**DH** *Department of Health*

**NHS**

Protecting
your NHS

# A Professional Approach to Managing Security in the NHS

# Contents

# Foreword

Security of people and property in the National Health Service is the concern of all of us. The NHS Security Management Service has been charged with ensuring that all possible measures are taken to deliver a properly secure environment for all who work, or receive treatment, in the NHS.

There are many NHS security issues to be addressed. Physical assaults and abuse are particular concerns that have to be given priority. All those who work so hard to deliver quality patient care and services have the right to do so without fear of violence. Violent or abusive behaviour will not be tolerated and we will press for measures to be taken against individuals guilty of such acts. We will not hesitate to seek prosecutions where appropriate.

Ensuring security within such a large and diverse service as the NHS is no small task. We recognise that we will need the support and assistance of all those working in the NHS in dealing with the challenges that we and they face. Creating an effective structure for engaging with security issues and ensuring high standards of professionalism within this work are the key to ensuring lasting improvements.

I am pleased to be able to introduce this initiative and look forward to seeing the benefits to all who use or work in the NHS.

Parliamentary Under Secretary of State in the Lords – Lord Warner of Brockley

# Preface

This document outlines how the NHS will provide the best possible protection for its patients, staff, professionals and property. It is simply not acceptable for standards of patient care to be diminished by the actions of an irresponsible and anti-social minority. The NHS Security Management Service (SMS) will lead work to deter this minority and to ensure that a properly secure environment is created for staff, professionals and patients.

The starting point is this strategy. It is intended to provide common goals, a clear business process to achieve them and a framework for all those working in this area. The strategy puts into context the new approach to the management of security in the NHS and outlines the new legal requirements that will apply to all NHS bodies, so that there can be guarantees that the highest possible professional standards are implemented. Importantly, the SMS will also seek to build on good practice where it exists and ensure that every part of the NHS has access to the professional skills needed to lead this work effectively.

Work has already started on accurately establishing the nature and scale of the various problems that need to be addressed. In particular we are tackling the most serious of these, violence against staff and professionals working in the NHS.

From the 1st December a new national reporting system was established based on clear legal definitions of violence. There will be specialist investigators to obtain evidence about violent incidents and a new NHS Legal Protection Unit to work with the police and the Crown Prosecution Service to apply criminal and civil actions. From early in 2004 the largest ever NHS training programme will begin. This will provide conflict resolution training to all frontline staff and professionals who work in the NHS so that more potentially violent situations can be defused.

The work of SMS in these areas reflects its general professional approach ensuring real, permanent improvements in the extent to which patients, staff, professionals and property are protected. Those who would irresponsibly endanger the NHS and the healthcare that the public relies on should be clear that their actions are completely unacceptable, that the toughest possible action will be taken to stop them and, where appropriate, seek to apply sanctions.

The CFSMS would like to extend its thanks to all those who have assisted with the development of the security management strategy, in particular the members of the Security Management Strategy Development Group and the health bodies who facilitated the fact-finding visits. The result is a strategy produced by the NHS for the NHS.

Bill Darling                                     Jim Gee
Chair, NHS SMS                              Chief Executive, NHS SMS

December 2003

# 1. Introduction

1.1 The NHS Security Management Service (SMS) is part of the Counter Fraud and Security Management Service (CFSMS), a Special Health Authority within the NHS, and has overall responsibility for all policy and operational matters related to the management of security within the delivery of NHS services.

1.2 The SMS is committed to the delivery of an environment for those who use or work in the NHS that is properly secure so that the highest possible standard of clinical care can be made available to patients. A key role of security management in the NHS is to ensure that patients can enjoy their rights to healthcare whilst living up to their responsibility to respect and value a service that they rely on.

1.3 **The aim of the SMS is a simple one – to protect the NHS so that it can better protect the public's health.**

1.4 It is easier to provide high quality clinical care for patients where there is a combination of skilled, well resourced and motivated staff and professionals using the best equipment and medical supplies in a modern, friendly and welcoming environment. Security management and counter fraud work are two separate professional areas within the CFSMS, as distinct from each other as dentistry and optometry. However, while there is a separation of the two services, their roles complement each other to ensure that people, property and resources are properly protected.

1.5 Urgent protection is needed from the problems of violence if all NHS staff and professionals are to feel secure and able to treat patients effectively. Similarly patients need to feel secure in the environment in which they are treated. So this aspect of SMS responsibility needs prioritisation.

1.6 The SMS work on security management will be about delivering real, lasting improvements and building on good practice where it exists. It will have a distinctive, fact driven approach based on high quality information concerning the nature and extent of the problems and risks, whilst working within the clear strategic framework described in this document.

1.7 Security management work in the NHS needs a common language, common professional skills and a common methodology and standards. It also needs a national structure, which can link together and support those leading the work in the context of a strong, legal framework with carefully defined roles.

1.8 The SMS believes that it is essential to the delivery of a properly secure environment for those who work in, use or provide services to the NHS to have skilled managers in place in each health body, able to lead this work effectively and ensure relevant standards are met. The aim will be to provide professional, accredited training for a Local Security Management Specialist (LSMS) based in each health body and to co-ordinate efforts to meet defined national standards.

1.9 This document explains the distinctive strategic approach the NHS will take in seeking to raise standards of security work and how this will be done in a *comprehensive, inclusive and professional* manner. It defines the overall aims, objectives and the generic elements of the business process model that the SMS will adopt in ensuring that this takes place. The publication of this document is the first step in seeking to achieve these objectives by seeking to raise the profile of this important issue, which has an impact on all areas of NHS healthcare provision.

1.10 Security affects everyone who uses or works within the NHS. The security and safety of staff, professionals, patients and property should be a priority within the delivery and development of health services. All of those working within the NHS have a responsibility to be aware of these issues and to assist in preventing security related incidents or losses. Reductions over time in losses or incidents through the consequences of violence, theft or damage will lead to more resources being freed up for the delivery of better patient care and contribute to creating and maintaining an environment where staff, professionals and patients feel and *are* secure.

1.11 The SMS recognises that the NHS is a diverse organisation providing healthcare to a wide range of people in different ways – from a large acute hospital to a local Primary Care Trust – and that, in terms of security management, one size will not necessarily fit all. Therefore, the approach the SMS will take is to set the national framework in which the management of security work will take place, with local application and delivery, along with appropriate central support. It is recognised that the provision of security needs to adapt to the environment in which it takes place – what is right for an inner-city ambulance service may not be appropriate to that of a rural community's General Practitioner service.

1.12 To support the development of this strategy, a series of visits were made to a variety of health bodies and many different people working in the NHS to see the reality of the problems faced and to listen to views and ideas on potential solutions. The strategic approach described in this document reflects this. The visits allowed the SMS to identify examples of good practice, which need to be generalised across the NHS. The SMS is clear that an *inclusive* approach means working in partnership with key stakeholders within and outside of the NHS, not just to develop the strategy, but to implement it and to ensure that the NHS is properly protected.
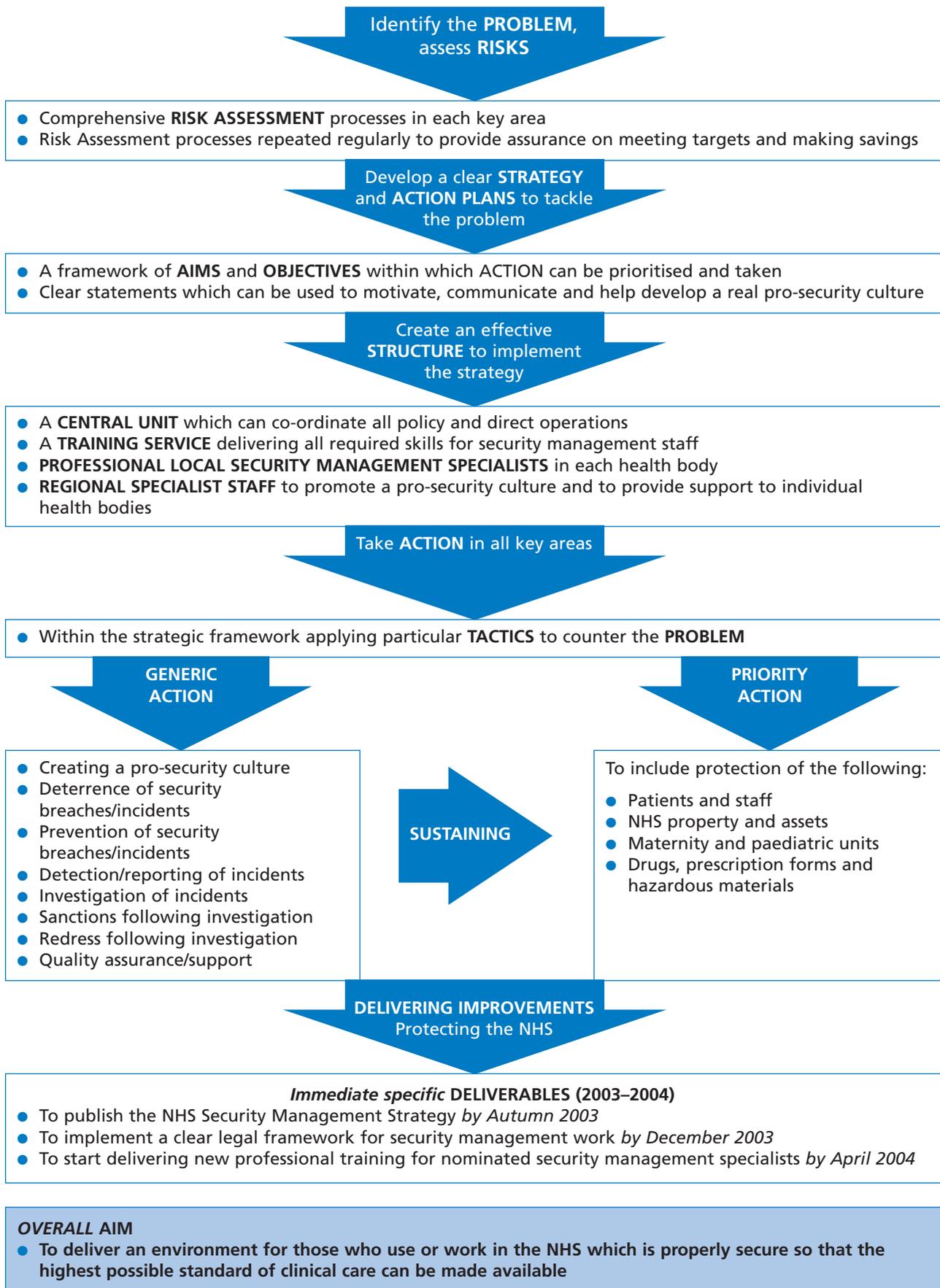
## 2.    The Security Management Remit

2.1    The SMS has responsibility for those aspects of NHS security management work that previously fell to various parts of Department of Health (DH) and the NHS or were not actually addressed. The SMS remit is defined in law (see Statutory Instrument 2002 No. 3039) and states that "the CFSMS shall have policy and operational responsibility…for the management of security in the NHS".

2.2    The SMS will work to raise standards and *professionalism* within the security management services being delivered, but will not directly manage operational staff who work in security within the NHS – this will remain the responsibility of the individual health body. The SMS will determine the policy, legal framework, operational guidance and minimum standards necessary to ensure that the objective of providing a secure environment for the NHS is achieved. The SMS will also provide central and regional support to those in health bodies charged with undertaking security management work (the LSMS) so that the required standards can be met.

2.3    The approach the SMS is taking is *inclusive* and places great value on involving stakeholders, from within and outside of the NHS, in the development of security management in the NHS. The SMS is working with a wide range of organisations in order to produce real and lasting improvements and achieve its objectives.

2.4    The approach is also *comprehensive* in that it will include the setting of standards and implementation of policy on a national level, as well as supporting staff carrying out security related work in health bodies. While necessary prioritisation of effort will mean that certain areas of concern will be emphasised in the first instance, the SMS remit covers all work on all NHS security risks and issues.

2.5    This means that the SMS is charged with tackling security management issues throughout the entire environment in which NHS services are delivered, therefore, everything in this document must be read as referring to all sectors of NHS healthcare provision.

# 3. Business Process – The NHS Security Management Model

3.1    The SMS approach will ensure that a clear business process model will be applied in respect of NHS security management. Elements of the counter fraud business process have been adapted specifically for security management work as they have proven to be successful. The key elements of this business process are:

- identifying problems by analysis of trends and risks;

- working within a clear strategic framework which establishes a common language of aims, objectives and methodologies;

- creating a strong and flexible working structure which can focus collective, professional expertise on the issues to be addressed;

- using the structure to take a generic range of action in respect of each specific area where security needs to be strengthened;

- quality assuring all work to ensure it meets common, high national standards; and

- continuously reviewing policy and procedure to learn from operational experience to minimise risks and prevent future security related incidents from occurring.

3.2    The various elements of the process and the range of action, both generic and specific, can be seen to link together and support each other – providing a *comprehensive* approach integrating both policy and operational work to provide a seamless service.

3.3    A diagram representing the business process model for NHS security management work is shown below.

# Managing security in the National Health Service: the optimum process

**Identify the PROBLEM, assess RISKS**

- Comprehensive **RISK ASSESSMENT** processes in each key area
- Risk Assessment processes repeated regularly to provide assurance on meeting targets and making savings

**Develop a clear STRATEGY and ACTION PLANS to tackle the problem**

- A framework of **AIMS** and **OBJECTIVES** within which ACTION can be prioritised and taken
- Clear statements which can be used to motivate, communicate and help develop a real pro-security culture

**Create an effective STRUCTURE to implement the strategy**

- A **CENTRAL UNIT** which can co-ordinate all policy and direct operations
- A **TRAINING SERVICE** delivering all required skills for security management staff
- **PROFESSIONAL LOCAL SECURITY MANAGEMENT SPECIALISTS** in each health body
- **REGIONAL SPECIALIST STAFF** to promote a pro-security culture and to provide support to individual health bodies

**Take ACTION in all key areas**

- Within the strategic framework applying particular **TACTICS** to counter the **PROBLEM**

**GENERIC ACTION**

- Creating a pro-security culture
- Deterrence of security breaches/incidents
- Prevention of security breaches/incidents
- Detection/reporting of incidents
- Investigation of incidents
- Sanctions following investigation
- Redress following investigation
- Quality assurance/support

**SUSTAINING**

**PRIORITY ACTION**

To include protection of the following:

- Patients and staff
- NHS property and assets
- Maternity and paediatric units
- Drugs, prescription forms and hazardous materials

**DELIVERING IMPROVEMENTS**
Protecting the NHS

**Immediate specific DELIVERABLES (2003–2004)**
- To publish the NHS Security Management Strategy *by Autumn 2003*
- To implement a clear legal framework for security management work *by December 2003*
- To start delivering new professional training for nominated security management specialists *by April 2004*

**OVERALL AIM**
- **To deliver an environment for those who use or work in the NHS which is properly secure so that the highest possible standard of clinical care can be made available**

# 4. Identifying the Problem and Assessing the Risk

4.1 Many of the general deficiencies around security in the NHS have been well documented and voiced publicly. They include:

- inconsistent standards of training for those engaged in security work;

- lack of nationally consistent guidance;

- lack of application of, or compliance with, guidance where it covers specific issues;

- limited awareness of the consequences of poor security both in financial and human terms; and

- inconsistent reporting and lack of co-ordination both at national and local levels.

4.2 Through its approach and the application of its business process, the SMS will aim to address these issues. By tackling these general deficiencies, and by generalising good practice and experience, the capacity of the NHS to tackle specific security management problems will be greatly improved.

4.3 Where there are specific problems, the SMS will seek to identify the nature and scale of these problems as the essential first step to providing a solution. For example, in respect of violence against staff and professionals working in the NHS, we will not only establish effective incident reporting systems which can provide accurate quantitative and qualitative information but will also collate information about their perceptions of this threat.

4.4 As problems are identified and risks assessed, appropriate solutions will be developed to tackle them. The SMS problem identification and risk assessment process will allow progress to be measured and evaluated to ensure that solutions have the intended impact.

# 5. Creating an Effective Structure

5.1    The NHS needs a structure to implement the strategy described in this document. That structure needs to be capable of linking and supporting those working in this area so that they can deliver a generic range of action to tackle specific issues.

5.2    At a national level there will be a unit within the SMS charged with policy work and from 2004 – 2005, stationed alongside the current Counter Fraud Service (CFS) operational units throughout the NHS, there will be SMS officers charged with promoting high standards and providing support to LSMS and their staff.

5.3    LSMS work will take place within a clear legal framework, set out in Secretary of State Directions issued by the DH to relevant health bodies. These will describe the functions of the new role of the LSMS, the duties of the health body and their relationship with the SMS. Once accredited, only the LSMS will be able to perform the duties and functions described in Directions and subsequent guidance. There will also be a requirement for each health body to nominate an Executive Director to lead on security management issues.

5.4    In line with the commitment that the management of security will continue to be delivered locally, health bodies will be required to nominate suitable members of staff for the LSMS role and new, professional security management training. The training is intended to consolidate existing knowledge and raise the overall level of skills across the NHS. LSMS nominees will be required to successfully complete the training so that the NHS has a guarantee that security management work will be undertaken with the required level of skill and expertise.

5.5    Training will begin early in 2004–05 and these LSMS, once they have successfully completed their training, will carry out defined roles within the new structure, meeting common high standards described in the NHS Security Management Manual to be issued from summer 2004 onwards. LSMS will be supported by the SMS in terms of national guidance, ongoing training and central advice.

5.6    The SMS recognises that there are many staff working in various security-related roles across the NHS, and acknowledges the need to work with all of them and involve them in the development of the service in order to achieve the objectives to which the SMS is committed.

5.7    This structure will need to reach out, seeking and maintaining the support of major stakeholders in this work, including representatives of staff and professionals, regulatory bodies such as the Health and Safety Executive (HSE) and those working in human resources and finance. Only by working together can the NHS tackle the diverse range of security issues that it faces.

# 6.    Generic Action

6.1    The SMS will develop both proactive and reactive initiatives in relation to NHS security management work across the whole of the generic range of action:

    6.1.1    Creating *a pro-security culture* amongst staff, professionals and the public – to engender a culture where the responsibility for security is accepted by all and the actions of the minority who breach security are not tolerated;

    6.1.2    *deterring* those who may be minded to breach security – using publicity to raise awareness of what the consequences of their intended actions could be, both personally and to the NHS;

    6.1.3    *preventing* security incidents or breaches from occurring, wherever possible, or minimising the risk of them occurring by learning from operational experience about previous incidents, using technology wisely and sharing best practice;

    6.1.4    *detecting* security incidents or breaches and ensuring these are reported in a simple, consistent manner across the NHS so that trends and risks can be analysed, allowing this data to properly inform the development of preventative measures or the revision of policies and procedures, both nationally and locally;

    6.1.5    *investigating* security incidents or breaches in a fair, objective and professional manner, to ensure those responsible for such incidents are held to account for their actions, and that the causes of such incidents or breaches are fully examined and fed into prevention work to minimise the risk of them occurring again;

    6.1.6    applying a wide range of *sanctions* against those responsible for security incidents and breaches, involving a combination of procedural, disciplinary, civil and criminal action as appropriate;

    6.1.7    seeking *redress* through the criminal and civil justice systems against those whose actions lead to loss of NHS resources, through security breaches or incidents, and ensuring that those who are the victims of violence within the NHS environment are supported to seek appropriate compensation from offenders for loss of earnings or for the effects of injuries sustained.

# 7.  Specific Areas of Action

7.1   The SMS remit is very broad and will translate into specific action in many different areas. In order to ensure that real progress is made, there is a need to focus initial effort and priorities on some key areas of security management work.

7.2   *Protecting people* – staff and professionals working in or providing services to, and patients using the NHS – minimising the risk of physical and non-physical assault;

   7.2.1   The first of these areas includes the most valuable resource in the NHS – the staff and professionals who work within it. A highly skilled and dedicated workforce needs to be properly protected if the NHS is to retain existing personnel and attract the best in the future. Staff and professionals have the right to work, as patients have the right to be treated, in an environment where all feel safe and secure and where the risk of violence in whatever form is minimised.

   7.2.2   The National Audit Office (NAO) report *A Safer Place to Work – protecting NHS hospital and ambulance staff from violence and aggression*, published in March 2003, commended the DH and the NHS for action taken through the NHS *Zero Tolerance* campaign, but made a number of recommendations to further strengthen efforts to make the NHS a safer place to work. In taking this work forward the SMS intends to go considerably beyond previous anti-violence initiatives. As a key preventative measure it will develop and ensure the delivery of a national syllabus in conflict resolution training for all staff and professionals working in, or providing services to, the NHS and at risk from violent behaviour.

   7.2.3   The consequences of violence on staff and professionals working in the NHS are difficult to quantify. The NAO have estimated the direct financial cost to NHS Trusts to be at least £69m per annum[1] but no exact figures currently exist. There are costs to the staff and professionals concerned, and to the NHS – in both human and financial terms. For the individual these can include pain, time away from work, depression and low self-esteem. For the NHS they can include the impact of the incident on colleagues, as well as the loss of key personnel for long periods of time, or possibly altogether.

   7.2.4   No one can guarantee that violence can be completely eradicated in any environment. However, through learning from the experience of staff, professionals and patients and through working with the DH and NHS bodies, the SMS aims to put in place tangible measures that will help to minimise the risk of assault, and meet the standards expected from health bodies under the Improving Working Lives (IWL) programme. The SMS will work with other government departments, such as the Home Office and with agencies such as the HSE, the police and the Crown Prosecution Service (CPS) to ensure that it can successfully deal with violence in the workplace.

   7.2.5   The SMS will work with partners in NHS professions and their representative bodies, trade unions and patient representative groups to ensure that where action is taken, it is relevant, credible and supported by all those working in, using, or delivering services to the NHS.

---

[1] *A Safer Place to Work: Protecting NHS Hospital and Ambulance Staff from Violence and Aggression* London: The Stationery Office 2003.

7.2.6 An example of how the SMS is already demonstrating how the whole range of generic action can be applied to a specific problem – physical and non-physical assaults on staff and professionals who work in, or deliver services to the NHS – is shown below:

- The development of a *pro-security culture* among staff, professionals and patients, building on work already done, to further raise awareness and encourage them to report violent incidents when they occur.

- The use of particular case studies to raise awareness of those who have or are minded to be violent towards others in the NHS of the consequences of their actions to themselves, the NHS or others, to assist in *deterrence* of further incidents.

- Identification of risks to help *prevention* of incidents in the first place. Enabling staff and professionals working in, or delivering services to the NHS, to be trained in preventing incidents occurring by developing and delivering a consistent and credible national syllabus in conflict resolution. The aim will be to equip staff and professionals with the necessary skills to recognise and de-escalate potentially violent incidents, and will include customer care/service skills and diversity awareness training. Learning from incidents that occur to inform development of policies and procedures on tackling violence.

- Simple, streamlined and consistent reporting systems, using clear and legally based definitions, enabling the *detection* of incidents of violence to be used for trend and risk analysis, which will allow it to be used in informing the appropriate action that needs to be taken to tackle problems identified and enable feedback on outcomes to those who have been subjected to violence.

- Work with the police and the CPS to ensure that a nationally consistent approach to the *investigation* and handling of cases of violence is taken, and ensuring that staff and professionals are supported throughout this process. Investigation of incidents in a fair and professional manner to ensure that offenders are dealt with appropriately, and to reassure staff and professionals that the NHS will take firm action against offenders.

- Action to ensure that that the full range of possible *sanctions* is considered when dealing with offenders, to ensure that these are applied consistently and appropriately, as well as to provide good quality feedback to those who have suffered from violence.

- Systems to enable those who are the victims of violence – and the NHS – to obtain *redress*, in appropriate cases, and ensure that appropriate counselling and support is provided where needed.

## 7.3  *Protecting property and assets*

7.3.1 All those who work in, use or provide services to the NHS have a collective responsibility to ensure that property and assets relevant to the delivery of NHS healthcare are properly secure.

7.3.2 Property can be defined as the physical buildings in which NHS staff and professionals work, where patients are treated and from where the business of the NHS is delivered. Assets, irrespective of their value, can be defined as the materials and equipment used to deliver NHS healthcare. In respect of staff, professionals and patients it can also mean the personal possessions they retain whilst working in, using or providing services to the NHS.

7.3.3 Protecting property involves buildings from where NHS healthcare is delivered, since damage to or theft from them can have an impact on the delivery of that healthcare, as well as depriving the NHS of resources that would otherwise go to patient care. There are also clear links between security of property and the potential for incidents of violence against staff, professionals and patients to occur, as well as theft of their property and of NHS assets. Poorly designed buildings or extended sites, with numerous exits and public rights of way, can make securing property difficult and can create the potential for those who have no proper business at a particular site to gain unchallenged access.

7.3.4 As examples of what can be achieved, through modernisation of Accident and Emergency departments and the re-building of some hospital sites by way of Private Finance Initiatives, much thought and resources have already been given to designing safer environments for staff, professionals and patients. Crime prevention expertise and development of technology have been used to secure access and monitor those on site. The CFSMS is already working with the Police Scientific Development Branch of the Home Office on a Treasury-funded initiative (*Safer Hospitals Project*) looking at how technology can be best used to protect NHS staff, professionals, property and assets.

7.3.5 Assets acquired by or donated to health bodies are the tools that allow the staff and professionals to do their jobs and deliver NHS healthcare to patients. While assets are often regarded as items over a certain value recorded on a health body's asset register, all items owned by or donated to a health body should be considered as assets and should be properly secure. This should be irrespective of whether they are low value stationery items, catering supplies, furniture, Information Technology equipment and consumables, drugs, expensive medical equipment or hazardous materials. Theft of, damage to or loss of these items has never been accurately quantified, whether in terms of the financial costs of replacement or the impact on NHS healthcare delivery by not having them when they are needed.

7.3.6 The SMS will work to ensure that consistent action across health bodies is taken in order to minimise the impact on the NHS and the ability of staff and professionals to work effectively. Specific guidance and best practice will be available in the forthcoming NHS Security Management Manual.

## 7.4  Other areas

7.4.1 Drugs, prescription forms and potentially hazardous materials are particular areas of concern for the NHS, since security here involves not only the need to avoid loss or damage, but also the potential consequences of misuse of such items.

7.4.2 Maternity and paediatric units also need to be properly secure. Although instances of security breaches here are thankfully rare, the NHS needs to be vigilant and remain alert to the risks that are present.

7.4.3 Secure units within the mental health environment are also of particular concern. Staff, professionals and patients have a wider range of sensitive and complex matters to deal with, where relevant expertise will be required to assess the risks faced and provide solutions to minimise those risks.

7.4.4 Specific areas of security work that are our initial priorities can be summarised as being around people and property. In order to meet our full responsibilities under the law, we will – in the future – also address security issues in relation to confidentiality of information, systems and records, as resources and people become available to take this work on.

# 8.  Progress Measurement

8.1   The SMS will develop initiatives relevant to all areas of work across areas of generic action. A range of accurate and credible processes will also be developed to continuously assess whether action taken to tackle security problems is having the right impact and helping to achieve overall objectives. The SMS will work with all relevant organisations to ensure that people and property are properly secured and protected.

8.2   Progress measurement systems will need to be comprehensive in respect of the whole range of security work. They should not concentrate simply on reported or detected security breaches or incidents although, of course, there needs to be reductions in levels of these. For example, in respect of violence, it is recognised that the perception and the reality of the risks may differ but that both have an adverse effect on the lives of those working in, using or providing services to the NHS. To address these concerns properly, the SMS needs to improve the situation around both perception and reality, and to demonstrate that it has done so.

# 9.   Standards

## 9.1   *Directions*

9.1.1   A distinctive aspect of the SMS approach will be the introduction of required foundation level training and minimum standards for security management in the NHS. Secretary of State Directions will be issued by the DH to set out requirements for health bodies and to ensure compliance with these.

9.1.2   Although some health bodies have a designated security manager in place, their duties are typically combined with others such as facilities management or catering. One immediate change will be the requirement, through Directions, for all health bodies to nominate appropriate and suitable staff for training, and subsequent SMS accreditation, as new LSMS nominees. By providing professional training for the LSMS the SMS intends to develop common, high standards of skills for all those undertaking security management work in the NHS.

## 9.2   *Training*

9.2.1   It is estimated that as many as 18,000 people may currently earn their living through NHS security work. Many health bodies provide some level of security presence through the employment of security staff. These are principally engaged to provide a level of deterrence against abuse and assaults, theft of assets, to protect buildings and to react to incidents. Provision varies from health body to health body and can be either in-house or external. Cost appears to be an overriding factor in determining provision and, in some cases, is funded in an unplanned way without consideration of the need for future investment.

9.2.2   Security-related training has been provided through a variety of in-house or external providers. There appears to have been little evaluation made of quality or impact and, again, cost may often have been a major factor in decisions on provision.

9.2.3   The existing CFSMS Training Service will expand to provide the foundation level training courses for LSMS nominees from health bodies. The SMS training content and direction will take full account of developments within the security industry and will be delivered to the highest standards, learning from those organisations within the NHS where good work is already taking place.

9.2.4   The Private Security Industry Act 2001 and the subsequent creation of the Security Industry Authority will, in due course, drive up standards in the private sector security industry through licensing arrangements and minimum training. As the SMS begins its programme of work to drive up standards over the coming years in the management of security, it will work to ensure that standards in the NHS are always equivalent to or higher than those emerging as a consequence of security management related legislation.

9.2.5   Beyond this foundation level training the SMS will, in time, develop advanced level training linked to academic qualifications. This will provide a clear learning path for those who undertake security management work.

## 9.3   *Professional and ethical framework*

9.3.1   As well as the technical standards of security training, the SMS will develop and promote a consistent approach with regards to how the work will be carried out. This is an important aspect of professionalism, and the SMS proposes to develop its existing professional and ethical framework and embed this within the new LSMS training. The principles at the heart of this are:

9.3.2   *Professionalism.* All staff involved in security work should maintain the highest standards of professionalism, in the best tradition of other NHS professions. Specifically this should cover areas of personal conduct, expertise and all work related to the management of security.

9.3.3   *Objectivity.* Security management work should be undertaken with an open mind, particularly in relation to assessment of incidents, evidence or information. Consideration should be given to all interpretations that may be placed on such incidents, evidence or information.

9.3.4   *Fairness.* A polite and courteous approach should be adopted, with an absence of any form of preconception or discrimination, in accordance with current equal opportunities or valuing diversity policy.

9.3.5   *Expertise.* All staff working in NHS security related positions have a duty to maintain the highest level of expertise and ensure that this is applied thoroughly and comprehensively.

9.3.6   *Propriety.* Those who work within all aspects of NHS security provision have a duty to ensure that they meet the highest standards of propriety. The personal and financial integrity of those who undertake security work must never be in question and checks will be undertaken to ensure that this is the case. Proper, accurate records meeting all relevant legislative requirements of NHS security management work must be kept with particular reference to issues of confidentiality so that information is passed only to those who are entitled to receive it. It is not simply enough to merely ensure that this propriety is maintained; it is also essential that there is never any perception of impropriety.

9.3.7   *Vision.* Work on NHS security must be understood in the context of the overall improvement of the NHS and overall strategic aims, including the continual development of a pro-security culture and effective joint working with other agencies.

## 9.4   *Continuous learning/development*

9.4.1   The SMS will, in due course, publish full details of the contents of all security management training courses. It will also work to ensure that standards in NHS security work are maintained and continually developed through a programme of quality assurance, and through the promotion, among staff working within NHS security, of continued professional development with a specific, structured learning and qualification route.

# 10. First Steps

10.1 Immediate work will cover general steps to build lasting arrangements that are capable of tackling the full range of security issues in the NHS, and to address immediate priority areas, such as reducing violence against staff, professionals and patients.

10.2 The first general step is the publication of this document describing a clear strategic framework. The next step will be to build a structure capable of implementing the strategy. The initial training and quality assurance timetable will be as follows:

● NHS LSMS accreditation training programme to be developed in 2003.

● Legislation through Secretary of State Directions requiring LSMS nominations to be issued in January/February 2004.

● LSMS nominations to be made by 31 March 2004.

● First LSMS training courses to begin April 2004.

● New NHS Security Management Manual to be made available to accredited LSMS staff from summer 2004 onwards.

● Quality assurance processes to be in place by Autumn 2004 – 2005.

10.3 Specific priorities have already required the SMS to develop initiatives related to reducing violence;

10.3.1 A new consistent and national reporting system for recording incidents of physical assault and a locally managed consistent reporting system for recording non-physical assault, based on clear and legally based definitions with the ability to track cases from report to conclusion and take action where necessary and appropriate, to ensure the best possible outcome for the person assaulted.

10.3.2 A new Legal Protection Unit to work with health bodies, the police and the CPS to increase the rate of prosecutions and to provide cost-effective advice on a wide range of sanctions against individuals who are violent towards staff and professionals working in, or providing services to, the NHS.

10.3.3 As an interim measure to cover the period until LSMS are trained and in place in all health bodies, the SMS will use its existing highly trained and professional CFS operational service units to investigate incidents of physical assaults, where appropriate.

10.3.4 As a key preventative measure to complement the range of reactive measures described above, the SMS is, in conjunction with stakeholders such as the Royal College of Nursing,
the British Medical Association and UNISON, developing a national syllabus for conflict resolution training for all staff and professionals who work in, or provide services to, the NHS and are at risk from violent behaviour. A separate syllabus will be developed to deal with mental health and learning disability environments, where it is recognised that particular specialist expertise is required. The issue of physical intervention techniques will also be addressed as part of this work.

10.3.5 New SMS-employed lead security management specialists, deployed in each NHS region during 2004-05, will begin to drive up standards of local work to reduce violence.

10.3.6 A Memorandum of Understanding with the Association of Chief Police Officers (ACPO) will be developed clearly outlining SMS, LSMS and police responsibilities and roles in relation to security management and, in particular, responsibilities around tackling violence in the NHS.

# 11. Conclusion

11.1 This document describes the strategic approach to be adopted to drive up standards in NHS security work. The SMS will identify security-related problems and risks, and put in place a structure of specialist, professional and skilled staff to implement solutions. Progress will be carefully assessed and a range of action will be taken to make improvements.

11.2 In this way the SMS will seek to ensure that measurable improvements take place. However, in an organisation as large and diverse as the NHS, the delivery of effective and lasting change is not easy and the implementation of the aims of this document will depend on the support of the wider NHS and the specific stakeholder groups for this area of work. The aim is to unite the NHS in its own defence. By delivering better protection for the NHS, the SMS aims to enable the NHS to deliver better health services to the public.

# APPENDIX 1

## Comparative examples of current security management practice in the NHS

- In some health bodies all staff are required to attend a mandatory safety training day which encompasses the delivery of conflict resolution training.

- Some health bodies issue external contractors with dated ID badges and coloured tabards to identify them as visitors. Contractors are required to return their ID badges at the end of each working day.

- Some health bodies have installed CCTV systems, which are monitored 24 hours a day, by dedicated control room staff. Also, some A&E departments have cameras linked to a liquid crystal display screen at the local police station. This allows the police to assess situations prior to attending incidents they are called out to.

- Some health bodies have set up external security cameras on their premises, with the assistance of local crime prevention officers to ensure good area coverage and correct installation.

- Some health bodies write to patients whose behaviour is deemed to be unacceptable during their attendance for treatment. Those patients are welcomed to comment on their behaviour, whilst making it clear that any reoccurrence of such behaviour will result in alternative arrangements for treatment.

- In some health bodies the Chief Executive writes to all staff who have been the subject of violence or abuse to acknowledge their report.

- All staff are encouraged to take ownership and responsibility for security through general and localised orientation induction in some health bodies.

- In other health bodies, conflict resolution training is only provided if requested by staff, or not at all.

- Other health bodies do not have any controls in place to identify external contractors nor do they keep any log of the dates or times of their attendance.

- Other health bodies, who have installed a large number of CCTV cameras, have not increased the number of control room staff to monitor images or respond to incidents. There is no mechanism in place to relay images to the local police.

- Other health bodies have not enlisted the help of the local crime prevention officer and anti-vandal cages protecting external security cameras obscure areas on which they focus. Camera wiring is external and may be easily disconnected.

- Other health bodies do not contact patients at all and no alternative arrangements are made.

- In other health bodies staff receive no feedback from the health body in respect of incidents of violence and aggression or how they are being tackled.

- Other health bodies do not address security awareness through induction or encourage to staff to take responsibility for security in general.

# APPENDIX 2

## Schedule of publications – Security Management in the NHS

| Document | Description | Intended date of publication |
|---|---|---|
| Security management in the NHS – Strategic Approach | ● Mission statement for the management of security in the NHS<br><br>● Overall aim and objectives<br><br>● Business process model<br><br>● Generic range of action<br><br>● Specific areas of action<br><br>● Progress measurement<br><br>● Standards<br><br>● First steps | December 2003 |
| Secretary of State Directions on management of security in the NHS (and guidance notes) issued by the Department of Health | ● Nominations from health bodies for the role of local security management specialists<br><br>● Description of the role of local security management specialists<br><br>● Description of the relationship of health bodies, the local security management specialists and the SMS | January/February 2004 |
| NHS Security Management Manual of Guidance | ● Guidance on work to be undertaken by local security management specialists under the generic range of action<br><br>● Guidance on work to be undertaken by local security management specialists under specific areas of action<br><br>● Standards of the work of local security management specialists<br><br>● Technical information and guidance on security | Summer 2004 |