advertised with a highly visible control room, signs and Public Display Monitors at principal entrances. The monitor in A&E is located just inside the doors and with integral cameras, records high quality images of all who arrive. The system has been designed to allow for live recordings which are frequently used during A&E incidents. In the event of an incident the Trust regularly provides video evidence to the police.

Learning from incidents

Reporting on the range of incidents encountered

3.8 The type of data collected on security incidents both crime and non-crime, and the way it is reported, ultimately determines the value of any information that may be obtained. The value in recording appropriate data that is clearly defined cannot be overstated, as it provides for better informed planning for crime reduction and the improvement to security services across the Boards healthcare premises.

3.9 Appendix C gives guidelines on the reporting of crime with recommendations on what details to include, what categories to assign to an incident, and points to assist with criminal investigations. Appendix D provides guidelines on the reporting of non-crime incidents, with recommendations on what details to report and using categories for such incidents.

3.10 There are a number of different software systems for incident reporting currently in use by the NHS that capture data relating to a multitude of incidents from minor thefts to serious physical assaults.

3.11 This data can be used for local risk management work, reporting to the National Patient Safety Agency (NPSA), and the Health and Safety Executive (HSE) on Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) incidents.

Involvement with security related organisations

3.12 It is important for Boards to be aware of, and be actively involved with wherever possible, the activities of organisations and groups associated with security, such as the National Association of Healthcare Fire Officers.

The Scottish branch of NAHFO can be found at http://www.nahfoscotland.co.uk.

Partnerships

3.13 Linking up with local authorities and other organisations to mutual advantage should be employed wherever possible, examples of which are set out below.

Good Practice Example

Informing staff and the public of local measures to 'reduce the fear of crime and improve the quality of life'.

In partnership with Merthyr Tydfil and Rhondda Cynon Taff Community Safety Partnerships, and at no cost to the Trust, North Glamorgan NHS Trust has embarked on an innovative method of informing staff and as many members of the public as possible of the action being taken to "*reduce the fear of crime and improve the quality of life*" for people working and living in the Merthyr and RCT area.

The method used is to install TV screens at sites around the Borough where they would receive maximum viewing. The screens feature a continuous supply of information, advice and up to date information about the crime reduction and community safety schemes already operating or being planned for the area.

The 'Crime Wise' TV screens have been installed in three areas of Prince Charles Hospital and a screen has also been installed at Hirwaun Health Centre. The scheme was officially launched at Prince Charles Hospital in August 2004.

Good Practice Example: Community Police Officers based at a hospital

A number of Trusts have arranged for a police officer to be stationed at the hospital. The Community Police Officer shares an office with the security team and uses this as a base for the working week that is divided between the hospital and the local community. The Trusts contribute toward the Police Officers salaries although all of the equipment that the officers require eg a computer is provided by the Officers Force.

The partnership has proved to be very beneficial to the Trusts and staff are happy in the knowledge that a Police Officer is based on site to deal with any queries or criminal acts that may take place.

Good Practice Example: Boards working with their local Police Force

Here are a number of examples of Boards working closely with the Police Force over a number of issues and in a variety of ways including:

- holding police 'surgeries' at a number of sites for members of staff;
- police representation on a number of Board bodies: security forum, Violence Group, Mental Health and A&E group;
- regular meetings of the Mental Health and Learning Disabilities Division regarding the Violence/Aggression issues of clients in police custody;
- police architect liaison officers involvement with Project Planning (Estates) initiated scheme, whereby all new build and major upgrades incorporate the 'design out of crime' whenever possible.

Staffing issues

Recruitment

3.14 As with the recruitment of any member of staff, an accurate job description is essential for the successful recruitment and retention of security personnel. The relevant aspects of the post may be set out in the description as follows:

- job purpose;
- organisational arrangements;
- general/detailed duties and responsibilities;
- key result areas;
- dealing with incidents using initiative.

Examples of job descriptions presented in this way for a Security Manager and Security Officer are given in Appendix E. These examples are based on guidelines provided by the National Association for Healthcare Security and may assist in the recruitment of suitable security personnel.

They provide a framework on which to include the requirements of a particular Board. For example, security personnel may be ideally placed to take first line action for a range of incidents and Boards may see this as an opportunity for such personnel to apply timely first aid, release person trapped from lifts (when safe to do so), or deal with fire alarms etc.

Training

3.15 The provision of appropriate training is clearly a pre-requisite if security staff are to meet the demands expected of them in providing an effective and professional service. However, given the unique nature of many incidents and the wide-ranging background knowledge needed to deal with them, it may be less than clear as to what may be appropriate to include within the training programme. An example of what to include in the basic training programme for a Healthcare Security Officer is provided in Appendix F, which covers the programme identified by the National Association of Healthcare Security.

The Knowledge and Skills Framework (KSF)

3.16 Boards will be aware that the NHS KSF provides a way of recognising the skills and knowledge that a person needs to apply to be effective in a particular NHS post, and ensure better links between education and development and career and pay progression.

The licensing of private security operations

3.17 From 10th January 2005 the Security Industry Authority (SIA) has accepted requests for licence application packs for the sectors to be licensed under the new licensing scheme for the private security industry in England and Wales. Boards will also be aware that compulsory licensing and regulation of the private security industry in Scotland came into force on 1st November 2007. From that day it is now illegal to operate in Scotland in a designated security role without a Security Industry Authority (SIA) licence.

The SIA will be responsible for licensing the private security industry across the whole of Great Britain, creating one security regulator and one set of security licences.

The four licensable security sectors are as follows:

- security guarding;
- cash and valuables in transit;
- CCTV in public space surveillance;
- close protection.

Anyone involved in the licensable sectors and who works under contract will need to be licensed. This includes employees, supervisors, managers and directors of security companies. Licensing does not extend to those employed in-house.

To gain a SIA licence, applicants will need to attend an approved training course, attain a nationally recognised qualification and undergo identity and criminal records checks. As licensing is introduced, the SIA undertake to engage with key stakeholders to continuously improve the standards of both training and qualifications.

Procedures for the specific security issues

3.18 Boards are required to have in place procedures for a range of issues in support of their security policies and action plans.

Outline example of security procedure - Child/Infant Abduction

This procedure describes the action to be taken in the event of a child or infant disappearing whilst on Board premises, and underpins the Board Security Policy. It clearly sets out its exact purpose and details warning signs before an incident is triggered by the actual event of a child or infant going missing in order to prevent such an occurrence wherever possible.

Detailed procedures for action to be taken by all members of staff at the location in the event of a child or infant being announced as missing, are set out as action cards, each tailored for an individual's role e.g. switchboard and bed manager/senior nurse.

The circumstances for police involvement, and where the police may decide to deal with the missing child or infant as a police matter is detailed with clear instructions on how staff should support the investigation. Following the incident, the important process of a structured de-brief is set out as part of the procedure.

Outline example of security procedure: Dealing with a suspect package

This procedure sets out the actions required in the event of discovering a suspect improvised explosive device.

The procedure starts by running through the key principles and lead roles of staff and the nature of appropriate warnings prior to the police taking command of the incident. This is followed by detailed procedures for action to be taken by all members of staff at the location, such as assisting with search and evacuation, in the event of the detection of a suspect package being identified. These are set out as action cards tailored for each individual's role e.g. security officer and senior nurse.

Following the incident a detailed checklist to accompany the incident report for the Risk Department has to be completed prior to the important process of a structured de-brief.

Outline example of security protocol: The Deployment of Police Officers with Firearms at Board Hospitals

This protocol is in place to provide a clear understanding between health and police professionals where planning and cooperation is required to accommodate the need for the deployment of Police Authorised Firearms Officers (AFOs) within Board hospitals.

The protocol draws attention to the hazards involved with such a deployment and the requirement for detailed contingency plans that consider the needs of particular departments. Considerations such as methods of communication, identification requirements and dealing with enquiries under particular circumstances are set out along with how to achieve the essential close management liaison at all stages of the deployment of an AFO.

Following the deployment, the protocol ends with instructions on the appropriate method of debrief and the submission of the required incident reports.

Healthcare Premises Site Closure

3.19 A report was commissioned in June 2008 by Dr Kevin Woods, Chief Executive, NHSScotland in response to reports that person identifiable information had been found by members of the public in buildings on the site of the former Strathmartin Hospital in Tayside.

This guidance is taken from the key findings of this report and from the proposed local and national recommendations to mitigate against similar incidents occurring in the future.

Responsibility and Site Security

3.20 When a decision has been taken to close healthcare premises, Boards should appoint an explicitly designated person with overall responsibility for the decommissioning and eventual handover of the building(s). The designated person should ensure strict control of access to the building(s) and a formal log should be kept. The issue of both staff and members of the public being able to access disused and potentially dangerous buildings has wider implications for health and safety.

The designated person should provide a Project Initiation Document to the Board along with a Risk Register in order to agree project objectives and to measure successful achievement of the objectives.

Local Recommendations

Project Management and Leadership

3.21 Boards should ensure a formal project management structure and the formation of a Retraction Group chaired by the responsible person. Boards should carefully consider the core membership of the retraction group, which should include the following activities:

- clinical;
- support services;
- estates;
- projects;
- medical records;
- information management/data protection;
- health and safety;
- trade unions;
- internal audit - Confirming NHS Board assurance that procedures have been implemented (statement of internal control).

Information Governance

3.22 The Caldicott Guardian, the designated director for information governance (who may be the same person), and individuals with responsibility for records management and data protection need to work collaboratively, and be fully involved, in the planning and operational aspects of a hospital retraction process.

Local policies for records management need to be effectively disseminated to all staff and fully implemented.

Physical Operations and Security

3.23 All sites should be effectively 'sanitised' prior to being vacated; this should be checked and confirmed by effective sweeping and thorough inspection, and fully documented before the site is handed over to a new owner.

National Recommendations

3.24 The national guidance currently available, in particular the recently issued 'The Records Management: NHS Code of Practice (Scotland)'(CEL 28(2008) which outlines the standards of practice in the management of records for NHS organisations in Scotland is comprehensive. NHS Boards must tailor the guidance to their local environment and translate the principles into practice. In addition, the learning from the previous recent closure and relocation of the Royal Infirmary of Edinburgh and the Princess Margaret Rose Orthopaedic Hospital, Edinburgh, and the imminent closure and relocation of Falkirk and District Royal Infirmary and parts of Stirling Royal Infirmary may prove useful to other NHS Board areas.

National recommendations:

- national protocols for NHS site decommissioning and disposal, written with an operational focus and bringing together the key estates and information management responsibilities is required. A national protocol is presently being produced by Health Facilities Scotland;
- disused buildings should not be used for the storage of any health records or personal identifiable information;
- the annual property transactions return should be used to confirm that buildings which are surplus to requirements are effectively cleared and closed;
- all NHS staff need to be aware of their responsibilities with regard to data protection and management and be trained to an appropriate level relative to the requirements of their post;
- guidance on the operational procedure for management and disposal as necessary of health records and other patient identifiable information retained by clinical staff on departure from their post (for example if the post holder moves out of the area or retires) is required;

- all information relating to patients should be stored as part of their formal health record; if the information is no longer required it should be disposed of appropriately;
- improved guidance about disposal of health records is required; NHS boards appear to be clear about retention periods but the process of actual disposal when this period expires could be streamlined. It is recognised that this would have significant resource implications, and although the majority do not normally hold or deal with health records, all future national correspondence relating to records management and information and estates security, particularly ad hoc guidance issued in response to isolated incidents such as this, should be routinely circulated to the Special Health Boards as well as the operational NHS Boards, since they all hold personal identifiable and commercially sensitive information.

4. National NHS Documents Relevant to Personal Identifiable Information

The Data Protection Act 1998, an action plan for the NHS in Scotland (NHSiS) published by ISD, December 1999, http://www.show.scot.nhs.uk/publications/dp/dpaction.pdf.

Issued to/audience those charged with data protection (DP) responsibilities, e.g. DP Officers and Caldicott Guardians,

Main provisions sets out 36 actions to help organisations comply with DPA in respect to both manual and computerised data.

Action required by whom/when: for example:

- action 22 - review procedures for retention and disposal of records;
- action 23 – review compliance with legal requirements and national guidelines for retention periods. But no guidance is given as to who should be responsible for doing this or what the timetable should be.

Caldicott Guardians NHS Management Executive, Health Care Policy Division, March 1999, http://www.sehd.scot.nhs.uk/mels/1999_19.doc.

Issued to/audience NHS board general managers (GM) /Trust chief executives (CE) - to be made available to the Caldicott Guardian but should also be copied to all NHS board members.

Cc – e.g. Health Board/Trust Chairmen; Directors of Public Health /Trust Medical Directors/Director, Scottish Association of Health Councils/Directors of Education/Directors of Social Work

Main provisions requires each NHS Scotland organisation to appoint a senior clinician as the Caldicott Guardian with responsibility for information governance arrangements and sets out the guardian's responsibilities.

Action required by whom/when: BNHS board GMs/Trust CEs to assign responsibility to an appropriate person and implement a work programme to ensure obligations are met. It outlines the action that each organisation should take during 1999/2000, as well as the Guardian's role and responsibilities. This action will include:

- a management audit of current practice and procedures;
- annual plans for improvement that will be monitored through the clinical governance framework;
- the development of clear protocols to govern the disclosure of patient information to other organisations.

Protecting and Using Patient Information - A Manual for Caldicott Guardians Caldicott Guardians (but no reference to other recipients), SEHD, 1999, http://www.show.scot.nhs.uk/publications/me/caldicott.manual.doc.

Main provisions sets out the six principles to which guardians should adhere, of which the most relevant here are:

- principle 4 - Access to patient-identifiable information should be on a strict need to know basis;
- principle 5 - Everyone should be aware of their responsibilities;
- principle 6 - Understand and comply with the law.

Acknowledges that *"Although there is considerable guidance available on different aspects of how the NHS should go about protecting and using confidential patient information, it is not always easy to locate the relevant guidance on a particular issue… Reflecting a lack of legal clarity, complex ethical dimensions and the different viewpoints of different sections of society, the guidance on some issues may reflect the perspective of the issuing body and conflict, at least in part, with guidance issued by other bodies".*

Action required by whom/when: paragraph 10 in relation to 1999/2000 *"Although it is intended that each organisation should determine the pace at which it addresses the work programme that was outlined in MEL(1999)19, and described in more detail in this manual, there is an important element of sequencing which the following suggested timetable of work illustrates."*

Protecting Patient Confidentiality, The Confidentiality & Security Advisory Group for Scotland (CSAGS), April 2002, http://www.csags.scot.nhs.uk/.

Issued to/audience: report to Ministers, Widely distributed to consultation responders and Health Boards

Main provisions: emphasises the need to ensure security of health service information systems and sets out the 9 principles of confidentiality

Action required by whom/when: complying with the principles should apply to all employees/students/volunteers contractors

NHS Code of Practice on Protecting Patient Confidentiality, Scottish Executive, July 2003 update, http://www.confidentiality.scot.nhs.uk/publications/6074NHSCode.pdf.

Issued to/audience: issued to Chief Executives, HR Directors and Communications Directors under NHS HDL (2003) 37 for distribution to all staff, volunteers and contractors.

Main provisions: explains, for example:

- the regulatory requirements covering the use of information about patients with particular emphasis on the DPA;

- the Caldicott Framework;
- what is patient identifiable data;
- that staff must comply with the DPA and Caldicott and take advice from their Data;
- Protection Officer (DPO) where they are not sure about issues relating to the use of patient information;
- failure to comply with the Code is a disciplinary offence.

Action required by whom/when: all employees / students/ volunteers contractors must be in compliance with the Code.

The use of personal health information in NHSScotland to support patient care, SEHD – Deputy CMO, August 2003, NHS HDL (2003) 37, http://www.sehd.scot.nhs.uk/mels/HDL2003_37.pdf.

Issued to/audience: Chief executives

Main provisions: Reiterates requirement to meet legal obligations plus the CSAGs' recommendations.

Action required by whom/when: CEs are required to, e.g.

- ensure that good clinical practice regarding PII is integrated with clinical and staff governance and frameworks for clinical risk;
- recognise and support Caldicott Guardians;
- take note of milestones to progress and resources/initiatives to improve practice;

Ensure that their Board:

- issues the new code of practice to all staff volunteers and contractors;
- inserts a confidentiality clause in contracts;
- customises a patient information leaflet to be available to all patients;
- customises a staff information leaflet to be available to all staff and uses it in induction / refresher courses;
- uses anonymised data whenever possible;
- reviews staffing/support for DP and records management;
- produces Caldicott Guardian out-turn reports.

A Review of the Work of Caldicott Guardians in Scotland, Review Group, 2004, http://www.confidentiality.scot.nhs.uk/publications/Caldicott%20Review.pdf.

Issued to/audience: commissioned by SEHD and MDs / DPHs / DPOs.

Main provisions: to *"provide advice to the Scottish Executive on the future role, relationships and functions of the NHS Caldicott Guardians in Scotland in the light of recent guidance and legislation on the handling of patient data".*

Action required Action required by whom/when: As a result of the increase in the use of IT and the inter-dependency of systems, recommends that Guardians need to work more closely between themselves and with their colleagues in Data Protection, IT security and Records Management if risks are to be effectively managed. Sets out 6 recommendations for consideration.

Clinical Governance and Risk Management - National Standards, NHS QIS, October 2005,
http://www.nhshealthquality.org/nhsqis/files/CGRM_CSF_Oct05.pdf.

Issued to/audience: NHS Board Chief Executives/Chairs/Medical Directors/Directors of:

Planning/HR/Nursing/Finance/Public Health/Divisional Chief Executives/NHS QIS Board Liaison Coordinators/Heads of Clinical Governance/risk managers network (including others).

Main provisions: The standards are the conclusion of a two-year process of development. They were finalised following an extensive period of consultation, which sought to obtain the views of a wide range of individuals and organisations with an interest in clinical governance and risk management, including patients and members of the public.

They cover 3 standards:

- standard 1- Safe and effective care and services;
- standard 2- The health, wellbeing and care experience;
- standard 3- Assurance and accountability which includes information governance as follows:

3e Information governance

3e.1 A governance framework is in place which promotes the ethical and lawful use of information in enhancing decision-making to support and drive improvement.

3e.2 A comprehensive system is in place to ensure the secure and confidential management of personal information, including how it is obtained, recorded, used, shared, stored and disposed of, in line with current legislation.

3e.3 Patients are informed about how their personal information is recorded and used, how to access their personal information, and about their rights to determine how their personal information is shared and protected.

3e.4 Formal policies are in place to manage situations where consent to share information is withheld, and where disclosure of personal information is required without consent.

3e.5 Information management links clearly into clinical governance arrangements, and engages staff and patients in the development and application of information and communication technology.

3e.6 Systems are in place to ensure that staff have access to information to support decision-making and facilitate the delivery of quality of care and services.

Action required by whom/when: The standards are supported by a self-analysis framework, which will be completed by every NHS Board. The information contained within the self-analysis and the supporting evidence will be reviewed by NHS Quality IS to assist the review team to undertake a peer review visit of each NHSBoard.

A peer review team, made up of healthcare professionals and members of the public, will meet with the NHS Board to review and assess performance against the standards.

The first national programme of reviews against the standards was completed in 2006/07 and a further programme is scheduled to commence in May 2009.

A brief guide to Information Governance, NHS National Services Scotland, ISD – Stuart Bain, 2005, http://www.shb.scot.nhs.uk/initiatives/informationgovernance/documents/V2Infogovernance-guide-070122.pdf.

Issued to/audience: CEs / MDs / NDs - for distribution to all staff

Main provisions: A guide for staff that covers:

- why we need information;
- what is information governance;
- why is information governance important;
- how we can improve information governance;
- how personnel can make sure that information governance works;

Action required by whom/when: covers 7 requirements for all staff, contractors and volunteers to adhere to requirements, i.e.

- involve people whose PII is being collected;
- get it right – accurate / complete / up to date;
- keep information secure – covers storing and sending;
- only record what you need;
- don't keep it longer than you need to;

- share with care;
- know your obligations.

National Guidance on the Destruction of Records Pre - 2005

4.1 **Destruction of hospital records**, Department of Health for Scotland, July 1958, SHM 58/60

Issued to/audience: Unclear

Main provisions: Authorises the destruction of various types of hospital records after certain specified (minimum) time periods. These include financial and audit records, employment records and payroll, medical records and all allied documents such as x-rays, consent forms, operation books and nursing report books.

Action required by whom/when: If in doubt obtain advice from the Department/Scottish Records.

Office; NB: Contains no detailed guidance as to who should oversee the destruction/how the exercise should be undertaken.

Disposal of records that have lost their value, SHHD, December 1969, ECS(A) 21/1969.

Issued to/audience: Clerks to the Executive Councils/The Drug accounts Committee/Scottish Dental Estimates Board.

Main provisions: Authorises the destruction of specified documents after the period indicated. These include medical cards, maternity service records cards, claim forms (e.g. for night visits) and salaries and wages.

Action required by whom/when: All forms listed are to be treated as confidential waste when Executive Councils make arrangements for their disposal. NB: contains no detailed guidance as to who should oversee the destruction/how the exercise should be undertaken.

Guidance for the retention and destruction of health records, SEHD - Director of Information Services, December 1993, NHS MEL (1993) 152.

Issued to/audience: BGMs/TCEs

Main provisions: Sets out changes to the minimum period for which certain categories of health records are retained. It updates SHM 58/60 and covers for example, general hospital and community health service records, psychiatric records, GP records, Records of cancer patients, x-ray films and histological specimens.

Action required by whom/when: ensure all appropriate staff are aware of and follow the guidance. Required to copy to UGMs /CAMO/and medical directors of NHS Trusts who should bring it to the attention of all relevant clinical staff.

Health Boards should make arrangements to inform GPs about the content of the letter. NB: contains no detailed guidance as to who should oversee the destruction / how the exercise should be undertaken.

National Guidance Relating to Site Closures Pre - 2005

4.2 Property Management Policy and other Related Matters, SEHD, Finance Directorate, May 1999, NHS MEL (1999) 44
http://www.sehd.scot.nhs.uk/mels/1999_44.pdf.

Issued to/audience: TCEs/BGMs

Main provisions: Updates the Property Management Policy, (previously referred to as the Estates Management Policy) and aims:

- to ensure that NHSiS property is used efficiently, coherently and strategically to support Government plans and clinical needs;
- to provide and maintain an appropriate quality of affordable health care facilities which complement and support the provision of quality health care and which are sustainable over the life cycle.

Action required by whom/when: BGMs /TCEs to ensure that property strategies are led by and consistent with the HIP / TIP and *"preparation should normally be led by a senior person with both the professional competence and the breadth of experience and responsibility needed to deliver a robust and focused strategic plan. The Strategy should also reflect collaboration with local authorities and others involved in implementing the healthcare agendas and those able to advise on means of delivery, (e.g. on the actions and timescale needed to enable the disposal of surplus property)."* It sets out mandatory requirements for *"holding bodies"* that apply with immediate effect, including the need to comply with the requirements for the disposal etc of property set out in the Property Transactions Handbook, 1997.

NHS Scotland Property Transactions Handbook, enquiries to - Building and Estates Adviser SEHD – Directorate of Finance, November 2000 Edition, http://www.sehd.scot.nhs.uk/propertymatters/nhsa.pdf.

Main provisions: aims to be a ready source of reference on Departmental policy and related requirements, guidance thereon and on the more operational aspects of all heritable property transactions with the exception of endowment property.

Part A covers management and legal issues and sets out responsibilities for property transactions.

Part B outlines the mandatory requirements and for example states that:

2.2 Holding Bodies must regularly review their property holdings in order to identify that which may be disposed of - either by outright sale, or in certain circumstances, by lease or excambion.

2.3 A Holding Body must support the delivery of national and local health care strategies and priorities by identifying its essential, non-essential and surplus property.

2.4 Holding Bodies must ensure that the procedures relating to closure of NHS Scotland property are followed. [See NHS Circular 1975(GEN) 46]- copy unavailable.

Part C sets out the procedures to be followed.

The aim of the procedures is to ensure that NHS Scotland buys, sells, leases or excambs property at a price and on other conditions which are the best obtainable for the public interest at that time. It is essential that Holding Bodies are able to demonstrate publicly if need be that this aim has been achieved in every case.

It identifies that there are 5 key stages in the disposal of property:

- stage 1: identification of surplus property;
- stage 2: preliminaries to sale;
- stage 3: marketing;
- stage 4: consideration of offers;
- stage 5: formal conclusion of sale.

However, the procedures do not contain any advice on clearing the site of records etc.

Action required by whom/when: Holding Bodies should ensure that their staff and external advisers are fully familiar with the contents of the Handbook, particularly when they are seeking advice on specific issues. NB: Primary day-to-day responsibility for achieving these objectives rests with the Chief Executive of the Holding Body. This is a significant responsibility and he/she is answerable to the Accountable Officer, to ensure that procedures are followed- and that it can be demonstrated, publicly if necessary, that the best obtainable outcome for the public interest has been achieved in every case. Property transactions can attract considerable public interest and are subject to scrutiny by the Scottish Parliament and Audit Scotland.

NHSScotland Property Transactions, SEHD Directorate of Finance, February 2001, HDL (2001) 15 http://www.sehd.scot.nhs.uk/mels/HDL2001_15.htm.

Issued to/audience: TCEs / BGMs and cc to Director, NHSiS Property and Environment Forum and SEDD Planning Division

Main provisions: makes it clear that service planning, the formal closure process and the development and agreement of Business Cases falls out with the immediate and direct influence of the Property Transactions Handbook.

Action required by whom/when: Holding Bodies to apply the Handbook guidance to individual transactions as soon as possible.

National Guidance on the Destruction of Records Pre - 2005

4.3 **The Management, Retention And Disposal Of Administrative Records**, SEHD, Directorate of Primary Care & Community Care, April 2006, HDL (2006) 28, http://www.sehd.scot.nhs.uk/mels/HDL2006_28.pdf.

Issued to/audience: NHSb Ces/Directors of clinical leads/IM&T leads/Directors of Finance

Main provisions: provides NHS Boards and special Health Boards with updated guidance on the retention and disposal of administrative records (it does not include the personal health records of individual patients).

This guidance replaces that relating to administrative records previously issued in Scottish Health Memorandum 60 of 1958 (SHM 58/60).

It emphasises the need to comply with the FOI (Scotland) Act 2002 and DPA 1998 and therefore the need to ensure sound records management practices.

It sets out minimum retention periods for general records, financial records, property, environment and safety records, human resources records, procurement and stores records, NHS Board records and service planning records.

Action required by whom/when: Chief Executives are asked to: Comply with the records management guidance set out in the Code of Practice on Records Management issued under Section 61(6) of the Freedom of Information (Scotland) Act 2002.

NB: contains no detailed guidance as to who should oversee the destruction/how the exercise should be undertaken.

Records Management: NHS Code of Practice (Scotland), SGHD – Healthcare Policy and Strategy Directorate and the Manual is published by the SG eHealth Directorate, July 2008, CEL 28 (2008) http://www.scotland.gov.uk/Publications/2008/07/01082955/0 and the associated Manual - http://www.scotland.gov.uk/Publications/2008/07/01082955/1.

Issued to/audience: CEs / Health Records Managers / Data Protection Managers / Caldicott Guardians / corporate records managers/FoI Leads

4.4 Main provisions

The manual aims to:

- establish best practice in relation to the creation/use/storage/management and disposal of records;
- provide information on legal obligations that apply to records;
- set out recommendations to assist the NHS to fulfil their obligations;

- explain the requirement to select records for permanent preservation;
- set out minimum retention periods for personal health records and refers to HDL (2006) 28 for other retention periods for other records – Annex D that replaces: SHM 58/60, ECS (A) 21/1969 and MEL (1993) 152.

As with the documents it replaces, this Annex contains no detailed guidance as to who should oversee the destruction/how the exercise should be undertaken.

4.5 The manual covers Accountability and the need to comply with the Law

14. Chief Executives and senior managers of all NHS organisations are personally accountable for records management within their organisation. NHS organisations are also required to take positive ownership of, and responsibility for, the records legacy of predecessor organisations and/or obsolete services.

15. In addition, NHS organisations need robust records management procedures to meet the requirements set out under the Data Protection Act 1998, the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004.

4.6 In terms of Management and Organisational Responsibility

25. The records management function should be recognised as a specific corporate responsibility within every NHS organisation. It should provide a managerial focus for records of all types in all formats, including electronic records, throughout their life cycle, from planning and creation through to ultimate disposal. It should have clearly defined responsibilities and objectives, and necessary resources to achieve them.

26. Designated members of staff of appropriate seniority (i.e. Board level or reporting directly to a Board member) should have lead responsibility for corporate and health records management within the organisation. The model within each Health Board may differ dependent on local accountability. This lead role should be formally acknowledged and made widely known throughout the organisation.

27. The manager, or managers, responsible for the records management function should be directly accountable to, or work in close association with the manager or managers responsible for Freedom of Information, Data Protection and other information governance issues.

28. All staff, whether clinical or administrative, must be appropriately trained so that they are fully aware of their responsibilities as individuals with respect to record keeping and management, and that they are competent to carry out their designated duties. This should include training for staff in the use of electronic records systems. It should be done through both generic and specific training programmes, complemented by organisational policies and procedures and guidance documentation.

4.7 In terms of Policy and Strategy

29. Each NHS organisation should have in place an overall policy statement, endorsed by the Board and made readily available to staff at all levels of the organisation on induction and through regular update training, on how it manages all of its records, including electronic records.

30. The policy statement should provide a mandate for the performance of all records and information management functions. In particular, it should set out an organisation's commitment to create, keep and manage records and document its principal activities in this respect. It gives high-level guidance on managing the information lifecycle from creation to disposal. Key paragraphs are quoted below:

35. Records created by the organisation should be arranged in a record-keeping system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of information while having regard to security.

37. It is important that all NHS organisations train staff appropriately and provide regular update training. Training and guidance in record-keeping should be an integral part of the procedures, induction and ongoing training for each role.

38. Implementing and maintaining an effective records management service depends on knowledge of what records are held, where they are stored, who manages them, in what form(s) they are made accessible, and their relationship to organisational functions (e.g. Finance, Estates, IT, Direct patient care). An information survey or record audit is essential to meeting this requirement.

44. The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions. The record-keeping system should also address the management of emails, including aspects such as the titling of emails and the handling of email attachments.

45. Storage accommodation for current paper records should be clean and tidy, should prevent damage to the records and provide a safe working environment for staff.

48. When paper records are no longer required for the conduct of current business, their placement in a designated secondary storage area may be a more economical and efficient way to store them. Procedures for handling records should take full account of the need to preserve important information and keep it confidential and secure. There should be policies and procedures in place for managing the lifestyles of both paper and electronic records.

59. It is particularly important under Freedom of Information legislation that the disposal of records – which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed – is undertaken in accordance with clearly established policies which have been formally adopted by the organisation and which are enforced by properly trained and authorised staff.

60. The design of databases and other structured information management systems must include the functionality to dispose of time-expired records. Databases should be subject to regular removal of non-current records in line with the organisation's retention schedule.

68. Each organisation must have a retention/disposal policy that is based on the retention schedules referred to in paragraphs 57 and 58 of this Code of Practice.

72. A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the Records Manager, so that the organisation is aware of those records that have been destroyed and are therefore no longer available. Disposal schedules would constitute the basis of such a record.

In annexes E and F the manual offers guidance by way of a template for an NHS board's management policy for personal health records and its health records strategy.

Action required by whom/when: Chief Executives are requested to *"Implement, and ensure, that all appropriate staff are aware of and follow, the updated Code of Practice"*. The necessary arrangements should be made to inform primary care contractors about the contents of this letter.

5. References

Great Britain. Data Protection Act 1998. Chapter 29. London Stationery Office; 1998. http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1.

The same as you? A review of services for people with learning disabilities 2003 [cited 2008 Jul 29]; Scottish Executive. Available from http://www.scotland.gov.uk/Resource/Doc/159140/0043285.pdf.

NHS code of practice on protecting patient confidentiality 2003 [cited 2008 Jul 29]; Scottish Executive Available from http://www.confidentiality.scot.nhs.uk/publications/6074NHSCode.pdf.

Scottish Government Healthcare Policy and Strategic Directorate Records management: NHS code of practice (Scotland). CEL 28(2008). Edinburgh: Scottish Government; 2008. http://www.scotland.gov.uk/Resource/Doc/230203/0062364.pdf.

6. Conclusion

Important points raised in this Framework include the following:

- all NHSScotland users have the right to expect a safe and secure hospital environment;
- common concern for the security of people and property in the NHSScotland, the NHS being a large and diverse service with the need to be as accessible as possible making this a considerable challenge;
- wide ranging security issues to be addressed including dealing with violence and aggressive behaviour and incidents of physical assaults and abuse. The links to other areas such as major incidents, fraud prevention and risk management;
- recognition that many groups of staff are involved in security, both clinical and non-clinical;
- the need to put in place an infrastructure that allows staff to meet the security needs in an effective way that adapts with change and allows continuous improvements.

Appendices

Appendix A: Security Risk Management Standard

Appendix B: Guidelines for the reporting of crime

Appendix C: Guidelines for reporting non-crime incidents

Appendix D: Typical Job Descriptions

Appendix E: Basic Training for a Healthcare Security Officer

Appendix F: Glossary of abbreviations

Appendix A: Security Risk Management Standard

Purpose

To ensure that there is a safe environment and systems in place to protect patients, staff and visitors, their property and the assets of NHSScotland organisations. Staff should be aware that separate processes/procedures exist for fraud prevention, major incidents including terrorist threats and lockdown to protect against 'swamping' (i.e. overwhelming) of a department.

Lockdown is used to secure a building for example:

- it is carried out by security officers when work ceases or at specific times when healthcare premises are not 24 hours, 7 days a week. For example training departments, day surgeries, office complex and outpatients departments etc;
- in situations where an infectious outbreak arises and lockdown is applied to the ward areas to prevent future admissions;
- a mental health ward to prevent patients entering or leaving the ward area;
- may be necessary where demand for services outstrips availability and facilities for waiting e.g. A&E.

Swamping refers to situations where concerns are raised because there are too many people congregating in a particular area. Certain areas are locked down prior to opening and then opened up at intervals or depending on the number of people congregating, for example, in the event of an incident it also aids public/staff evacuation. In the NHS or public building context, the measure may be used for major incidents, terrorist threats etc.

Rationale

Patients, staff and visitors should be secure in the knowledge that they are in a safe environment, where a high priority is placed upon their well-being and security. Although responsibility for security management in NHS organisations rests with senior management, all stakeholders have a part to play in reducing the security risks. In order to develop effective policies and procedures it is therefore essential to have the support of all concerned and establish a culture that aims to prevent criminal activity and promote a secure environment.

Area for Assessment 1: Accountability

All Boards must nominate an Executive Director with responsibility for security. This role must be clearly defined with clear lines of accountability for security matters throughout the organisation, leading to the Board.

Guidance

The Chief Executive of the organisation has overall statutory responsibility for security management although an Executive Director will have accountability for controlling and co-ordinating security measures. In practice, direct responsibility for key tasks will be delegated to the Security Manager/Specialist and other identified and competent individuals e.g. risk managers, nurse managers and estate managers. Any delegated responsibilities and duties will need to be clearly defined and appropriate specialist training provided.

This standard requires that:

1. The duties of the nominated Executive Director are clearly defined within their job description.
2. There is Board level awareness of security issues.
3. NHS organisations should demonstrate that they have obtained adequate and appropriate levels of expertise and competence.

Area for Assessment 2: Accountability

All Boards must have a dedicated Security Manager or an individual with specific operational responsibility for all Board security matters. This postholder should be adequately trained and demonstrate knowledge and expertise.

Guidance

There should be a clear and direct communication line between the post holder and the nominated Executive Director.

This standard requires that:

1. There is a clear and direct communication line between the postholder and the nominated Executive Director.
2. The duties of the operational manager must be clearly defined within their job description.
3. Postholder should be trained and arrangements for continuous professional development should be in place.
4. Structured and clear lines of communication between the postholder, the estates department and the fire officer are established and maintained to enable building/physical security issues to be dealt with expediently.
5. There is evidence of clear communication between the postholder and all other departments/directorates.

Area for Assessment 3: Accountability

There is a Board approved security policy and strategy that has been communicated throughout the organisation and is supported by an agreed plan.

Guidance

The organisation should adopt a formal security policy and strategy and have a clear plan for implementing and communicating the policy and strategy at all levels within the organisation. An annual security report should be submitted to the Board that includes statistics and performance in meeting planned objectives.

The policy and strategy is required to:

- set out the intentions of the policy and strategy and the management committed to it;
- state exactly what the objectives are;
- identify how security will be assessed;
- recognise specific areas of risk such as Ambulance, A&E, Maternity and paediatrics, lone working etc;
- address how specific security risks will be tackled;
- identify how the policy and strategy will be communicated to staff and all relevant stakeholders e.g. Police etc and how communication will be maintained;
- address the requirements for security devices and equipment;
- set out the security accountabilities and responsibilities of individual managers and groups of staff;
- state how security fits with other organisational functions such as health and safety and internal audit;
- identify where to go for advice on security matters.

This standard requires that:

1. The organisation has adopted a formal security policy and strategy and has a clear plan for their implementation and communication. This covers the key areas of security risk including the protection of patients, staff and visitors, their property and the assets of the NHSScotland organisations.
2. The policy and strategy meets the needs set out above.
3. The security strategy looks to the future by containing robust reduction objectives for crime and other security related incidents.
4. Other policies and procedures exist and are disseminated to staff for:
    - suspected abduction of an infant;
    - major incidents;
    - vulnerable adults;
    - reduced access to wards with vulnerable patients – Special Care Baby Unit and Paediatrics;
    - reduced egress from wards with vulnerable patients – EMI, Paediatrics and Care for the Elderly.

Area for Assessment 4: Processes

A crime prevention programme is developed, utilising relevant risk assessments implemented and maintained throughout the organisation. In addition, specific crime prevention plans should be developed for sensitive/high risk areas such as A&E, Ambulance, Mental Health, Paediatrics, Maternity and Lone Working.

Guidance

Crime prevention is the cornerstone of a fundamental security strategy. Crime prevention programme documentation will cover operational practices required for all staff at all levels to implement the strategy. Where necessary, these will be area specific.

This standard requires that:

1. A crime prevention programme is produced, implemented and communicated to staff, patients and hospital users/stakeholders which will:
   - deter criminal activity where possible;
   - deny the criminal the opportunity and delay the attack if it happens;
   - detect crime when it happens.
2. All staff are involved in the crime prevention and security programme; their degree of involvement will depend on a training needs analysis.
3. Mechanisms are in place for ensuring all staff have a clear channel for communicating concerns, providing and receiving feedback and improving practices/procedures.

Area for Assessment 5: Process

There is proper and timely response to security incidents in accordance with appropriate response plans.

Guidance

The key to limiting the impact of any security related incident is for properly trained security personnel, or other persons with the recognised responsibility, to respond quickly and appropriately to a security incident. However, in order to ensure that a timely and effective response is possible, there must be a system in place.

This standard requires that:

1. The organisation's security response plans are based on the following principles:
   - respond effectively to an event and ensure it is fully investigated;
   - make available/communicate follow-up procedures and advice that provides for:
   - staff support;
   - media liaison;
   - counselling;
   - loss analysis;
   - prosecution/civil action;
   - disciplinary action;

- review and feedback.

2. The response plans are designed to enable the organisation to react effectively to ANY security incident and must include the following six key elements:

   - raising alarm, wherever appropriate, within Boards and the community;
   - initial response, involving: identifying type of incident, location and time, invoke the remedial action plan;
   - consolidation involving recording facts, informing senior management etc;
   - recovery involving continuing support, de-brief all involved, submit detailed incident report to appropriate authority etc;
   - restoration involving ensuring unit is working normally, restoring security arrangements;
   - review of existing plans where necessary.

Area for Assessment 6: Processes

Security hazards and incidents are reported and analysed in accordance with the process contained within the incident and Hazard Reporting Standard (Standard 3).

Guidance

An effective hazard/incident reporting system will help organisations identify problem areas where incidents are frequently arising and will help organisations to conduct robust risk assessments.

An incident can be defined as any event, which has given or may give rise to actual or possible personal injury, to patient dissatisfaction, or to asset or property loss or damage.

This standard requires that:

1. The hazard and incident reporting system for security purposes meets the following requirements:

   - complies with Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) and National Patient Safety Agency (NPSA) reporting requirements;
   - preferably uses one form for internal reporting of all incidents involving people, assets, property or money;
   - defines the type of incident which requires onward reporting to appropriate external agencies e.g. Police;
   - all incidents to be graded by severity;
   - investigations of all incidents carried out to determine underlying cause, trend analysis and subsequent remedial action and revision of process;
   - regular management reports should be produced which result in management action;
   - monitor continued effectiveness.

Area for Assessment 7: Processes

The risk management process contained within the Risk Management Policy and Strategy standard (Standard 1), and the Risk Assessment and Treatment standard (Standard 2) is applied to security risks.

Guidance

Risks can be systematically identified using a number of approached including:

- the review of inspection/audit reports;
- workshops with staff;
- use of compliance checklists;
- risk assessments.

This standard requires that:

1. Procedures are in place for security risks to be systematically identified, recorded and assessed on a continuous basis.

2. Risk management elements are in place to provide for the following:
   - all identified risks to be documented as part of a 'risk register' and systematically analysed and prioritised for action;
   - risk treatment plans to be developed and implemented (in order of priority and alongside other risk treatments which are necessary to deal with wider risks faced by the organisation, where appropriate) in order to minimise risk;
   - risks and the effectiveness of the implemented risk treatments to be monitored and reviewed on a continuous basis;
   - all relevant staff including senior management and the Board are to be informed of any significant risks and associated risk treatment plans;
   - all relevant staff, including those on fixed term contracts, and other relevant stakeholders to receive information on systems in place to minimise security risks;
   - where appropriate, staff training to be undertaken to reduce knowledge gaps.

Area for Assessment 8: Capability

The organisation has up to date security related legislation and guidance.

Guidance

Access to legislation and guidance is essential for the organisation to carry out its statutory duties imposed upon it by law and mandatory duties imposed upon it by the Scottish Government.

There are many sources of information on legislation and security related guidance.

Up to date guidance can be accessed through the Scottish Government Health Directorate at www.sehd.scot.nhs.uk and on the Department of Health database on www.dh.gov.uk. Other useful sites are www.hse.gov.uk and http://www.official-documents.gov.uk/

This standard requires that:

1. As a minimum, the organisation has access to key references listed on the front page of this standard, together with any additional references noted in the guidance associated with the criteria contained in this standard.
2. The Security Manager/Specialist with specific operational responsibility for Board security matters has a PC and Internet access.

Area for Assessment 9: Capability

All employees receive security training that is commensurate with the risks in their work area.

Guidance

Training is the essential foundation for reducing risk to personnel safety and for crime prevention, and needs to be targeted to all levels of the organisation to have maximum benefit. However, not every staff member needs the same training. Special security training will most likely need to be provided for certain staff, for example in maternity, A&E and children's services, mental health, ambulance workers and for lone workers where there is known to be heightened risk at the point of care.

This standard requires that:

1. Security awareness training is part of the overall training profile for all NHS staff.
2. As a minimum, general security awareness training covers areas such as those listed below and should be cross referenced with the Violence and Aggression passport scheme:
    - crime prevention practices;
    - management of violence and aggression;
    - security response procedures (proper timely response duties by staff);
    - use and management of security equipment;
    - incident reporting procedure
3. Security training is based upon the risk that a given employee will experience with a security incident in his or her work area, based on historical data and other factors, including the results of detailed risk assessments.
4. Basic crime prevention training should be provided which may include:
    - how best to protect patients, staff, carers, assets and property;
    - how best to guard against assault and theft of personal belongings and Board property;
    - what relevant staff/patients/visitors are expected to do to safeguard property belonging to patients;
    - when and in what circumstances to call the police;
    - the scale of the crime problem;
    - what is being done to reduce crime.

5. Specific and separate training is provided for staff on conflict resolution including management of violence, aggression and, where necessary, physical intervention techniques, as appropriate to their job requirements.

Area for Assessment 10: Capability

The competency and performance of security personnel, whether employed internally or out sourced, is monitored.

Guidance

In general, the duties of security staff may differ between organisations, as security sometimes fills other responsibilities. Thus, the competency and performance expectations for security staff should be assessed and determined for each unique organisation.

Where external contractors are employed, it should be noted that the Security Industry Act dictates that all persons working in the security industry will have to be vetted, licensed and trained. Further information can be obtained from the SIA website at http://www.the-sia.org.uk/

This standard requires that:

1. There are adequate screening and training procedures in place for the security staff who are employed by the organisation.
2. In accordance with personnel/health and safety/security policies, clear instructions on actions to be taken for all foreseeable events are available, and security personnel including external contractors are fully and appropriately trained to perform their duties. For example security staff must clearly understand their powers of arrest.
3. The competency and performance expectations of security staff are assessed and determined for each unique organisation. Security staff are then evaluated against competency requirements and performance expectations.
4. If an external contractor is employed to provide security services, the service contract clearly sets out:
    - screening procedures for all staff;
    - compliance with the working time directive;
    - uniform requirements;
    - duties and responses required;
    - training standards;
    - equipment requirements;
    - performance monitoring and record keeping;
    - call out procedures;
    - liaison with local police.

Area for Assessment 11: Outcomes

Key indicators capable of showing improvements in security management, and the management of associated risks, are used at all levels of the organisation, including the Board, and the efficacy and usefulness of the indicators is reviewed regularly in association with the Risk Management Committee.

Guidance

The organisation should utilise indicators to indicate that all stages of the security management process are being properly managed and risks are minimised. The organisation should monitor the key indicators developed for this standard as follows:

- level of compliance with the standard;
- RIDDOR – security reports;
- NPSA – Number of physical assaults on patients broken down by perpetrator;
- performance against training needs analysis for security training;
- number of incidents of non-physical assault;
- number of assaults on staff;
- number of security incidents reported;
- number of security incidents requiring police attendance;
- number of security incidents resulting in prosecution;
- number of thefts;
- number of rehearsals testing the suspected abduction of baby policy.

Note: These indicators although compulsory are not exclusive. The number of indicators devised should be sufficient to monitor the security management service and the efficiency and usefulness of the organisations own indicators, is reviewed regularly. Wherever appropriate, these indicators should be designed to demonstrate improvement in managing the risks associated with security management over time.

This standard requires that:

1. The organisation makes use of the compulsory indicators which demonstrate the improvement in services provided by the security management system.
2. Internal performance indicators have been identified or developed and are available for inspection.
3. Indicators are used and regularly reviewed and reported to the risk management committee via the usual reporting systems.

Area for Assessment 12: Monitoring and review

The system in place for managing security is monitored and reviewed by management and the Board in order to make improvements to the system.

Guidance

It is the responsibility of the Chief Executive and the Board to monitor and review all aspects of the security management system that the organisation has in place, and management information should be provided regularly to the Executive Board.

Boards should either use a recognised software system or develop one in-house that ensures clear data definitions and is adequate for performance monitoring and management purposes.

This standard requires that:

1. The nominated Executive Director will monitor and review all aspects of the security management system including:
   - accountability arrangements;
   - processes including risk management arrangements;
   - capability;
   - outcomes, including key performance indicators;
   - internal audit findings.
2. The Risk Management Committee and the Health and Safety Committee play a significant role in monitoring and reviewing all aspects of the system as a basis for establishing significant information that should be presented to, and dealt with by the Board.
3. The Audit Committee has reviewed internal audit findings at the appropriate intervals.

Area for Assessment 13: Audit

The internal audit function, aided as necessary by relevant security specialists, carries out periodic audits to provide assurance to the Board that a system of security management is in place that conforms to the requirements of this standard.

Guidance

Internal auditors, in collaboration with relevant security specialists and, where appropriate, others, should verify that a system of internal control exists with respect to security management.

Management should consider the range of independent internal and external assurance available, and avoid duplication and/or omission.

The adequacy of the independent assurance will depend upon the scope and depth of the work performed, bearing in mind its timeliness and the competency of the staff performing it. The level of reliance that can be placed on such assurances should consider, among other things, the professional standing of the assuror, their level of independence, and whether they could reasonably expect to provide an objective opinion.

It is important that any review that takes place results in a report, recommendations for action where necessary, and the retention of sufficient evidence to enable other potential reviewers to rely upon work already undertaken. The reports should be submitted to the appropriate sub-committee of the Board.

This standard requires that:

1. Internal auditors, in collaboration with the relevant security specialists and, where appropriate other verify that a system of internal control exists with respect to security management.
2. The level of independent audit carried out is based on risk, which will be determined principally by reference to assurances given by the security specialists.
3. Reports are presented to the Audit Committee and copied to the Risk Management Committee and any other relevant committee or group (e.g. specialist security, health and safety committee, etc.)

4. An annual internal audit statement is provided to the Chief Executive that sets out the audit work carried out for the year. Where the system in place for the security management has been audited, this is referred to in the statement.

Appendix B: Guidelines for the reporting of crime

B1: Details to include for the reporting of crime

Consider the inclusion of details of the following, as appropriate.

Details of Criminal Activity

- initial notification of the crime;
- scene(s) visited: day, date, time and person(s) seen;
- any enquiry made to trace a witness and outcome(s) including when a witness will be available for interview;
- any search made for missing property and outcome(s);
- any item preserved for forensic examination by Scene of Crime Officer (SOCO) and what instructions, if any, were given to staff at the scene(s);
- SOCO having attended, day, date and time along with result of forensic examination, i.e. finger marks lifted, impressions made of damage by jemmy or other implement;
- interview with suspect(s) and reason for elimination, or otherwise from enquiry;
- relatives or friends notified;
- assistance rendered to victim(s)/ victim support;
- step(s) taken to secure premises, property etc;
- CCTV tape(s) reviewed and outcome(s);
- any tape(s) handed to the police, with details of the police officer taking possession and log number;
- any crime prevention advice given;
- steps taken to prevent repetition of offence;
- any further action/enquiries regarding investigation delegated, and to whom;
- any manager supplied with 'losses and compensation form' (where a Board is the victim);
- why a 'No Crime' classification may have resulted;
- any additional relevant information.

Note: Remember to append details of any subsequent visit(s) to scene(s) when next on duty and the time spent on the investigation.

Additional requirements: Initial and subsequent investigation reports should be dated/timed, and the identity of all Reporting Officers involved noted. A hard copy of the full crime report should be produced for the security management.

B2: Guidance for crime classification

Crime Classification	Description
Assault **Menaces**	A crime at common law, and is every attack directed to take effect physically on the person or another, whether or not actual injury is inflicted. A form of assault; this is a threatening gesture inducing a state of bodily fear, such as someone threatening you with a knife.
Breach of the Peace	A crime at common law and is constituted by one or more persons conducting himself or themselves in a riotous or disorderly manner, to the alarm, annoyance or disturbance of the lieges.
Break-in (Housebreaking)	When a person enters a building or part of a building by the use of force as a trespasser with the intention of stealing, causing grievous bodily harm, raping any person or committing any criminal damage to any property.
No Break-in (Attempted housebreaking)	When a person enters a building with no sign of forced entry, as a trespasser with the intention of stealing, causing grievous bodily harm, raping any person or committing any criminal damage to any property.
Child Abduction	When a person, other than the parent, without lawful authority or reasonable excuse, takes or detains a child under the age of 16 years for the purpose of removing the child from the lawful control of any person having that control. Note: It is irrelevant whether the child consents.
Criminal Damage	When a person without lawful excuse: a) destroys or damages any property belonging to another, intending to destroy or damage it, or being reckless as to whether it is destroyed or damaged; b) destroys or damages his own property intending to destroy or damage it, or being reckless as to whether it is destroyed or damaged, and intending by the destruction or damage to endanger the life of another or being reckless as to whether the life of another would be endangered.
Fire-raising	Fire is 'set' or 'raised' whenever the property concerned has started to burn and some part of it, however small has been consumed. **Wilful** The crime of wilful fire raising is committed when a person 'intentionally sets fire' to any form of property. **Culpable and reckless** Is committed when property is set on fire as a result of a reckless act.
Forgery and Uttering	A crime at common law and consists in the making and publishing of a writing, feloniously intended to represent and pass for the genuine writing of another person.
Theft of Electricity Act 1989	Restoring a supply that has been cut off, damaging electricity plant, line or meter, interference with meters.

Crime Classification	Description
Reset	A crime at common law, committed by any person with intent to deprive the owner, to receive and keep property knowing that has been appropriated by theft, robbery, embezzlement or fraud.
Indecent Assault on Female	Over the age of 12, indecent assault is not a separate crime, but a form of common law assault accompanied by indecent circumstances. It has been held that any uninvited handling of the victim's private parts constitutes the crime.
Indecent Assault on Male	Over the age of 14, indecent assault is not a separate crime, but a form of common law assault accompanied by indecent circumstances. It has been held that any uninvited handling of the victim's private parts constitutes the crime.
Public Indecency	Where it constitutes lewd, indecent and libidinous practices and behaviour to an individual and where it causes public offence.
Kidnapping	When a person without lawful excuse takes or carries away another by force or fraud without the consent of the person taken.
Culpable Homicide	The unlawful killing of a person by another is subdivided into murder and culpable homicide, depending on both the intent of the accused and the circumstances of the case involved.
No Crime	In cases where a crime is alleged and is subsequently found to be based on incorrect belief, i.e. a reported theft of a pedal cycle that had in fact been borrowed by a friend, then the original report should be classified as 'No Crime'
Obtaining a Pecuniary Advantage	When a person by any deception obtains for himself or another any pecuniary advantage. Note: 'Deception' can be any act or words whereby a person is led to believe that something that is false is true. 'Pecuniary advantage' can be given the opportunity to earn remuneration or greater remuneration in an office or employment e.g. when an individual makes false statements on an application form or CV which if the employer had known were false would have meant the individual would not have been given the job. The Collins dictionary defines pecuniary advantage as: "*In Law-financial advantage that is dishonestly obtained by deception and that constitutes a criminal offence*".
Obtaining Property by Deception	When a person by the use of deception, dishonestly obtains the property of another with the intention of permanently depriving that person of his property. Note: 'Deception' can be any act or words whereby a person is led to believe that something that is false is true. Having accepted, they part with property.
Other (not listed)	In such a cause, there is the need for consultation with a Security Manager/Specialist for an additional crime classification to be included on the database as appropriate.

Crime Classification	Description
Possessing Offensive Weapon	When a person who without lawful authority or reasonable excuse, the proof of which lies with him, has with him in a public place an offensive weapon. **Note:** A public place will include any part of the healthcare premises that at the material time the public have, or are permitted to have, access. Offensive weapon means any article made or adapted for causing injury, or intended by the person having it for such use by him.
Putting a person in Fear of Violence	When a person by his/her conduct on at least two separate occasions, causes another person to fear that violence will be used against them, and the accused knew or ought to have known that such fear would be caused. Note: The conduct must be towards the same person on each occasion.
Rape	A crime at common law and consists of the carnal knowledge of a female by a male person without her consent.
Robbery	A crime at common law, committed by any person, who feloniously appropriates property, by means of violence or threats of violence.
Sending Dangerous Article by Post	When a person sends a postal package that encloses any sharp instrument intended to injure another who may open the packet.
Sending Obscene Material by Post	When a person sends a letter or article which conveys a message that is indecent, with the intention of causing distress or anxiety to the recipient or to another person to whom he intends that the message should be communicated.
Supplying Controlled Drugs	When a person supplies a controlled drug to another without lawful authority.
Theft of a motor vehicle or letting yourself be a passenger in a stolen motor vehicle	Section 178(1)(A) of the road traffic acts states that a person who takes and drives away a motor vehicle without the consent of the owner, or other lawful authority shall be guilty of an offence. Section 178(1)(B) of the road traffic act states that a person who knows that a motor vehicle has been stolen, drives it or allows themselves to be carried in or on it without consent or authority, shall be guilty of an offence.
Theft of a pedal cycle or letting yourself be a passenger on a stolen pedal cycle	Same as above
Theft (by an Employee)	When a person steals from his employer.
Theft (of Mail)	When a person steals any article of mail. The mail does not have to have any value attached to it and can be internal or external.
Theft (Shoplifting)	When a person steals property belonging to a shop from within the public area of the shop premises.

Crime Classification	Description
Theft – (from Automatic Machine or Meter)	An overcoming of the security of the lock fast place and unauthorised appropriation of property from within intent to deprive the owner
Theft – (from Vehicle)	An overcoming of the security of the lock fast place and unauthorised appropriation of property from within intent to deprive the owner
Theft – (miscellaneous)	An overcoming of the security of the lock fast place and unauthorised appropriation of property from within intent to deprive the owner
Threat to Commit Criminal Damage	Breach of the peace
Threats to Kill	Breach of the peace
Unlawful Possession of Controlled Drugs – Intent to Supply	Produce a controlled drug, or to supply or offer to supply a controlled drug to another.
Unlawful Possession of Controlled Drugs – Own Use	It is an offence for any person to have a controlled drug in their possession without lawful authority. The amount of drugs the person has possession of is immaterial.
Uttering Counterfeit Currency	Comes under Forgery and Uttering

B3: Modus Operandi

Consider the inclusion of details of the following, as appropriate.

Modus Operandi
Each criminal records office maintains a register of the Modus Operandi or method(s) used by criminals to commit crime. The method used is indexed under and up to 10 points in the register. The more that is known about how the crime was committed, the greater chance there is of identifying the culprit by comparing how he/she committed the crime in relation to other crimes committed in the same fashion.

Use of the 10 points of the register to cover the method:

1. **Class word:** The class of person or property attacked, (hospitals, doctor's surgery etc).
2. **Entry:** The point of entry to the premises (skylight, window, through the roof etc).
3. **Means:** The means used to gain entry (forcing entry with instrument, smash and grab, con trick).
4. **Object:** The motive for the crime or property stolen (sex, jewellery, cash, drugs etc).
5. **Time:** The hour, day, date and associated details, e.g. public holidays, hours of darkness.
6. **Style:** The criminal's alleged trade or profession.
7. **Tale:** The story told by the criminal accounting for his/her presence at the scene of the crime.
8. **Pal:** Was there more that one person involved in the crime, if so how many?
9. **Transport:** How did the criminal arrive at and leave the scene of the crime?
10. **Trade Mark:** Was there anything peculiar or unusual done at the scene of the crime? Use of the toilet, consumption of food graffiti?

Appendix C: Guidelines for reporting non-crime incidents

C1: Details to include in the reporting of non-crime incidents

Guidance notes for the details to report on all categories of non-crime incidents.

Note: Fire-related incidents are dealt with separately.

Be brief,

1. The day, date, time, and place the incident was reported, along with full details of who/how reported to security.
2. What happened and why.
3. Steps taken to trace witnesses. The details of witnesses and a verbatim account from them of the incident.
4. Details of injury to any person(s), where treated and by whom (including first aid). The time an ambulance was called.
5. Details of any damage to Board or private property. Details of the owners of any damaged property.
6. Action taken by a security officer to alleviate any problems, including:
   - informing estates and maintenance department;
   - securing the area;
   - providing assistance;
   - any advice given, etc.
7. Police assistance requested (non-crime)? The police were called and the time of arrival, details of Police Officers along with any police action taken or advice given.
8. Management informed? Departmental Management and/or Security Management. The delegation of any further action and to whom.
9. Full details of property, receipt numbers and other similar references.
10. CCTV tapes reviewed; tape numbers and details.

Supplementary guidance notes for the details to report on fire-related incidents can be found in NHS HDL (2005) 53 Fire Safety Policy for NHSScotland.

C2: Categories for non-crime incidents

Guidance on categorisation for non-crime incidents that should be recorded.

Category	Sub-Category
Access/Egress	Non residential
	On-Call Rooms
	Residential
Accidental Damage	Accidental Damage
Activism Indicators	Demonstrations
	Graffiti
	Leaflets
	Letters
	Posters
	Telephone Calls
	Other
Baby Tagging Alarm	Activated in error
	Fault
	Test
	Incident/Crime
Cash Reconciliation	Monies paid in by Security to Cashier
	Other
Civil Disputes	Between Members of Staff
	Between Patients and Visitors
	Between Patients or Visitors and Staff
	Contractors
	Retail Outlets
	Other
Cleaning Problems	Dirt
	Rubbish
	Spillage
	Other
Complaints of Noise	Loud Speaker
	Noisy Party
	Radios
	Verbal
	Other
Complaints to Security by Public	About other Staff/Department
	About Security Service
	About Security Staff
	Other

Category	Sub-Category
Complaints to Security by Staff	About other Staff/Departments About Security Service About Security Staff Other
Dangerous Waste/Debris	Building Material Chemical Waste Clinical Sharps Other
Disturbances	Abusive Patient to Staff Abusive Staff to Staff Abusive Visitor to Staff Excessive number of Visitors Physical Violence Patient to Staff (NON CRIME) Physical Violence Staff to Staff (NON CRIME) Physical Violence Visitor to Staff (NON CRIME) Other
Escorts	Cashier – Private Patients Cashier – Trust Catering Patient Affairs Personal (on request) Pharmacy Other
Estates and Maintenance – General	Broken windows Dangerous Roads/Footpaths Dangerous Structures Defective Lighting Door Security Unprotected Hazards Vehicle Access Systems Other

Category	Sub-Category
Fire *Please note the requirement for the Fire Officer/Fire Safety Advisor to be notified in all fire incidents/false alarms for specific fire reporting procedures to be followed.*	Alarm Activated – Contractor's/Workman Negligence Alarm Activated – Staff Carelessness Alarm Activated – Reason not known Damage to Fire Alarms/Equipment Faulty Alarm Panel Faulty Alarm Sounder Faulty Fire Fighting Equipment Fire Alarms Disconnected for Maintenance Fire Escape Routes Obstructed Fire Prevention Advice Interference with Alarm Smell of Burning Test/Drills Other
High Security Key Pouches	High Security Key Pouch
Infected Areas	Infected Area
Intruder Alarm	Activated – Cause Unknown Activated by Staff Accidentally Activated by Trespasser Activated by Workmen/Contractors Fault Test Other
Lifts	Alarm Activated – Mistake Failure – No Person Trapped Failure – Person Trapped False Alarm Routine Checks of Alarms/Telephones Other
Major Incident Alerts	Major Incident Major Incident – Standby Only
Medical Gas Supply	Failure Low Warning
Miscellaneous Incidents	Miscellaneous Incidents
Missing Patients	Missing Patients
Panic Button Activated	Fault In Error Incident/Crime Test

Category	Sub-Category
Patients Property	Property Deposited in Drop Safe Property Recovered from Cashiers Store Property Recovered from Drop Safe
Pay and Display Ticket Machines	Cash Collection Clock Adjustment Maintenance/Repair Visit Minor Fault Clearance Ticket Replenishment
Persons Collapsed	Patient Staff Visitor
Persons Smoking in Prohibited Areas	Patient Staff Visitor
Premises Security	Insecure Premises Routine Patrol Special Patrol
Property	Found Property Lost Property Restored Property Valuable Property Pouch Opened/Sealed
Stray Dogs	Stray Dog
Substance Abuse	Discarded Drug/Wraps Disposal Witnessed Paraphernalia Found Patients in Possession of Unlawful Drugs Pharmacy Escort Posters/Graffiti Other
Suspect Packages	Left Unattended Through Royal Mail – X-Rayed Other
Suspicious Persons	Questioned Satisfactorily Search No Trace Other

Category	Sub-Category
Traffic Management	Contractor's Diversion Exemption of Clamping Fee Obstruction by Vehicle Pay and Display Sign damaged/Missing Traffic Accident Traffic Sign – Damaged/Missing Trolley Wheels Used Other
Trespassers	Cab Tout Exclusion Order Issued Hawker Mischievous Children Vagrant/Drunk Other
Utilities Problems	Access Control Alarms C.C.T.V Electricity Gas IT Network Pagers Security PC Telephones

Appendix D: Typical Job Descriptions

D1: Typical Job Description for a Security Manager

1. Job identification

Job Title: **Security Manager**

Responsible to (insert job title): **Facilities Director**

Department(s):

Directorate:

Operating Division:

Job Reference:

No of Job Holders:

2. Purpose: To fulfil the role of manager for the Security Department of……..., ensuring that hospital premises are protected against theft and damage and a safe, secure environment is provided for patients, staff and visitors.

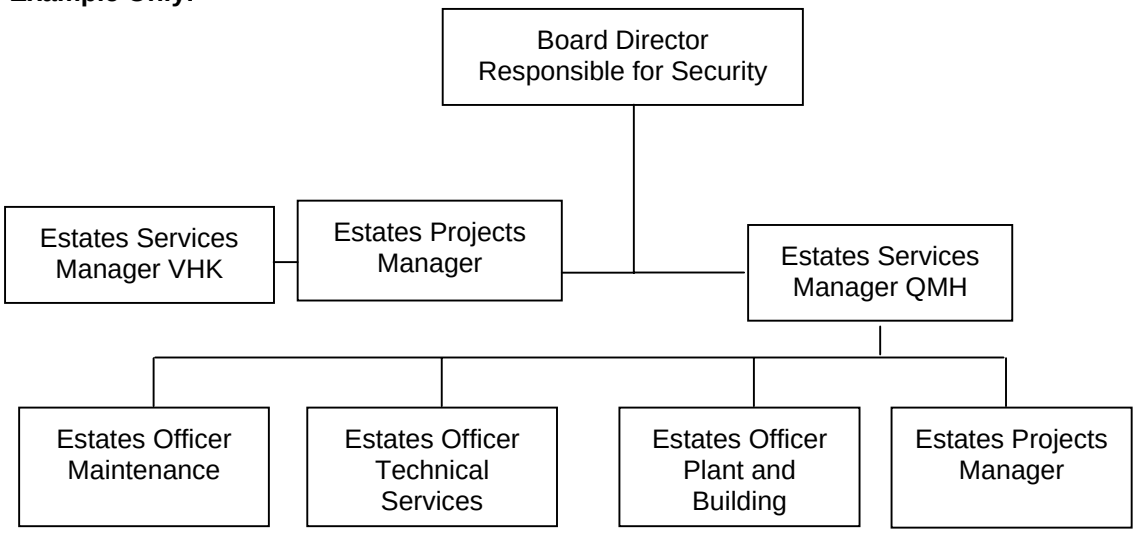
3. Dimensions: The post holder manages Security at ……Service level agreements with Primary Care Division account for a security service being provided to clinics, health centres within the …… area.

Directly employed staff total ….WTE consisting of … Charge hands and … Security Officers.

The revenue budget for wages and salaries is £…….. In addition there is a budget of £… for supplies and services.

4. Organisational Position

Example Only:



5. Role of Department: The Department provides an integrated 24 hours a day security services to the Acute Division ensuring that all the hospitals in the Division can provide healthcare in an environment free from the risk of crime, violence or disruption.

The services include:

- identifying and minimising security risks;
- maintaining a capability for immediate response to calls for assistance;
- operating an identity badge system;
- designing and delivering crime prevention and reduction initiatives;
- investigating security incidents;
- operating and maintaining CCTV recording equipment;
- delivering training on induction and other courses;
- working in partnership with Police, …….. Council and other agencies;
- conducting Crime Prevention Briefings and medical department security training;
- investigate formal complaints from the general public and staff alike;
- investigate recovery claims from staff and public;
- management of traffic flow and car parking.

6. Key Result Areas:

- manage the tactical deployment of security staff and equipment to ensure resources are targeted at the main areas of risk throughout the Acute Division;
- conduct ongoing security reviews to identify weaknesses, developing policies and procedures to ensure a secure safe environment for patients, staff and visitors;
- assist the police and other agencies in the investigation of crime by providing CCTV recordings and any other information which can identify suspects and lead to the recovery of property;
- participate in the Estates Data risk management group to identify and minimise health and safety risk;
- initiate regular communication and dialogue with other agencies and organisations to obtain the best advice on crime prevention and reduction;
- organise and chair the Hospital Watch meetings to identify local security issues and ensure that these issues are quickly addressed;
- identify security training needs for all staff and develop training schemes for staff induction, statutory training days and individual department needs so that staff can develop an understanding of personal and wider security procedures;
- manage car parking and traffic flow throughout the Acute Division and develop initiatives that can improve travel to and from the various hospital sites and ensure the free movement and unhindered access for Emergency Service vehicles;
- continually appraise Intruder Alarm and CCTV systems to ensure that they are well maintained and are providing maximum coverage to vulnerable property;
- administer personnel policies and procedures in respect of discipline, training, sickness, grievance and recruitment to ensure fairness and equity to all staff;
- play a leading role in the Health Board's Zero Tolerance initiative so that staff, visitors and patients are made aware of the types of behaviour deemed unacceptable within the Health Service;
- produce an Annual Security Report for the Executive Team which highlights statistically, the work of the Department over the year, numbers and types of incidents dealt with and recommendations for developments;
- play a leading role in the Board's Lone Worker Policy group to ensure policies are produced to ensure the safety of staff required to work in isolation;
- co-ordinate Emergency Evacuation procedures so that areas can be evacuated quickly in the event of fire or other serious situations;

- co-ordinate security measures in the event of a major incident as part of Emergency planning procedures;
- managing separate security department on fully operational hospital sites within Acute division, looking at individual security needs whilst investigating ongoing difficulties;
- responsible out of hours for further hospital/teaching locations, dealing with general security and investigations;
- responsible for all security matters linked to staff accommodation off site;
- investigate complaints and insurance claims from staff and public;
- conduct in-house and statutory training events;
- carry out police/security clinics on the hospital sites, raising security awareness and crime prevention to staff groups;
- responsible for overseeing contractual equipment arrangements, for the testing of alarms and control of access cards to departments;
- advise users on security equipment and oversee on their behalf, installation and commissioning;
- prepare, issue and evaluate tenders for the provision of security services within the department(s) budget;
- keep up to date with best practice and government guidelines in all aspects of security;
- responsible for the control assurance for security, working towards full compliance.

7. Equipment and Machinery:

Technical applications as follows:

- BM 5000 secure badge maker;
- Wintex access control;
- e-mail;
- Moresman Electronic security system;
- fire alarm system swipe and barrier card access control system;
- CCTV recording/monitoring and CD production;
- internal communication systems and radio network operations.

8. Systems:

Operating a complex computer based security identification system and the production of ID cards with the addition of swipe access. Other systems:

- Wintex access control;
- digital camera operation and retrieval system;
- radio communications system;
- mobile phone network;
- internal phone system;
- pager;
- computer for word processing, spreadsheets and presentations.

Production of manual records such as:

- training records;
- leave records;
- sickness records;
- personnel records;
- disciplinary/ investigation records;
- time sheets and wage returns;
- minutes of project meetings;
- project work records;

- security updates for onward dissemination;
- producing business reports for ongoing projects;
- introducing parking restrictions and traffic flow assessments and reports;
- generating information for press release;
- maintaining accurate incident and investigation reports for line Managers;
- maintaining equipment registers;
- the ordering, purchase and distribution of uniform whilst keeping within uniform budget;
- maintaining the Hospital Art collection, keeping a digital record of all items whilst updating the Art catalogue.

9. Assignment and Review of Work: All day to day work is self generated, as a result of the continual analysis of the service provided, so that high levels of quality and standards are maintained. The postholder continually assesses and adjusts existing procedures and performance to ensure that resources are properly targeted and used efficiently.

Long term plans and strategy are discussed with the manager and approved before implementation.

The postholder's work is reviewed regularly, by the immediate Manager, through meetings and reports on all security services matters. On critical corporate issues, the post holder can report to the Board Director.

10. Decisions and Judgements: The postholder works with a high degree of autonomy on a daily basis and reacts and assesses situations, resulting in precise decisions being made which fall within current strategies, policy and procedures. Decisions, when made, are based on fact, experience and good judgement and are essential to ensure that the department promotes good practice in all security matters.

11. Most Challenging/difficult parts of the job: Co-ordinating all security efforts across …… Acute Hospitals whilst providing additional security services to Primary Care and the School of Midwifery.

Prioritising a wide variety of needs within available budgets and time restraints.

It is also challenging to manage normal workload while dealing with a large quantity of phone calls, e-mails and letters from members of the public and staff who raise issues regarding security.

12. Communications and Relationships:

Internally:

- the Chief Executive, on various matters such as security or hospital policy;
- main Board Director responsible for Security;
- all Directorate Managers, personal briefing about incidents and or difficulties suffered by the security department;
- Estates Services Manager on all sites, looking at security matters in general, car parking, budget and tasks observations and concerns and future security needs;
- all department managers who need guidance in security matters;
- NHS staff when a complaint has been raised or concerns about security/parking arrangements;
- cashier, escorts service to and from the bank;
- shop staff and perceived threat levels;
- café staff and their perceived threat level;
- domestic supervisors and portering managers regarding breaches in security and operational procedures;
- security staff meetings to discuss matters of concern, training issues, course, general health, equipment, procedures, leave sickness, annual leave, general security practices;
- legal department, re legal matters and investigations;

- catering department, theft investigations and ongoing security review;
- nursing and medical staff on all sites;
- emergency planning officer, examining procedure and strategy and the use of security;

Externally:

- police, Fire and Prison service. Looking at procedures and security related incidents;
- community Police team, running a Police and security clinic on site for staff, patients and visitors to the hospital;
- security company engineers when new installations are installed;
- the general public/patients, when they need clarification or wish to make a formal complaint be it verbally or by report;
- security companies supplying training facilities;
- council departments looking at traffic flow and parking;
- bus company, looking at H&S when on site;
- delivery companies, supplying the hospital, reacting to concerns raised by them;
- traffic wardens and illegal parking on site;
- external security company providing additional manpower when required to do so.

13. Physical, Mental, Emotional and Environmental demands of the job: Dealing with various forms of communication has a physical and mental effect when attempting to dealing with a number of issues all at the same time.

The ability to compile accurate reports for the Executive team and also to the courts on criminal matters

Communicating and briefing large groups of NHS staff, on a weekly basis.

Controlling all security projects across all Acute sites is mentally demanding due to the nature of the problems encountered which being constant and varied.

Supporting staff in internal complaint procedure which is mentally and emotionally demanding.

Dealing with abusive offensive patients and visitors to the hospital.

Dealing with internal staff on staff complaints which are mentally demanding.

14. Knowledge, Training and Experience required to do the job:

Minimum required to undertake the role.

Qualifications

A Higher National or equivalent in Management

An appropriate Security Management Certificate

Comprehensive training in current digital security systems

Appropriate Training qualification

Experience

An experienced investigator with a good working knowledge of the law.

Experienced in project management.

Experience of working with small operational departments.

Experienced in dealing with violent and abusive offenders.

Experience in staff training.

A separate job description will need to be signed off by each jobholder to whom the job description applies. Job Holder's Signature: Head of Department Signature:	 Date: Date:

D2: Typical job description for a Security Officer

1. Job Identification:

Job Title: **Security Officer**

Responsible to (insert job title): **Security Manager**

Department(s): **Security**

Directorate: Operations

Operating Division:

Job Reference:

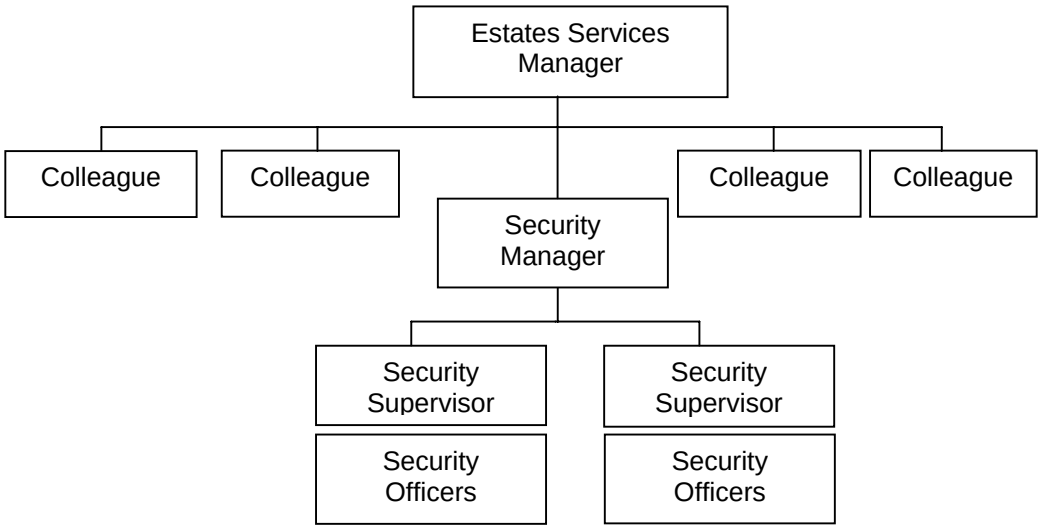
No of Job Holders:

Last Update (insert date):

2. Job Purpose: To provide a safe environment for patients, staff and visitors which is free from crime and the risk of fire, achieved through routine patrols and the investigation and careful inspection of incident and complaints as received from staff and the general public.

3. Dimensions: To provide a service which is customer focussed, requiring Security officers to interact with and recognise the needs of the NHS workforce which it serves. It is a necessary requirement for security officers to have the ability to deal with the general public and have the interpersonal skills to resolve difficult demanding scenarios and have the confidence to put people at ease or deal with matters in a more robust fashion.

4. Organisational Position:
Example Only:



5. Role of Department: The role of the security department is to maintain security throughout the Hospital by means of CCTV monitoring and recording, the issuing of computer generated security identification badges and the strict control of authorised access systems. Securing departments and buildings throughout. To conduct foot and mobile patrols of the main Hospital complex and car parks plus the patrolling and monitoring of satellite medical facilities within the community. To identify and assist all staff patients and visitors.

6. Key Result Areas: Speak on a daily basis with Charge hand or Security Manager to accept duties and exchange crime intelligence. Consult on a needs basis with Fire Adviser and Facilities staff on matters relating to building repairs and concerns, fire prevention and unhindered egress through emergency exits.

The post holder is constantly in discussion with various department Managers such as Pharmacy, Hospice, Community Hospital, Nursing College Hospital staff as part of the service, giving support and first line advice and assistance.

Security Officers maintain a high profile within the hospital and its grounds, being seen as a source of information and direction aiding all those needing the guidance, reassurance and assistance.

Providing physical assistance to hospital staff when requested to a difficult demanding situation which at the time has been deemed as confrontational and potentially physically damaging. Security officers provide the following at times of need:

- being at hand when nursing staff and doctors find themselves in vulnerable situations when dealing with patients and their families who have been emotionally effect by events or news;
- patient or visitor engaging staff in verbal or physical confrontation through human nature reasons.

They are required to placate difficult individuals by communication or with physical restraint whilst providing a protective cover to staff in difficult demanding situations. This is primarily achieved due to the Security Officers vast experience in human nature and individual habits

- Officers are fully trained in Violence and aggression training;
- first aid;
- fire Trained.

A full Security Escort Service is provided for staff and visitors alike to and from the hospital car parks and buildings within the grounds.

They are required to hold keys to various specialist departments including the restaurant and cashiers and are on call to secure and open said locations. The also have a responsibility for key safety and the issue to appropriate individuals.

The maintenance of the Hospital Key register and subsequent re issue of keys as required.

They are required to allow access out of hours to various companies.

The monitoring, detection and reacting to emergency alarm systems or incident within the hospital and its grounds. Alarm activations such as:

- department alarm systems;
- personal alarm activation;
- telephone alarm activations;
- fire alarm activation;
- phone call from distressed person.

Playing a pivotal role with the Fire and Police Service, providing physical or electronic assistance to incident and ongoing investigations such as:

- reacting to the fire alarm activation, by viewing the digital reader;
- locating the fire point or disturbance;
- escort Fire/Police service directly to the point of concern;
- providing Fire/Police service with internal communication systems;
- providing a cordon for emergency services;
- Security Officers are trained in basic life support in case of emergency.

Receiving and acting upon complaints, be it criminal or other, followed by active investigations, conducted in close cooperation with the local police authorities and hospital staff and visitors:

- confronting and calming the victim;
- conducting a full search for the offender(s);
- confronting the offender(s) or identifying and monitoring offender(s) which may be single or large groups disturbing or upsetting staff and patients;
- detaining the offender(s) until handed over to appropriate authorities;
- recording all details and compiling reports for onward transmission to the appropriate authorities.

Maintain the flow of traffic within the grounds of the hospital for all vehicles especially emergency vehicles:

- standing for long periods at times in adverse weather conditions, directing or stopping drivers from manoeuvring their desired driving course;
- placing bollards and security tape in areas where events or larger vehicles need to be parked i.e. MRI vehicle and maintaining the area until occupied.

Enforcing the policies of the hospital. The interviewing of staff and preparation of written reports and documents for follow up enquiry and investigation:

- enforcing the no smoking police;
- focussing on the illegal parking issues throughout the hospital;
- confirming general security issues about the hospital.

To investigate reports of missing patients, requiring a detailed logical physical search of the immediate area followed by a wider sweep whilst maintaining communication with the department and also the Police. Only to be concluded on the authority of the police or when the missing patient returns.

To play a major role in the evacuation of wards staff and patients due to fire or other hazard.

Assisting patients/visitors who have found themselves lost within the grounds of the Hospital complex.

To maintain a high profile uniformed presence in at risk areas to deter offenders and support vulnerable staff working quickly and efficiently with a minimum of supervision.

Security Officers when attending become an instant target simply due to their distinctive uniform, which is a vital part of the job.

Engage in the transit of monies between hospitals and external banking facilities along with accompanying medical staff in the movement of drugs between Pharmacy and the hospice to deter theft.

Complete both written and computerised records of security and fire incidents to provide statistics data.

Liaising and supporting Estates personnel:

- assisting Estates staff on issues about the hospital;
- giving physical support when events require it.

Providing security cover in the event of a Major incident or as a result of a Terrorist Attack. This support is in line with Emergency planning direction. Setting up cordons, directing staff and visitors away from secure and contaminated areas and closing down the hospital.

To ensure that all departments are secure and to investigate breaches of security when discovered.

Provide a guide service to specialists (Non medical) attending the hospital.

Provide a security presence when departments are open out with normal working hours due to maintenance or other reasons.

Provide a security presence when departments are open out with normal working hours due to maintenance or other reasons.

To routinely check fire appliances/hydrants across the hospital complex.

Maintain the flow of traffic with in Hospital grounds, which require the direction to drivers and the issuing of information notices to vehicles left unattended and illegally abandoned.

To provide escorts throughout for visitors, fire and police and prison service.

To assist in the sighting and guarding of visiting medical facilities such as the MRI Scanner Training units to the hospital.

Provide security cover and assistance to the Police when VIPs visit the hospital.

Provide electronic evidence to Police when requested.

To provide mobile support, responding to alarms from external NHS sites around the region and also accommodation units.

To accept deliveries into the hospital out of hours.

To conduct enquiries relating to contractors operating at the hospital.

To discourage drug addicts from entering the hospital.

Maintain observation in areas frequented by drug addicts, to ensure the area is clear of syringes and other drug paraphernalia, which being harmful to others. Investigating Fire appliance abuse.

Escort Fire officers on routine checks along with providing an escort to Trainee Fire Fighters on a site familiarisation exercise, requiring an extensive knowledge of the hospital and facilities.

7a. Equipment and Machinery:

Mobile patrols are undertaken by a dedicated vehicle. Computer applications include:

- BM5000 badge maker;
- Wintex access control;
- e-mail;
- windows based access control system and security incident report system;
- the computerised MORSEMAN security system;
- CCTV and monitoring equipment is used on four sites for which the Security Officer is responsible;
- charge hands must be able to operate computers and have a capacity to assimilate new applications;
- fire alarm systems;
- swipe and barrier access control systems.

Security Officers must have a working knowledge and understanding of the Hospital's fire alarm system, coupled with an accurate knowledge of the Hospital layout; this includes all fire procedures and fire point locations. Officers are required to check that all fire point is fully equipped and serviceable during their duty period. All fire alarms have to be attended and full fire reports compiled.

7b. Systems

Operating a complex security identification computer based system and the production of ID cards with the addition of swipe access. Officers are also required to have a very good understanding of the Wintex access control system while understanding and using the NHS intranet and messaging systems.

Full working knowledge of digital camera.

They are expected to complete time sheets and forward them to the Charge-hand for checking and onward transmission.

They are required to maintain all security logs and associated security monitoring systems and checks which are carried out regularly throughout their duty period.

8. Assignment and Review of work: Security Officers are given tasks to complete by the Security Manager, after which a full de-brief is carried out focussing on all aspects of the task and its results. The main aim is to identify and to take from the task, better skills and procedures which are then incorporated into future operations. Meetings are held as follows:

- one to one with Manager;
- manager and charge hand and security officer;
- manager holds section meeting to discuss matters of security.

Security Officers do conduct investigations into matters resulting from unrelated enquiries. They are encouraged to identify weaknesses in the day to day running of the Hospital in terms of security and make informed suggestion to rectify the situation. Assignments are given out on a weekly basis after which all areas are examined.

9. Decisions and Judgements: Security Officers are expected to make calculated decisions based on fact, judgement and detail known at the time this is carried out on a daily basis as swift decisions are required by a demanding work force. It is commonplace for the Security Officer to liaise with the night time Hospital coordinator. Security Officers play a recognised role in decision making, be it instant or advisory especially when lives are at risk through fire or other hazards on the Wards.

As part of the security policy, all incidents have to be reported to the line Manager, giving not only a written account, but also a full debriefing explaining in detail all actions, and decisions.

They have to make instant decisions, based on knowledge, judgement and written directions from manager.

They are required to investigate crime and, if required, make decisions regarding who to inform and when.

Security Officers make daily decisions in accordance with training and written instruction to call for Police assistance:

- when to issue security identification;
- when and to whom to issue keys;
- when to involve other member of staff.

10. Most challenging/difficult parts of the job: Dealing with a patient who is either Drug or Alcohol dependant and, who due to their condition, are extremely violent, and whose violence level is such that physical restraint is a necessity, simply to remove the potential threat to nursing staff, patients and visitors alike;

- physical restraint means taking hold for long periods of time until either the person is calmed or they are handed over to the Police which can be for long periods up to one hour;
- offensive and scathing verbal abuse which is regularly directed at security, nursing staff, visitors and patients alike has to be controlled and removed; this is carried out by Security Officers who, through experience, have developed a unique ability to resolve such matters, removing the problem, and dealing mentally with the situation.

11. Communications and Relationships: Security Officers are required on a daily basis to liaise with the Charge hand or Manager to examine set duties procedures, exchange criminal intelligence and current investigation and training needs. Consult on a regular basis with fire advisor and facilities staff on matters relating to building repairs and general building concerns such as Health and Safety issues fire prevention and maintenance of access through emergency exits across the site

Security Officers are required to operate a number of communication systems to ensure that they are contactable at all times.

- radio communication;
- mobile phone;
- internal phone system;
- pager.

They patrol on foot all internal areas along with external, during which they liaise with all departments confirming their presence, giving assistance and direction if required, whilst reacting to calls for immediate assistance. At these times security advice is given and explained.

Fostering good relationships will staff and patients alike.

Liaising with Police, Fire and Ambulance staff during incidents and events, requiring action whilst attempting to prevent further problems. Assisting police on ongoing criminal investigations along with the detention of criminals found on site. Recovering CCTV footage through electronic transfer onto disc for court use. Attending and giving evidence at court in criminal cases.

Possessing the ability to communicate with either difficult or violent patients/relatives, defusing the situation to a workable conclusion. Able to convince through understanding, confused patients back to their respective wards without putting them in fear or causing further unrest.

They regularly attend court to give evidence.

They are required to assist in producing accurate statements for defence and prosecution.

12. Physical, Mental, Emotional and Environmental demands of the job: Security Officers are expected to deal with, at times, violent and physically/verbally demanding incidents to ensure staff, patient and visitor safety. This type of situation where physical restraint is required puts a heavy physical demand on Security officers who have to restrain violent offenders for long periods.

When dealing with violent and aggressive individuals and then empathising with victims, the emotional impact is very high.

They regularly deal with patients who have become disorientated through their medical condition who at the same time may become violent. The physical, mental and emotional effect on the Security Officer can become immeasurable.

They have to demonstrate a high level of vehicle driving competence whilst patrolling NHS sites and roads between locations.

They have to deal with all forms of communication simultaneously which is mentally and emotionally taxing.

They are required to patrol all external areas regardless of weather conditions. They are also expected to patrol areas such as boiler houses and roof space of the hospital both of which have their own hazards.

They have to be able to compile accurate precise reports for onward transmission to Police and Court which also have to be on time and relevant to the subject matter, which has a psychological effect on the officer.

They are required to be constantly on the move throughout the hospital irrespective of inclement weather and conditions.

Accurate reports are required irrespective of time or event, which has an effect on one.

13. Knowledge, Training and Experience required to do the job: Security Officers must have experience and knowledge of restraint and defence coupled with the ability to communicate with difficult individuals in the hope of removing the threat before violence is experienced.

They must be willing to undergo training in violence and aggression training, if required.

They must be able to communicate at all levels whilst dealing with difficult situations.

They must be able and willing to operate computerised systems.

They must have a working knowledge of the law especially when dealing with violent and aggressive individuals.

They must have a driving licence and be able to drive.

They must be prepared to attend further training when required to do so.

They must be willing to operate between hospital sites.

They may be required to work at short notice in a National Emergency Situation.

They must demonstrate a flexible working attitude.

They must attend a First Aid course.

Appendix E

Basic training for a Healthcare Security Officer

The following table provides recommendations for what is considered to be the essential elements of a basic training programme for a Healthcare Security Officer. These elements have been grouped into the relevant topic areas for a modular approach to training provision, along with their recommended time allocation.

Topic Areas	Hours
Introduction to Hospital Security	
Security as a Service Organisation	2
Hospital Organisation	1
Relation with staff organisations	1
Hospital vulnerabilities	1
Sub Total	5
Security's Role in Hospital Operations	
Nursing Units	1
Administration	1
Pharmacy	1
Support Services	1
Maternity Units/Anti Infant Abduction measures	2*
Child Protection issues	1
Accident and Emergency Department	1*
Lost and Found Property	1
Missing Patients	1
Sub Total	8
Developing Communication and Investigative Skills	
Resolving Informal Complaints	1
Conflict resolution	4
Management of aggressive behaviour	2
Communication skills	1
Handling the Disturbed Patient, Visitor, Employee	2
Psychiatric Patients	1
Patrol Procedures/Techniques	2
Use of Note Books and Report Writing	2
Computer Procedures	4*
First steps at the scene of a crime	2
Investigations	3
Interviews	1
Courtroom and Prosecution Procedures	1
Rules of Evidences	1

Topic Areas	Hours
Developing Communication and Investigative Skills (continued)	
Sub Total	23
Protective Measures	
Lock and Key Systems/Access Control	1
Physical Security Controls	1
Alarms	1
Crime Prevention/Property Marking	1
Equipment usage/Maintenance	1
Sub Total	5
Hospital Safety and Emergency Preparedness	
Health and Safety at Work	2
Environment Hazards	2
Fire Prevention	2
Fire Control	4
Bomb Threats	1
Disaster Control	2
Emergency Lift Procedure	1*
Helicopter Landing Procedures	1*
Sub Total	13
Security and the Law	
Powers of Arrest/Search Seizure	2
Method of Arrest, caution and preservation evidence	1
Police and Criminal Evidence Act	1
Attempts to commit crime	1
Theft and related offences	1
Criminal damage and arson	1
Misuse of drugs and substance abuse	2
Mental Health Legislation and Procedure	1*
Offences against the Person, Assaults and Wounding	1
Sexual offences	1
Trespass	1
Industrial disputes, Picketing and Public Order	1
Protection from Harassment	2
Data Protection legislation	2
Human Rights legislation	1
Sub Total	17

Specialised Skills	
Restraint Techniques/Self Defence	7
First Aid	32
Resuscitation	2
Customer Care Skills	7
Moving and handling	2
CCTV Control Room Procedures	14*
Topic Areas	**Hours**
Sub Total	50
Total (mandatory)	**121**
Note: The total mandatory training for this programme would range from 121 hours to 145 hours. * Denotes examples of additional elements that may be appropriate for a particular location.	

Appendix F: Glossary of abbreviations

A & E	Accident and Emergency
AFO	Authorised Firearms Officer
ACPO	Association of Chief Police Officers
BS	British Standards
BSIA	British Security Industry Association
CCTV	Closed Circuit Television
CFSMS	Counter Fraud and Security Management Service
CRB	Criminal Records Bureau
EFPMS	Estates and Facilities Performance Management System
EMI	Elderly, Mental and Infirm
FM	Facilities Management
HPE	Hospital Patient Environment
HSE	Health and Safety Executive
KSF	Knowledge and Skills Framework
LHB	Local Health Board
LSMS	Local Security Management Specialist
NAHFO	National Association of Hospital Fire Officers
NAHS	National Association of Healthcare Security
NHS	National Health Service
NHS SMS	National Health Service, Security Management Service
NPSA	National Patient Safety Agency
PC	Personal Computer
PIF	Performance Improvement Framework
PIs	Performance Indicators

RIDDOR	Reporting of Incidents, Diseases and Dangerous Occurrences Regulations 1995
SIA	Security Industry Authority
SoCO	Scene of Crime Officer

References

Acts and Regulations

Mental Health Act 1983, The Stationary Office (TSO), Parliament ISBN 0105420832

Radioactive Substances Act 1993 (RSA93), TSO, ISBN 0105412937
http://www.hmso.gov.uk/acts/acts1993/Ukpga_19930012_en_1.htm

Health and Safety at Work etc. Act 1974, TSO, ISBN, 0105437743
http://www.healthandsafety.co.uk/haswa.htm

Crime and Disorder Act 1998, Parliament TSO, ISBN 0105437980

Human Rights Act 1998, TSO, ISBN, 0105442984
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Crime and Disorder Act 1998, TSO, ISBN 0105437980
http://www.legislation.hmso.gov.uk/acts/acts1998/19980037.htm

Data Protection Act 1998, TSO, ISBN 0105429988
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Department of Health and Welsh Office, Code of Practice: Mental Health Act 1983 (revised 1999), **1999,** TSO, ISBN 0 11 322 1118
http://www.dh.gov.uk/assetRoot/04/07/49/61/04074961.pdf

Protection from Harassment Act 1997, TSO, ISBN 0105440973
http://www.hmso.gov.uk/acts/acts1997/1997040.htm

Regulation of Investigatory Powers Act 2000, TSO, ISBN 0105423009
http://www.hmso.gov.uk/acts/acts2000/2000023.htm

Private Security Industry Act 2001. TSO, ISBN 0105412015
http://www.hmso.gov.uk/acts/acts2001/20010012.htm

Protection of Children (SCOTLAND) Act 2003
http://www.scotland.gov.uk/publications/2003/08/17880/23848

Protection from Harassment Act 1007, Parliament TSO, ISBN 0105440973

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 1995, SI 3163:1995, TSO, ISBN 0110537513
http://www.legislation.gov.uk/si/si1995/Uksi_19953163_en_1.htm

Ionising Radiation Regulations 1999, SI 1999 No 3232, (IRR99), TSO, ISBN 0110856147 http://www.legislation.hmso.gov.uk/si/si1999/19993232.htm

Ionising Radiation (Medical Exposure) Regulations 2000, SI **2000** No 1059 (IRMER), TSO, ISBN 0110991311
http://www.healthcarecommission.org.uk/_db/_documents/IRMER_-_DH_letter_to_all.pdf

Control of substances hazardous to health: The Control of Substances Hazardous to Health Regulations 2002, Health and Safety Executive**.** Approved codes of practice and guidance, 2002, HSE, ISBN 0717625346
http://www.hmso.gov.uk/si/si2002/20022677.htm

NHSScotland Publications

NHSScotland, 'Firecode' Scottish Fire Practice Note 6, Version 3. **The prevention and control of wilful deliberate fire-raising in NHSScotland healthcare premises,** 2007 Health Facilities Scotland

All Scotland Area Child Protection Committees
http://www.scotland.gov.uk/Resource/Doc/1044/0016152.doc

Health Facilities Note 05 – Design against crime: A strategic approach to hospital planning, 1994, NHS Estates**,** TSO. ISBN 0113217366

Scottish Government Health Directorates,
http://www.scottishexecutive.gov.uk

Disclosure Scotland, http://www.disclosurescotland.co.uk

NHS England publications

Hospital Security EL (93) 47, 1993, NHS Executive

Model engineering specification C56 – Internal security systems, 1997, NHS Estates TSO, ISBN 0113223692

Model engineering specification C57 – Security of access and control, 1996, NHS Estates TSO, ISBN 0113223706

Model engineering specification C58 – Closed circuit television (CCTV) systems, NHS Estates 1997, TSO, ISBN 0113223714

EL(96)13 – Security in the NHS, 1996, NHS Executive **,**

EL(97)34 Update to EL(96)13: Security in the NHS, 1997, NHS Executive,**,**

EL(97)34 Update to EL (96)13: Security in the NHS, 1997, DH
http://www.dh.gov.uk/assetRoot/04/01/14/19/04011419.pdf

NHS Security Manual – A practical approach to planning the response to security incidents in the NHS, 1995, NHS Executive

NHS Security manual management Supplement, Safe and Sound: security in NHS Maternity units, 1995 NHS Executive

Effective management of security in A&E, 1997, NHS Executive

HSC 1999/226 – Campaign to stop violence against staff working in the NHS: NHS Zero Tolerance Zone, 1999, DH
http://www.dh.gov.uk/assetRoot/04/01/22/32/04012232.pdf

Mental Health Policy Implementation Guide, 2004, DH

Delivering race equality in mental health care: An action plan for the reform inside and outside services and the Government's response to the independent inquiry into the death of David Bennett, 2005, Department of Health

HSC 1999/226 – Campaign to stop violence against staff working in the NHS: NHS Zero Tolerance Zone, 1999, DH

HSC 2001/018 – Campaign to stop violence against staff working in the NHS: NHS zero tolerance zone, 2001, DH,
http://www.dh.gov.uk/assetRoot/04/01/22/05/04012205.pdf

Department of Health http://www.dh.gov.uk/publicationsAndStatistics/fs/en

Mental Health Policy Implementation Guide, 2004, DH
http://www.publications.DH.gov.uk/pdfs/mentalhealthimpgraphics.pdf

The NHS Knowledge and Skills framework (NHS KSF) and the Development Review process (October 2004)
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4090843

Department of Health, http://www.dh.gov.uk/Home/fs/en

Other sources of information

The Basic Training Manual and Study Guide, 1997. National Association for Healthcare Security This document is available free of charge to all members of the National Association for Healthcare Security. http://www.nahs.org.uk

Code of Practice for the protection of unoccupied buildings, 1996,Loss Prevention Council LPA, ISBN 090216712X

Guidance and the standards specification for electronic security systems: Facilities Management Specification 3, Pike, PG,1998, Building Services Research and Information Association (BSRIA), ISBN 0860225011http://www.bsria.co.uk/

A watching brief, A code of practice for CCTV, 1999. Local Government Information Unit (LGIU) (currently out of print but a photocopy can be obtained from the LGIU)

Code of Practice for Trainers in the Use of Physical Interventions: Learning Disability, Autism, Pupils in Special Educational Needs, 2001, British Institute of Learning Disabilities ISBN 1 902519 78 7

Construction site security and safety. Forgotten Costs! FBE – Report 4, 2002, Building Research Establishment (BRE), ISBN 1860815979 http://www.bre.co.uk

The recognition, prevention and therapeutic management of violence in mental health care, 2002, Nursing and Midwifery Council http://www.positive-options.com/news/downloads/UKCC_-_Therapeutic_Management_of_Violence_-_summary_-_2002.pdf

Violence at work: Findings from the 2002/2003 British Crime Survey, 2004, Home Office

A safer place to Work – Protecting NHS Hospital and Ambulance Staff from Violence and Aggression, 2003, National Audit Office TSO, ISBN 0215012070 http://www.nao.org.uk/publications/nao_reports/02-03/0203527.pdf

BS 7858 – The code of practice for security screening of personnel Employed in a Security Environment, 2004, BSI 0 580 43512 1 British Standards Institute http://www.bsi-global.com

Violence of work: Findings from the 2002/2003 British Crime Survey, 2004, Home Office http://www.homeoffice.gov.uk/rds/pdfs2/rdsolr0404.pdf

Security Management Framework for NHS Trusts in Wales, produced by the All Wales Security Task Force and Finish Group for the Welsh Assembly Government, July 2005.

British Institute of Learning Disabilities http://www.bild.org.uk/

Health and Safety Executive http://www.hse.gov.uk

Home Office http://www.homeoffice.gov.uk/

Legislation http://www.hmso.gov.uk/

NHS Security Management Services (SMS) http://www.cfsms.nhs.uk/press/index.html

Guidance for Health Bodies on the Security of Radioactive Sources

Foundation Level training for Local Security management Specialist

Not Alone – A Guide for Better Protection of Lone workers in the NHS.

Nursing and Midwifery Council, http://www.nmc-uk.org/

Association of Chief of Police Officers (ACPO), http://www.acpo.police.uk

British Security Industry Association, http://www.bsia.co.uk

Crime Fraud and Security Management Services (CFSMS), http://www.cfsms.nhs.uk

Crime Reduction Programme, http://www.crimereduction.gov.uk/cpindex.htm

Crime Concern, http://www.crimeconcern.org.uk/

Criminal Records Bureau, http://www.crb.gov.uk

Data Protection, http://www.dataprotection.gov.uk

Department of Trade and Industry, http://www.berr.gov.uk/

National Patient Safety Association, http://www.npsa.nhs.uk

Connecting for Health, http://www.connectingforhealth.nhs.uk/

Skills for Security http://www.sito.co.uk

Security organisations

British Security Industry Association (BSIA) The British Security Industry Association is the professional trade association for the security industry in the UK. Its aim is to help its member companies succeed and ensure they provide the highest possible standard of products and services to their customers. http://www.bsia.co.uk/

Counter Fraud and Security Management service (CFSMS) The Counter Fraud and Security Management Services (CFSMS) is a Special Health Authority, which has responsibility for all policy and operational matters relating to the prevention, detection and investigation of fraud and corruption and the management of security in the NHS Scottish division of NSS Counter Fraud Service. http://www.cfsms.nhs.uk/

National Association for Healthcare Security (NAHS) The National Association for Healthcare Security was formed in 1994, as a non-profit making UK professional organization for Healthcare managers with responsibility for security. It works to improve security in healthcare facilities through training, the exchange of information and experiences, and the provision of current information through conferences, meetings and events designed to meet the challenges and complexities of protecting modern medical facilities. http://www.nahs.org.uk/

Security Industry Authority (SIA) This authority exists to manage the licensing of the private security industry as set out in the Private Security Industry Act 2001. This Act outlines a system for the statutory regulation of the private security industry, and also aims to raise standards of professionalism and skills within the private security industry and to promote and spread best practice. http://www.the-sia.org.uk/