Standards for providers 2017-18
Security management

www.nhsprotect.nhs.uk
<table>
<thead>
<tr>
<th>Version number</th>
<th>Publication date</th>
<th>Changes made</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>??</td>
<td>-</td>
</tr>
</tbody>
</table>
# Contents

<table>
<thead>
<tr>
<th>Chapters</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>15</td>
</tr>
</tbody>
</table>

Appendix 1: Reasonable expectations – quality assurance programme .................................... 79
Appendix 2: Security management quality assurance flowchart ................................................. 80
Appendix 3: Summary of changes to standards ............................................................................. 81

## Quick links to standards in Chapter 5
Please click on the links below to go to the detailed explanation for each standard.

<table>
<thead>
<tr>
<th>Strategic Governance</th>
<th>Key Principle 1 Inform and Involve</th>
<th>Key Principle 2 Prevent and Deter</th>
<th>Key Principle 3 Hold to Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard 1.1</td>
<td>Standard 2.1</td>
<td>Standard 3.1</td>
<td>Standard 4.1</td>
</tr>
<tr>
<td>Standard 1.2</td>
<td>Standard 2.2</td>
<td>Standard 3.2</td>
<td>Standard 4.2</td>
</tr>
<tr>
<td>Standard 1.3</td>
<td>Standard 2.3</td>
<td>Standard 3.3</td>
<td>Standard 4.3</td>
</tr>
<tr>
<td>Standard 1.4</td>
<td>Standard 2.4</td>
<td>Standard 3.4</td>
<td>Standard 4.4</td>
</tr>
</tbody>
</table>
1.1 This document aims to provide information to providers of NHS services on the security management clauses in the NHS Standard Contract 2017/18 and 2018/19, and explain what providers need to do to comply with them.

1.2 NHS Protect leads on work to identify and tackle crime across the health service. The aim is to protect NHS staff and resources from activities that would otherwise undermine their effectiveness and their ability to meet the needs of patients and professionals. Ultimately, this helps to ensure the proper use of valuable NHS resources and a safer, more secure environment in which to deliver and receive care.

1.3 NHS Protect has five high-level organisational aims. These are:

• To provide national leadership for all NHS anti-crime work by applying an approach that is strategic, co-ordinated, intelligence-led and evidence based.

• To work in partnership with the Department of Health, commissioners and providers, as well as our key stakeholders, such as the police, CPS and local authorities to coordinate the delivery of our work and to take action against those who commit offences against the NHS.

• To establish a safe and secure physical environment that has systems and policies in place to protect NHS staff from violence, harassment and abuse; safeguard NHS property and assets from theft, misappropriation, or criminal damage; and protect resources from fraud, bribery and corruption.

• To lead, within a clear professional and ethical framework, investigations into serious, organised and/or complex financial irregularities and losses which give rise to suspicions of fraud, bribery or corruption.

• To quality assure the delivery of anti-crime work with stakeholders to ensure the highest standard is consistently applied.

1.4 The NHS Standard Contract includes mandatory clauses that require providers of NHS services to put in place and maintain appropriate counter fraud and security management arrangements. The clauses take a risk based approach, requiring providers to carry out a risk assessment, and follow the applicable standards. Further explanation of the NHS Standard Contract is provided in chapter 2 of this document.
2.1 The NHS Standard Contract is published by NHS England. The 2017/18 and 2018/19 version is available from [http://www.england.nhs.uk/nhs-standard-contract](http://www.england.nhs.uk/nhs-standard-contract). The contract should be used by clinical commissioning groups (CCGs) and NHS England when commissioning NHS funded services including acute, ambulance, care home, community-based, high secure and mental health and learning disability services. CCGs must also use the NHS Standard Contract for all community-based services provided by GPs, pharmacies and optometrists that have been previously commissioned as Local Enhanced Services.

2.2 The counter fraud and security management clauses are set out in Service Condition 24 and place the following obligations on providers of NHS services:

- Service Condition 24.1 requires all providers to put in place and maintain appropriate counter fraud and security management arrangements, having regard to NHS Protect’s standards.

- Service Condition 24.2 requires those providers which are licensed¹ by Monitor², and NHS Trusts, to take the necessary action to meet the standards set by NHS Protect.

- Service Condition 24.3 requires the provider to allow, if requested by the co-ordinating commissioner or NHS Protect, a person duly authorised to act on behalf of NHS Protect or on behalf of any commissioner to review, in line with the appropriate standards, security management and counter fraud arrangements put in place by the provider.

- Service Condition 24.4 requires the provider to implement any modifications to its counter fraud and security management arrangements required by a person referred to in Service Condition 24.3 within such timescales as that person may reasonably require.

- Service Condition 24.5 requires the provider to report any suspected fraud or corruption involving a service user or NHS funds to the LCFS of the relevant NHS body and NHS Protect. Any suspected security incident or breach involving staff who deliver NHS funded services or involving NHS resources must be reported to the LSMS of the relevant NHS body, to NHS Protect and to the LSMS of the Co-ordinating Commissioner.

- Service Condition 24.6 requires the provider, on the request of the Department of Health, NHS England, NHS Protect or the co-ordinating commissioner to ensure that NHS Protect or any LCFS or LSMS appointed by a commissioner is given access within five operational days to properties, information and staff for the purpose of detecting and investigating cases of fraud and corruption and security incidents and breaches.

2.3 The standards referenced in Service Condition 24.3 are explained in chapters 3 and 5.

---

¹ A licence granted by Monitor under section 87 of the Health and Social Care Act 2012.

² Monitor is a corporate body provided by section 61 of the Health and Social Care Act 2012. NHS Improvement has brought together two distinct legal entities: Monitor, a non-departmental public body and the NHS Trust Development Authority, a special health authority, under a single leadership and operating model. Both organisations continue to maintain their current legal underpinnings as two separate bodies.
Overview of the standards

Introduction

3.1 NHS Protect is committed to raising the standards of security management within the NHS and has developed a national strategy and a series of security standards for providers, which follow a risk based approach to providing a safe and secure environment for patients, staff and visitors and to protecting NHS properties and assets.

3.2 Anyone working in the NHS, receiving NHS treatment or visiting NHS properties has the right to feel safe and secure from violence and abuse, both physical and verbal. Funds and assets belonging to the NHS or used to provide NHS services should also be kept safe and secure at all times. A failure to do so can have a major impact on patient and staff welfare and the standard of care patients receive from the NHS.

Standards for security management

3.3 The standards in this document have been developed to support NHS providers in ensuring they have appropriate security management arrangements in place within their organisation, to protect staff and patients and to ensure NHS assets are kept safe and secure. They will assist providers in implementing key aspects of security management, identifying areas requiring improvement and developing their own plans for improvements. It is the responsibility of the organisation as a whole to ensure it meets the required standards, though one or more departments, business units or individuals may be responsible for implementing a specific standard.

3.4 The security management standards are set out in detail in chapter 5 of this document and there are four key sections that follow NHS Protect’s strategy:

**Strategic Governance.** This section sets out the standards in relation to the organisation’s strategic governance arrangements. The aim is to ensure that anti-crime measures are embedded at all levels across the organisation.

**Inform and Involve.** This section sets out the requirements in relation to raising awareness of crime risks against the NHS and working with NHS staff, stakeholders and the public to highlight the risks and consequences of crime against the NHS.

**Prevent and Deter.** This section sets out the requirements in relation to discouraging individuals who may be tempted to commit crimes against the NHS and ensuring that opportunities for crime to occur are minimised.

**Hold to Account.** This section sets out the requirements in relation to investigating security related incidents, obtaining sanctions against those responsible and seeking redress where appropriate.
### Strategic Governance

1.1 A member of the executive board or equivalent body is responsible for overseeing and providing strategic management and support for all security management work within the organisation. This person is nominated to NHS Protect.

1.2 The organisation’s audit committee chair, non-executive directors and board level senior management provide clear and demonstrable support and strategic direction for security management work. Evidence of proactive management, control and evaluation of security management work is present. If NHS Protect has carried out a quality assessment, the non-executive directors and board level senior management ensure recommendations made are fully actioned.

1.3 The organisation employs or contracts a qualified, accredited and nominated security specialist(s) to oversee and undertake the delivery of the full range of security management work.

1.4 The organisation allocates resources and investment to security management in line with its identified risks.

1.5 The organisation reports annually to its executive board, or equivalent body, on how it has met the standards set by NHS Protect in relation to security management, and its progress on local priorities as identified in its work plan.

### Key Principle 1: Inform and Involve

2.1 The organisation has an ongoing programme of work to raise awareness of security measures and security management in order to create a pro-security culture among all staff. As part of this, the organisation participates in all national and local publicity initiatives, as required by NHS Protect, to improve security awareness. This programme of work will be reviewed, evaluated and updated as appropriate to ensure that it is effective.

2.2 The organisation develops and maintains effective relationships and partnerships with local and regional anti-crime groups and agencies to help protect NHS staff, properties and assets.

2.3 The organisation ensures that security is a key criterion in any new build projects, or in the modification and alteration (e.g. refurbishment or refitting) of existing properties. The organisation demonstrates effective communication between risk management, capital projects management, estates, security management and external stakeholders to discuss security weaknesses and to agree a response.

2.4 All staff know how to report a violent incident, theft, criminal damage or security breach. Their knowledge and understanding in this area is regularly checked and improvements in staff training are made where necessary.

2.5 All staff who have been a victim of a violent incident have access to support services if required.

2.6 The organisation uses the Security Incident Reporting System (SIRS) to record details of physical assaults against staff in a systematic and comprehensive manner. This process is reviewed, evaluated and improvements are made where necessary.
Key Principle 2: Prevent and Deter

3.1 The organisation risk assesses job roles and undertakes training needs analyses for all employees, contractors and volunteers whose work brings them into contact with NHS patients and members of the public. As a result, the level of training on prevention of violence and aggression is delivered to them in accordance with NHS Protect’s guidance on conflict resolution training. The training is monitored, reviewed and evaluated for effectiveness.

3.2 The organisation ensures that staff whose work brings them into contact with NHS patients are trained in the prevention and management of clinically related challenging behaviour, in accordance with NHS Protect’s guidance. Training is monitored, reviewed and evaluated for effectiveness.

3.3 The organisation assesses the risks to its lone workers, including the risk of violence. It takes steps to avoid or control the risks and these measures are regularly and soundly monitored, reviewed and evaluated for their effectiveness.

3.4 The organisation distributes national and regional NHS Protect alerts to relevant staff and action is taken to raise awareness of security risks and incidents. The process is controlled, monitored, reviewed and evaluated.

3.5 The organisation has arrangements in place to manage access and control the movement of people within its properties and any associated grounds.

3.6 The organisation has systems in place to protect all its assets from the point of procurement to the point of decommissioning or disposal.

3.7 The organisation has departmental asset registers and records for business critical assets worth less than £5,000.

3.8 The organisation has clear policies and procedures in place for the security of all medicines and controlled drugs.

3.9 The organisation has policies and procedures in place to ensure prescription forms are protected against theft and misuse. These policies and procedures are reviewed, evaluated and updated as required.

3.10 Staff and patients have access to safe and secure facilities for the storage of their personal property.

3.11 The organisation records all security related incidents affecting staff, properties and assets in a comprehensive and systematic manner. Records made inform security management priorities and the development of security policies.

3.12 The organisation takes a risk-based approach to identifying and protecting its critical assets and infrastructure. This is included in the organisation’s policies and procedures.

3.13 In the event of increased security threats, the organisation is able to increase its security resources and responses.

3.14 The organisation has suitable lockdown arrangements for each of its sites, or for specific buildings or areas.

3.15 Where applicable, the organisation has clear policies and procedures to prevent and respond to a child or infant abduction. These are regularly tested, monitored and reviewed.
Key Principle 3: Hold to Account

4.1 The organisation has arrangements in place to ensure that security related incidents are investigated in a timely and proportionate manner and these arrangements are monitored, reviewed and evaluated.

4.2 The organisation is committed to applying all appropriate sanctions against those responsible for security related incidents.

4.3 The organisation has a communications strategy which allows for appropriate publicity of sanctions following security related incidents.

4.4 The organisation has a clear policy on the recovery of financial losses incurred due to security related incidents and can demonstrate its effectiveness.
The quality assurance programme

Overview

4.1 NHS Protect provides national leadership for all NHS anti-crime work and is responsible for strategic and operational matters in relation to security management and anti-fraud work in the NHS. A key part of this function and one of NHS Protect’s five strategic aims is to quality assure the delivery of anti-crime work with stakeholders to ensure that the highest standards are consistently applied.

4.2 The aim of the NHS anti-crime quality assurance programme is to ensure that quality requirements are fulfilled. This will be done through systematic measurement, comparison with standards, monitoring of processes and a continuous loop of feedback.

4.3 Using the security management standards set out in this document, NHS Protect will support organisations through regular benchmarking, compliance testing, and evaluation of effectiveness and value for money. The quality assurance programme also enables the analysis of trends and patterns in performance in relation to each standard for each organisation type. This will assist in providing comprehensive and focused support to organisations.

4.4 Additionally, NHS Protect will provide robust assurance to stakeholders, including participating organisations, NHS England and the Department of Health (DH). Using our strong links with regulators such as the Care Quality Commission (CQC), Health and Safety Executive (HSE) and Monitor, we will share information about the standards of anti-crime work to eliminate duplication of effort for providers.

4.5 Quality assurance of anti-crime work has been shown to drive up standards and NHS Protect has developed a flexible, responsive and transparent process for this. This will ensure that the anti-crime work carried out mitigates both national and local identified risks.

4.6 This section provides guidance on the quality assurance programme and should be used in conjunction with other relevant instructions and guidance that have been issued to support security management work.

These documents include:

- The NHS Standard Contract
- NHS Protect standards for providers - security management (as outlined in chapter 5 below)
- The document Conflict Resolution Training: implementing the learning aims and outcomes
- Meeting needs and reducing distress: Guidance for the prevention and management of clinically related challenging behaviour in NHS settings

4.7 This list is not exhaustive and additional guidance can always be sought from NHS Protect if required.

Security management quality assurance programme

4.8 The NHS Protect quality assurance programme comprises two main processes: assurance and assessment. Both are closely linked to the security management standards set out in this document.

4.9 The assurance process includes an annual self review against the standards, which is conducted by organisations and submitted to NHS Protect. The assessment process is conducted by NHS Protect’s Quality and Compliance team in partnership with the organisation.

Assurance and the self review tool

4.10 The self review tool (SRT) enables the organisation to produce a summary of the security management work conducted over the previous twelve months. Organisations are required to complete the SRT annually and return it to NHS Protect. The SRT also covers the key areas of activity outlined in the standards.

4.11 Upon completion, the SRT provides a red, amber or green (RAG) rating for each of the key areas and an overall RAG rating. Further
details of the red, amber and green ratings are outlined in paragraph 4.36.

4.12 Organisations should use the SRT in conjunction with their work planning. They can use it to review the progress made against the work plan. The SRT can also assist them in identifying risk areas and formulating objectives and tasks as they develop the work plan. Organisations can also use the SRT to monitor their compliance with the requirements of the standards throughout the year.

Assessment

4.13 The assessment process is a means of evaluating an organisation’s effectiveness in dealing with the security management risks it faces. The process is designed to be flexible, transparent and responsive to locally and nationally identified security management risks. Where required, we shall provide organisations with recommendations to support them in mitigating their risks.

4.14 If an organisation, in the judgement of the Quality and Compliance team, requires an assessment, one of four types of assessment will be carried out: full, focused, thematic or triggered.

Full assessment

4.15 A full assessment would normally be used when an organisation’s security management arrangements are identified as being at significant risk. Such an organisation may demonstrate some or all of the following areas of concern (the list is not exhaustive):

• The red, amber or green rating provided in the SRT is not supported by comments made in the SRT.
• Security management provision is lacking or inadequate.
• There are recommendations from previous assessments that have not been addressed.
• There is no evidence of a risk-based approach to security management work.
• The organisation is new or has started to provide significant additional services, and no previous history of effective security management work exists.
• There are significant gaps in NHS Protect-required activity across key areas of activity or NHS Protect priority areas.

• Significant concerns are raised by another part of NHS Protect.
• The member of the executive board responsible for overseeing security management work raises concerns regarding the quality of the local security management service received.
• A regulator such as the HSE or CQC raises concerns regarding the quality of the service received.

4.16 A full assessment is carried out on all the NHS Protect key areas of activity as outlined in the standards.

Focused assessment

4.17 A focused assessment is undertaken in cases where an organisation demonstrates a risk in a specific area of security management activity. A focused assessment is conducted on one or at most two of the key areas of activity, for example Strategic Governance or Inform and Involve.

4.18 A focused assessment might be conducted with organisations demonstrating some or all of the following characteristics (this list is not exhaustive):

• The red, amber or green rating provided in the SRT is not supported by comments made in the relevant section of the SRT.
• There is a lack of evidence of measurable outcomes from the work conducted to mitigate risk.
• There are gaps in one of the key areas of activity, for example Hold to Account.

Thematic assessment

4.19 A thematic assessment applies to a number of organisations and may be conducted regionally or across organisations of a similar type.

4.20 Driven primarily by NHS Protect and DH priority areas, thematic assessments focus on compliance, or on areas of concern identified by the Quality and Compliance team. New NHS Protect guidance, after a reasonable period given for it to be embedded in organisations, may be followed up by a thematic assessment.

4.21 Thematic assessments are likely to focus on a specific part of the standards, possibly only one standard rather than
Triggered assessments

4.22 Some organisations will not be selected for a full, focused or thematic assessment when the annual assurance is received. However, at any stage during the year, organisations may be selected for a triggered assessment. Triggered assessments are driven by emerging risk, normally of a serious nature, which may have come to the attention of the Quality and Compliance team through Senior Quality and Compliance Inspector (SQCI) liaison with other parts of NHS Protect. Reasons for a triggered assessment may include, but are not limited to, the following:

- a significant and adverse change in security management provision
- a significant failure to manage organisational security management risks
- an ongoing lack of engagement with NHS Protect’s anti-crime strategy
- a lack of positive and proactive engagement with NHS Protect staff over a significant period, with a failure to improve after this has been highlighted
- an ongoing failure to action recommendations from NHS Protect assessments, in spite of support and assistance offered

4.23 If the organisation is selected for a triggered assessment, this may be either a focused, full or thematic assessment.

4.24 Following a full, focused or thematic assessment, whether triggered or not, the organisation is provided with a written report which provides advice and guidance on driving up the quality and value for money of its security management work. The intended outcome is improved standards of work, measured by future self review and annual reports and assessments.

4.25 Other quality assurance and compliance activities, in addition to assessments, may also take place to support and develop security management work at NHS organisations. These could include one-to-one meetings with key personnel and meetings with audit committees.

4.26 The purpose of the security management quality assurance programme is to be constructive and supportive. The assurance and assessment processes do not focus solely on non-compliance with the standards; they also highlight compliance and outcomes achieved. Where standards are not being met, NHS Protect will provide advice, support and assistance to organisations in order to help them improve performance.

Assessment process

4.27 If an organisation is selected for assessment, at least four weeks’ notice will be given of any site visit. The SQCI conducting the assessment will notify the organisation of the dates for the assessment and will indicate the type of assessment and the areas that will be reviewed. The organisation will be asked to name a specific contact to make the arrangements for the site visit.

4.28 At this stage it is likely that the SQCI will request information from the organisation in relation to the areas that will be reviewed. This information enables the SQCI to formulate relevant questions before the assessment meeting and it helps in the review of evidence collected during the site visit. It is essential that any information requested is received by the SQCI within the deadline given. Failure to provide this information or the provision of late information is likely to extend the site visit and may have an impact on organisational compliance with standard 1.2.

4.29 During the site visit, the SQCI will wish to speak to the nominated security management specialist about the security management work carried out at the organisation. Depending on the area of enquiry and the type of assessment conducted, the SQCI may also wish to speak to the Security Management Director, the non-executive director with responsibility for security management and other key staff. The organisation will be informed of this and given timely notice to make arrangements for these interviews to take place.

4.30 Following the interviews and any additional request for materials, the SQCI will produce a series of recommendations for the organisation to action. The ratings and recommendations will be discussed at a closing meeting, which ideally will be on the same day as the assessment visit or very shortly afterwards. It is expected that the ratings and recommendations can be agreed at this stage.

4.31 A quality assessment report will follow within four weeks of the closing meeting. The report will outline the findings of the site visit in full and will include the recommendations discussed at the closing meeting. Within another four weeks,
the organisation will be expected to complete an action plan for the recommendations and return it to the SQCI.

4.32 Following this, the organisation will be expected to comply with NHS Protect’s review process. This will involve sending progress reports and audit committee minutes to NHS Protect to demonstrate progress against the recommendations made in the final report. The organisation will be advised of requirements in relation to the review process at the closing meeting and in writing.

4.33 Some organisations may have a review assessment, between nine and twelve months following the original assessment process. Review assessment site visits will take place when, in the opinion of the SQCI, one is necessary based on information received. The review assessment site visit should only focus on the recommendations made at the previous assessment, unless there are significant matters that have arisen in the meantime.

4.34 As indicated above, discussion and liaison are an essential part of the assessment process. Organisations and staff members have a number of opportunities to discuss the assessment process and the recommendations, including during the assessment itself, at the closing meeting and as part of ongoing liaison. For this reason, there is no formal appeal procedure. However, if the organisation is dissatisfied with any aspect of the assessment process, the matter may be raised in the first instance with the Quality and Compliance Lead (Security Management).

Performance ratings

4.35 As a result of both assurance and assessment processes, organisations will be rated as being red, amber or green depending on how well they have performed against NHS Protect standards. The benefits of this for organisations include:

- a clear snapshot of organisational progress against each of the standards
- an overall rating, which will assist with benchmarking against other organisations in similar groups or sectors
- the ability to monitor and measure ongoing improvement
- a means of assurance for DH and NHS England

4.36 The definitions for each performance rating are listed below.

NON-COMPLIANCE with the standard: RED.
A risk has been identified but no action has been taken to mitigate it, or the action taken is insufficient in scope.

PARTIAL COMPLIANCE with the standard but little or no impact of work undertaken: AMBER.
A risk has been identified and action has been taken to mitigate it. There is evidence of compliance through outputs. However, the effectiveness of work undertaken has not yet been evaluated or there is no reduction of the risk. There is therefore little or no evidence of outcomes.

FULL COMPLIANCE demonstrating impact of work undertaken: GREEN.
A risk has been identified, work has been carried out and the effectiveness of this work has been measured. The risk has been mitigated or significant progress has been made in mitigating the risk. Outcomes are therefore present.

4.37 Organisations which fulfil the requirements of a standard and can provide evidence of this through evaluation can determine performance to be green for that standard. Organisations which can provide evidence of activity carried out, but cannot yet demonstrate that the activity has been assessed for effectiveness will determine performance to be rated amber for that standard. Organisations which have carried out no activity or do not have evidence of sufficient activity will need to determine performance at the red rating. The rating reached for each standard contributes to an overall rating for the relevant key area of activity as well as an organisational rating for achievement against all of the standards.

Identifying and mitigating risks

4.38 Organisations should adopt a risk-based approach when determining the amount of resources required to achieve the highest performance rating for each standard. Organisations vary in size and needs and a risk-based approach ensures that appropriate resources are utilised to identify and address the security management needs of the organisation.

4.39 Local Security Management Specialists, Security Management Directors and any non-executive directors with security management responsibilities should analyse each standard, consider what action is required and utilise appropriate resources to ensure that the standard is met. By applying this method,
organisations should end up with a series of tasks which enable the development of a work plan.

4.40 The process that organisations should adopt in identifying and mitigating risks is as follows:

Risk

4.41 The organisation should identify and assess the security management risks it faces and put in place measures to address them. Nominated security management specialists should be working in areas where risk is present in order to maximise effectiveness. Working in areas where there is no security management risk is not an appropriate use of resources.

Objectives

4.42 Once areas of risk have been identified and assessed, the organisation and the nominated security management specialist should be very clear about their objectives, or what they want to achieve in relation to mitigating or addressing the risk. Objectives should be clearly formulated (for example, percentage reductions or increases), as this helps with measuring and demonstrating outcomes.

Task

4.43 The organisation should then carry out the appropriate tasks to meet the defined objectives.

Outputs

4.44 These are the products of the tasks performed to meet objectives. Outputs provide evidence that the task has been carried out but generally do not, on their own, provide evidence of outcomes. Outputs may include presentation materials, policies and procedures or terms of reference.

Outcomes

4.45 These are the pieces of evidence that demonstrate the effective addressing of identified risks and the fulfilment of defined objectives. Outcomes may include, among other things: staff survey results, case closure reports, evidence demonstrating awareness and understanding of policies among staff, and procedures to reduce risk.

4.46 Following this methodology is not compulsory, although organisations will be assessed on the evidence of outputs and outcomes.

Weightings

4.47 Some standards are weighted to reflect the overall importance of that particular standard in security management work. Standards are weighted to reflect areas where specific improvement is required nationally or where action is particularly required to mitigate organisational risk. The weightings reflect NHS Protect priorities and are subject to ongoing review.

4.48 Weightings may be changed to reflect new and emerging risks reflected in the standards. If an organisation does not conduct activity against a weighted standard, the overall RAG rating, either for the relevant key area of activity or for the self review as a whole is affected. Further information on weightings will be shared with providers and any queries may be directed to securitymanagementqa@nhsprotect.gsi.gov.uk.

Reasonable expectations

4.49 In order to make the working relationship between organisations and the Quality and Compliance team as effective as possible we have outlined what organisations can reasonably expect from us and what we can reasonably expect from organisations. Understanding these reasonable expectations (which are set out in Appendix 1) will help both parties make the most of working together.

Feedback

4.50 Your opinion counts and as part of our commitment to continuous improvement, we encourage feedback from stakeholders on the quality assurance programme. You can send your comments by email to securitymanagementqa@nhsprotect.gsi.gov.uk.
Strategic Governance

A red rating means non-compliance with the standard.

An amber rating means partial compliance with the standard. While the organisation has done work to meet the standard, this work has not been evaluated or it has not had a demonstrable impact.

A green rating means full compliance with the standard. The organisation has not only done work to meet the standard, but it has also evaluated the outcome of this work or can demonstrate its impact.

Rationale

An organisational culture that is focused on security management requires effective leadership and a high level of commitment from senior management. Identifying a senior individual to lead on the organisation’s security management strategy and security issues can help the organisation and its contracted providers to focus on their strategic security management priorities, ensure adequate resources are allocated to meeting them and deliver improvements across the organisation.

The nominated individual must be a member of the executive board or equivalent body, which may include, but is not limited to, the board of directors, the board of trustees or the governing body. Oversight of security management work should not be delegated to an individual below this level of seniority in the organisation.

A key tool to assist with a corporate approach will be an organisational security management strategy document. A security management strategy should be aligned with the three key principles for action as identified by NHS Protect: Inform and Involve, Prevent and Deter and Hold to Account.

Ratings

Organisation does not meet the standard

There is little or no evidence that a nominated member of the executive board, or equivalent body, oversees and provides strategic management and support for all security management work within the organisation.

In relation to security management work, there is little or no evidence that a nominated member of the executive board, or equivalent body, has ensured the provision of relevant and timely information upon request from the coordinating commissioner.

There is evidence of strategic management and support by a member of the executive board, or equivalent body, for all security management work within the organisation, but this person is not nominated to NHS Protect.

The nominated member of the executive board or equivalent body has not ensured there is a corporate/organisational strategy for security management work. Where a strategy is in place, this does not address the priorities included in the work plan arising from the self review tool and is not based on NHS Protect’s national strategy.
Organisation partially meets the standard

Not applicable to this standard.

Organisation meets the standard

A member of the executive board, or equivalent body, oversees and provides strategic management and support for all security management work within the organisation. There is evidence that these responsibilities are discharged effectively.

A member of the executive board, or equivalent body, has ensured the provision of relevant and timely information upon request from the coordinating commissioner.

A member of the executive board, or equivalent body, is nominated to NHS Protect.

Security management objectives are discussed and reviewed at a strategic level within the organisation and this is documented.

Where additional or corrective action is necessary, this is discussed and the appropriate actions are taken.

The nominated member of the executive board or equivalent body has ensured there is a corporate/organisational strategy document for security management work. The strategy document demonstrably addresses the priorities included in the work plan arising from the self review tool. It is based on NHS Protect’s national strategy.

Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect strategy document ‘Tackling crime against the NHS: a strategic approach’
- Confirmation received from NHS Protect that a member of the executive board or equivalent body has been nominated to NHS Protect
- Meeting minutes of the executive board or equivalent body
- Security management work plan
- Annual report on security management work
- Progress reports to the board or equivalent body
- Minutes of relevant meetings, action points and records of their execution
- Materials generated by NHS Protect’s quality assurance programme
- The organisation’s security management strategy
- Policy review process
- Meeting minutes, decisions, action points and records of their execution, particularly for decisions taken at board level
- Communications to staff directly attributed to the chief executive and/or board members, particularly communications to all staff
- Staff surveys
- Evidence of review and evaluation of policies and procedures
- Evidence of the implementation of any recommendations made
• Documents covering:
  o Roles and responsibilities, including those of the executive board member (or equivalent) responsible for security management work, the nominated security specialist (LSMS), associated functions (risk management, health and safety) and all staff
  o The organisation’s risk management strategy
  o The process for reviewing security incidents and identifying and implementing lessons learned
  o The way(s) in which staff should report a security incident (theft, criminal damage, security breach)
  o Monitoring and auditing of the effectiveness of the security management policy
Strategic Governance

Standard 1.2

The organisation’s audit committee chair, non-executive directors and board level senior management provide clear and demonstrable support and strategic direction for security management work. Evidence of proactive management, control and evaluation of security management work is present. If NHS Protect has carried out a quality assessment, the non-executive directors and board level senior management ensure recommendations made are fully actioned.

Rationale

In order for the organisation to adequately address security management risks, there must be proactive support for NHS Protect’s strategy at senior management level. This will ensure security management work meets organisational and NHS Protect requirements, and there is sufficient buy in for it at senior level. This will assist in mitigating security management risks.

N.B. References to board level senior management include, but are not limited to, the board of directors, the board of trustees or the governing body.

Ratings

Organisation does not meet the standard

There is little or no evidence of proactive support for security management work from senior management at the organisation.

Senior management demonstrates a lack of awareness of its responsibilities in relation to security management work and organisational objectives in this area.

Where there is an awareness of responsibilities, there is little or no evidence that senior management has discharged them effectively.

Senior management do not fully ensure the organisation’s compliance with the requirements of NHS Protect’s quality assurance programme.

Following an NHS Protect quality assessment, senior management do not ensure action plan recommendations are implemented and there is no evidence of demonstrable outcomes.

Updates on the implementation of action plan recommendations are not provided to NHS Protect upon request.

Organisation partially meets the standard

There is evidence of proactive support for security management work from senior management at the organisation.

There is evidence that senior management recognises its responsibilities in relation to security management work.

Support for the trained and nominated person carrying out security management work on the part of the organisation is present and evident.

Senior management fully ensures the organisation’s compliance with the requirements of NHS Protect’s quality assurance programme. This includes, but is not limited to, ensuring action plan recommendations are implemented following any NHS Protect quality assessment.

However, there is little or no evidence to indicate this work has been assessed for effectiveness by the organisation. There is little or no evidence of demonstrable outcomes from this work.
**Organisation meets the standard**

There is evidence of proactive support for security management work from senior management at the organisation.

There is evidence that senior management recognises its responsibilities in relation to security management work.

Support for the trained and nominated person carrying out security management work on the part of the organisation is present and evident.

Senior management fully ensures the organisation’s compliance with the requirements of NHS Protect’s quality assurance programme. This includes, but is not limited to, ensuring action plan recommendations are implemented following any NHS Protect quality assessment.

There is evidence of demonstrable outcomes from the implementation of action plan recommendations.

Updates on the implementation of action plan recommendations are provided to NHS Protect upon request, in line with NHS Protect’s review process.

Any corrective or preventative actions identified as a result of evaluation are implemented to ensure security management work continues to address organisational risks.

**Guidance, supporting documentation and evidence**

Organisations should consider the following (the list is not exhaustive):

- NHS Protect strategy document ‘Tackling crime against the NHS: a strategic approach’
- Meeting minutes, decisions, action points and records of their execution, particularly for decisions taken at board level
- Audit committee minutes
- Security management work plan
- Communications to staff directly attributed to the chief executive and/or board members, particularly communications to all staff
- Staff surveys
- Documentation arising from NHS Protect’s quality assurance programme
- Evidence of the implementation of any recommendations made, including those made by NHS Protect as part of the quality assurance programme
- NHS Audit Committee Handbook (relevant sections)
Strategic Governance

Standard 1.3

The organisation employs or contracts a qualified, accredited and nominated security specialist(s) to oversee and undertake the delivery of the full range of security management work.

Rationale

By appointing a security specialist trained and accredited by NHS Protect to oversee and undertake the delivery of the full range of security management work, the organisation will be able to apply a consistent and professional approach to security management. Having a qualified, accredited and nominated security specialist also helps to ensure that the organisation is a safe and secure place to work and deliver care.

Ratings

**Organisation does not meet the standard**

There is no evidence of a qualified and accredited security specialist being employed or contracted to oversee and undertake the delivery of security management work within the organisation.

There is a qualified and accredited security specialist employed or contracted to oversee and undertake the delivery of security management work within the organisation, but they are not nominated to NHS Protect.

The nominated security specialist does not update their skills or undertake continuing professional development.

The nominated security specialist does not attend the regional security management forums hosted by NHS Protect.

**Organisation partially meets the standard**

Not applicable to this standard.

**Organisation meets the standard**

There is a qualified and accredited security specialist employed or contracted to oversee and undertake the delivery of security management work within the organisation.

The security specialist is nominated to NHS Protect.

The security specialist attends all necessary training courses and undertakes continuing professional development to update their skills.

The security specialist attends the regional security management forums hosted by NHS Protect.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect strategy document ‘Tackling crime against the NHS: a strategic approach’
- Confirmation received from NHS Protect that a local security management specialist (LSMS) has been nominated to NHS Protect
- Attendance records for security management forums
- Training records held by NHS Protect
- Accreditation records held by NHS Protect
- Evidence of continuous professional development

Links

Care Quality Commission, ‘Guidance for providers on meeting the regulations’, Regulation 18
http://www.cqc.org.uk/sites/default/files/20150210_guidance_for_providers_on_meeting_the_regulations_final_01.pdf
Strategic Governance

Standard 1.4

The organisation allocates resources and investment to security management in line with its identified risks.

Rationale

Identifying the organisation's overarching and strategic security risks will help the organisation to ensure that its resources and investment are prioritised and targeted appropriately to mitigate these risks.

Ratings

Organisation does not meet the standard

There is little or no evidence of any strategic risk assessment work being carried out to identify security risks within the organisation.

Where strategic risk assessment work has been carried out, adequate resources have not been allocated to mitigate the identified risks within a reasonable timescale.

Identified security risks within the organisation have not been entered onto the risk register.

Where measures to mitigate identified risks have been included into an organisational work plan, the objectives of the work plan are not clear or measurable.

Organisation partially meets the standard

The organisation has carried out strategic risk assessment work to identify security risks within the organisation.

Identified security risks within the organisation have been entered onto the risk register. Where they have not, the reasons for this are clearly documented.

As a result of strategic risk assessment work, proportionate levels of resources and investment have been allocated to effectively progress security management work within the organisation.

There is an organisational work plan in place which sets out security management work required within the organisation. This has clear and measurable objectives. However, progress against the workplan is not regularly monitored at a senior level.

Organisation meets the standard

The organisation has carried out strategic risk assessment work to identify security risks within the organisation. Identified risks have been entered onto the risk register. Where they have not, the reasons for this are clearly documented.

Measures to mitigate identified security risks have been included into an organisational work plan. A proportionate level of resources and investment has been allocated to deliver against it.

There are clear and measurable objectives within the organisational work plan. Where necessary, additional resources and investment are allocated in year to address emerging risks.

(continues on next page)
Progress against the organisational work plan is regularly monitored at a senior level. The workplan reflects the priorities arising from assessment of the organisation’s risks. This ensures resources and investment allocated to security management work within the organisation are sufficient to mitigate identified risks.

Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect strategy document ‘Tackling crime against the NHS: a strategic approach’
- Security risk assessments clearly recorded in the organisational risk register
- Risk assessment materials
- Evidence of liaison with risk management staff within the organisation
- Evidence of risk monitoring being done at a senior level
- Relevant meeting minutes, action points and records of their execution
- Security management work plan
- Progress reports
- The previous year’s work plan, along with evidence of a link between its contents and actions reported
- The current year’s work plan, along with evidence of a link between actions reported against the previous work plan and the contents of the new one
Strategic Governance

Standard 1.5

The organisation reports annually to its executive board, or equivalent body, on how it has met the standards set by NHS Protect in relation to security management, and its progress on local priorities as identified in its work plan.

Rationale

An annual report to the organisation’s executive board or equivalent body, which may include, but is not limited to, the board of directors, the board of trustees or the governing body, is the main way for the organisation to report on performance against its security management objectives, both internally and externally. Reviewing its success or otherwise in achieving objectives will assist the organisation in planning ahead, driving up performance and verifying that it has the appropriate level of assurance in this area.

Review and sign off of the annual report should not be delegated to any other committee below the executive board, or equivalent body, within an organisation.

Ratings

Organisation does not meet the standard

There is no evidence that the organisation has completed an annual report demonstrating progress against security management objectives.

Where an annual report has been completed, it does not cover all key areas of security management activity as outlined in NHS Protect's strategy. The report does not provide a full update on actions taken to address security management risks as outlined in the work plan for that year. Where an NHS Protect quality assessment has been conducted, there is no update on the progress made against the action plan.

The annual report does not contain a fully completed self review against the standards or a statement of assurance. There is no evidence that the annual report has been reviewed or signed off by the organisation’s executive board or equivalent body.

Organisation partially meets the standard

Not applicable to this standard.

Organisation meets the standard

The annual report on security management work complies with NHS Protect’s guidance in relation to content, referring to all applicable standards for security management appropriately and providing a full update on progress against work plan objectives.

Where an NHS Protect quality assessment has been carried out, the annual report provides an update on the progress made against the action plan.

An appropriately signed statement of assurance is included in the annual report and the report is reviewed or signed off by the organisation’s executive board or equivalent body. A fully completed self review tool is included with the annual report.

Where standards have not been met, the reasons for this are documented and corrective action is suggested for the following year.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect strategy document: ‘Tackling crime against the NHS: a strategic approach’
- Annual report of security management work
- Completed self-review tool
- Relevant meeting minutes, action points and records of their execution
- Minutes from the meeting of the executive board, or equivalent body, at which the annual report has been approved
Key Principle 1: Inform and Involve

A red rating means non-compliance with the standard.

An amber rating means partial compliance with the standard. While the organisation has done work to meet the standard, this work has not been evaluated or it has not had a demonstrable impact.

A green rating means full compliance with the standard. The organisation has not only done work to meet the standard, but it has also evaluated the outcome of this work or can demonstrate its impact.

Inform and Involve

Standard 2.1

The organisation has an ongoing programme of work to raise awareness of security measures and security management in order to create a pro-security culture among all staff. As part of this, the organisation participates in all national and local publicity initiatives, as required by NHS Protect, to improve security awareness. This programme of work will be reviewed, evaluated and updated as appropriate to ensure that it is effective.

Rationale

Raising and maintaining security awareness among staff is a key part of creating a strong pro-security culture within organisations.

The aim of this work is to ensure that all employees receive the key information they need to understand how security affects them and what their role and responsibilities are in creating a safe and secure organisation.

In addition, participating in national and local initiatives can help the organisation raise awareness of its security work and encourage staff to take a proactive role in security management.

Ratings

Organisation does not meet the standard

The organisation has not raised awareness of security measures and security management among staff and has not created a pro-security culture.

There is some work within the organisation to raise and maintain security awareness, but it is limited in scope and reach.

The awareness work carried out does not take identified organisational risks into account and is not fully in line with NHS Protect strategic requirements.

The organisation has not participated in any national or local publicity initiatives, as required by NHS Protect, to improve security awareness.

Organisation partially meets the standard

The organisation has an ongoing programme of work to raise awareness of security measures and security management among all staff, based on local risk and needs and in line with NHS Protect’s strategy. A range of methods are used to reach the widest possible audience.

The organisation participates in all national and local publicity initiatives, as required by NHS Protect, to improve security awareness.

Advice is taken from the organisation’s communications staff, where appropriate, and from the Deterrence

(continues on next page)
Organisation meets the standard

The organisation has an ongoing programme of work to raise awareness of security measures and security management among all staff using a range of methods that are appropriate to different staff groups.

There is evidence that presentations and other awareness materials are targeted to specific staff groups.

The organisation meaningfully evaluates the success of the programme of work and measures levels of awareness.

The results of the evaluation inform planning for future awareness work.

Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect strategy document ‘Tackling crime against the NHS: a strategic approach’
- Security awareness presentations
- Corporate intranet pages and materials
- Staff newsletters and team briefs
- Leaflets and posters
- Evaluation of awareness work
- Staff surveys
- Work plans
- Contents of the induction programme
- Training learning aims and outcomes
- Lesson plans
- Trainer notes
- Evaluation forms
- Training evaluation results
- Induction materials
- Presentation evaluations
- Staff surveys
- Evidence of where awareness-raising work has been evaluated and changed to maximise its impact
- Organisational risk assessments
- Meeting minutes, action points and records of their execution
Links

Care Quality Commission, ‘Guidance for providers on meeting the regulations’, Regulation 15
http://www.cqc.org.uk/sites/default/files/20150210_guidance_for_providers_on_meeting_the_regulations_final_01.pdf

Health and Safety at Work Act 1974

Management of Health and Safety at Work Regulations 1999
Inform and Involve

Standard 2.2

The organisation develops and maintains effective relationships and partnerships with local and regional anti-crime groups and agencies to help protect NHS staff, properties and assets.

Rationale

Developing effective relationships and partnerships with anti-crime groups and agencies can help all involved to deliver shared objectives and gain a better understanding of their individual roles and responsibilities.

Ratings

Organisation does not meet the standard

There is no evidence that the organisation has developed or maintained effective relationships or partnerships with local and regional anti-crime groups and agencies.

There may be some arrangements, but these do not cover the whole scope of the standard in relation to protecting staff, properties and assets.

Organisation partially meets the standard

The organisation can provide evidence that it has developed and maintained effective relationships and partnerships with anti-crime groups and agencies.

There is little or no evidence that the organisation regularly evaluates the effectiveness of these relationships and partnerships.

Organisation meets the standard

There are positive outcomes as a result of the development and maintenance of relationships in relation to protecting staff, properties and assets.

Relationships are regularly reviewed for effectiveness.

Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- Correspondence or documentation relating to joint initiatives
- Agendas, minutes and action points and records of their execution
- Investigations demonstrating the effectiveness of local relationships and partnerships, even when no sanctions or redress are obtained
- Service level agreements
Inform and Involve

Standard 2.3

The organisation ensures that security is a key criterion in any new build projects, or in the modification and alteration (e.g. refurbishment or refitting) of existing properties. The organisation demonstrates effective communication between risk management, capital projects management, estates, security management and external stakeholders to discuss security weaknesses and to agree a response.

Rationale

As NHS services are constantly evolving, the organisation may need to commission new properties or the modification and alteration of existing ones. Providing a secure environment should be a key consideration in this work.

Security requirements should be evaluated at the briefing, planning and design stages of the new build or refurbishment project, using a risk-based approach. Outcomes of this evaluation should be documented.

Effective communication between different units within the organisation, as well as with external stakeholders, is essential to delivering a coordinated and proportionate response to identified security weaknesses.

Ratings

**Organisation does not meet the standard**

There is no evidence of a cross-organisational response to security weaknesses, involving risk management, capital projects management, estates, security management and external stakeholders.

Risk assessments of properties from a security perspective are not undertaken or are limited in scope. There may be some work to provide for a secure environment in the design of new, modified or altered premises, but it is not carried out continuously, or in a risk-based manner.

There may be some evidence of a cross-organisational response to security weaknesses, but this is limited in the context of the standard.

**Organisation partially meets the standard**

The organisation has adopted a cross-organisational approach to tackling security weaknesses, involving risk management, capital projects management, estates, security management and external stakeholders.

The cross-organisational approach has led to an agreed response to security weaknesses.

Risk assessments of properties from a security perspective have been carried out but resulting actions have not been completed.

There is little or no evidence that the organisation has reviewed or evaluated the effectiveness of its cross-organisational approach to tackling security weaknesses, or its work to provide for a secure environment in the design of its properties.
Orgmisation meets the standard

There is evidence that the organisation evaluates the effectiveness of its cross-organisational approach to addressing security weaknesses and that, where appropriate, changes are made to increase its benefits.

Risk assessments of properties from a security perspective are carried out and resulting actions are completed.

Where appropriate, the results from this evaluation lead to specific changes in the design of properties.

Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- Minutes of meetings where risk management, capital projects management, estates, security management and external agencies have worked on a joint approach to tackling security weaknesses
- NHS Protect guidance found on the Safe and Secure Health Facilities website [http://www.sshf.nhs.uk/sfh](http://www.sshf.nhs.uk/sfh)
- ACPO Secured by Design initiative
- Evaluation of the cross-organisational approach to tackling security weaknesses and evidence of changes made as a result
- Meeting minutes, action points and records of their execution
- Examples of work done by the cross-organisational group
- Security reports and surveys
- Minutes of estates management meetings which include security elements
- Evidence of a reduction in security breaches
- Positive crime pattern analysis
- Outcomes of staff surveys where an improved sense of security can be shown
- Evidence of risk assessments conducted on the properties
- Examples of security risks being pro-actively designed out of newly built, modified or altered properties, and evidence of how this has worked
Inform and Involve

Standard 2.4

All staff know how to report a violent incident, theft, criminal damage or security breach. Their knowledge and understanding in this area is regularly checked and improvements in staff training are made where necessary.

Rationale

Incident reporting enables the organisation to formally record events, and provides an opportunity to learn lessons, oversee performance and make sure that systems are put in place to prevent incidents from reoccurring.

For these purposes it is essential that staff know how to report incidents and that their knowledge and understanding is regularly checked to ensure they remain up to date on local policies and procedures. Staff training and staff awareness of reporting systems are key elements of meeting this standard.

Ratings

**Organisation does not meet the standard**

There is little or no evidence to show that staff know how to report a violent incident, theft, criminal damage or security breach.

There may be some work to support staff in reporting security related incidents, but this is not carried out systematically across the organisation.

**Organisation partially meets the standard**

There is evidence of systematic and coordinated measures in place across the organisation to enable staff to report security related incidents, but there is little or no evidence to suggest that staff know how to report security related incidents; and there are no measures in place to ensure that reporting procedures are effective.

**Organisation meets the standard**

The organisation can provide evidence of ongoing work to raise awareness of reporting of security related incidents among all staff. This is done using a variety of methods appropriate to different staff groups.

Staff know how to report security related incidents.

There is evidence that the organisation uses sound data to regularly evaluate the effectiveness of its reporting awareness work.

Where appropriate, the results from the evaluation lead to improvements in the organisation’s reporting awareness work.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect strategy document ‘Tackling crime against the NHS: a strategic approach’
- Learning aims and outcomes
- Lesson plans
- Trainer notes
- E-learning
- Evaluation forms
- Evaluation of the training
- Staff awareness surveys
- Evidence of a link between feedback received, evaluation and changes to the training
- Sample of incident reports for violent incidents, theft, criminal damage and security breaches
- Incident analysis using local reporting systems, providing evidence that reporting is taking place and that staff understand the reporting process
- Incident reporting policies and procedures (this may be a free standing incident reporting policy or a part of the security policy)
- SIRS input in relation to security breaches

Links

Health, Safety and Wellbeing Partnership Group
health-safety-and-wellbeing-partnership-group-hswpg
Inform and Involve

Standard 2.5

All staff who have been a victim of a violent incident have access to support services if required.

Rationale

All staff have a right to feel safe and secure in their working environment and to be protected from physical or verbal abuse. The Health and Safety at Work Act 1974 places a legal duty on employers to ensure, as far as is reasonable and practicable, that their staff work in a safe and secure environment and that their welfare is considered in any work-related activity.

However, sometimes things go wrong and in these cases it is important that the organisation provides the member of staff involved with appropriate support. Being a victim of a violent incident can be a traumatic experience and the individual may require different types of support to assist them in their recovery.

Ratings

Organisation does not meet the standard

There is no evidence of support services being made available to staff who have been victims of violent incidents.

There may be some measures in place to support victims of violence, but there is no evidence that they are comprehensive enough or that they have been made available to all victims.

Organisation partially meets the standard

There is evidence of systematic and comprehensive measures in place across the organisation to ensure that staff who have been a victim of a violent incident have access to support services if required.

There is little or no significant evidence to suggest that the support measures in place for staff who are victims of violence are effective.

Organisation meets the standard

Staff who have been victims of a violent incident have access to support services should they require it.

The organisation has evaluated the effectiveness of the support services available to victims of violent incidents.

Where appropriate, evaluation results feed into improvements of the support services.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect strategy document ‘Tackling crime against the NHS: a strategic approach’
- The NHS Security Management Manual, in particular the section on Developing a Policy for the Management of Violence and Aggression
- Local policy for the management of violence and aggression
- Guidance and advice provided through specific NHS Protect literature, such as the ‘Not part of the job’ booklets
- Staff surveys, in particular those looking at knowledge of support services
- Feedback from users of support services
- Sample of incident reports versus support service usage to test for take up
- Evidence of a link between feedback, evaluation and changes to the support services

Links

Health, Safety and Wellbeing Partnership Group
health-safety-and-wellbeing-partnership-group-hswpg

Victim Support
https://www.victimsupport.org.uk
Inform and Involve
Standard 2.6

The organisation uses the Security Incident Reporting System (SIRS) to record details of physical assaults against staff in a systematic and comprehensive manner. This process is reviewed, evaluated and improvements are made where necessary.

Rationale

SIRS is an online tool which enables organisations to report their security incidents to NHS Protect, including physical assaults against staff. Users can enter their data directly into SIRS as well as importing data from other risk management systems.

Capturing information in this way helps organisations and NHS Protect to better understand the pattern and nature of physical assaults against staff and enables the development of appropriate ways to mitigate this risk.

Ratings

Organisation does not meet the standard

The organisation does not use SIRS to record physical assaults against staff.

The organisation may use SIRS to record some physical assaults against staff but this is not done in a systematic and comprehensive manner.

The use of SIRS is not covered by the organisation’s incident reporting policies and procedures.

Organisation partially meets the standard

Physical assaults against staff are recorded on SIRS in a systematic and comprehensive manner.

The use of SIRS is covered by the organisation’s incident reporting policies and procedures.

There is little or no evidence to demonstrate that regular review and evaluation of SIRS reporting has taken place.

Organisation meets the standard

Physical assaults against staff are recorded on SIRS in a systematic and comprehensive manner.

The use of SIRS is covered by the organisation’s incident reporting policies and procedures.

SIRS reporting is regularly and soundly reviewed and evaluated. Where necessary, findings lead to improvements.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect document ‘Tackling crime against the NHS a strategic approach’
- NHS Protect document ‘Tackling Violence against staff: Explanatory Notes for reporting procedures’ (Updated 2009)
- Reported physical assaults (RPA) returns (indicating use of SIRS)
- Inclusion of SIRS reporting within the job description of appropriate post holders
- SIRS upload reports
- Evidence of consistency between the number of records held within SIRS and records held within local incident reporting systems
- Incident reporting policies and procedures covering the use of SIRS
- Evidence of the reporting of SIRS data at board and committee level
**Key Principle 2: Prevent and Deter**

A **red** rating means non-compliance with the standard.

An **amber** rating means partial compliance with the standard. While the organisation has done work to meet the standard, this work has not been evaluated or it has not had a demonstrable impact.

A **green** rating means full compliance with the standard. The organisation has not only done work to meet the standard, but it has also evaluated the outcome of this work or can demonstrate its impact.

---

### Prevent and Deter

**Standard 3.1**

The organisation risk assesses job roles and undertakes training needs analyses for all employees, contractors and volunteers whose work brings them into contact with NHS patients and members of the public. As a result, the level of training on prevention of violence and aggression is delivered to them in accordance with NHS Protect’s guidance on conflict resolution training. The training is monitored, reviewed and evaluated for effectiveness.

---

**Rationale**

It is important that staff feel safe in their working environment. Violent behaviour not only affects them personally but it also has a negative impact on the delivery of patient care.

Conflict resolution training (CRT) is an essential preventative tool in tackling violence and aggression against staff. It is clearly not enough to react to incidents after they occur; ways of reducing the risk of incidents occurring and preventing them from happening in the first place must be found.

---

**Ratings**

**Organisation does not meet the standard**

There is little or no evidence that the organisation risk assesses job roles and undertakes training needs analyses for all employees, contractors and volunteers whose work brings them into contact with NHS patients and members of the public.

The organisation risk assesses job roles and undertakes training needs analyses for all employees, contractors and volunteers whose work brings them into contact with NHS patients and members of the public. However, this has not resulted in staff being correctly identified as requiring training on prevention of violence and aggression.

Where training is delivered, this does not follow current NHS Protect guidance.

---

**Organisation partially meets the standard**

The organisation risk assesses job roles and undertakes training needs analyses for all employees, contractors and volunteers whose work brings them into contact with NHS patients and members of the public. This leads to staff being correctly identified as requiring training on prevention of violence and aggression.

The risk based approach leads to staff receiving a level of training on prevention of violence and aggression which is equal to or greater than that specified within NHS Protect guidance.

The organisation does not regularly review and evaluate the training delivered to ensure it is effective.
**Organisation meets the standard**

The organisation risk assesses job roles and undertakes training needs analyses for all employees, contractors and volunteers whose work brings them into contact with NHS patients and members of the public. This leads to staff being correctly identified as requiring training on prevention of violence and aggression.

The risk-based approach leads to staff receiving a level of training on prevention of violence and aggression which is equal to or greater than that specified within NHS Protect guidance.

The organisation regularly reviews and evaluates the training delivered and can demonstrate it is effective. Where necessary, findings lead to improvements being made.

**Guidance, supporting documentation and evidence**

Organisations should consider the following (the list is not exhaustive):

- NHS Protect document ‘Tackling crime against the NHS: a strategic approach’
- NHS Protect guidance ‘Conflict Resolution Training: implementing the learning aims and outcomes’
- Skills for Health document ‘UK Core Skills Training Framework’, subject 4
- Skills CFA document ‘Prevention and Management of Violence in the Workplace: National Occupational Standards’
- Reported Physical Assaults (RPA) statistics
- Strategy for delivery of CRT across the organisation
- Risk assessment records
- Records of training needs analyses
- CRT learning aims and outcomes
- CRT lesson plans, presentations and training materials
- Delegate feedback
- Training records
- Knowledge check
- Training evaluation

**Links**

Meeting needs and reducing distress: Guidance on the prevention and management of clinically related challenging behaviour in NHS settings  
http://www.nhsprotect.nhs.uk/reducingdistress

Conflict Resolution Training guidance  
http://www.nhsbsa.nhs.uk/Protect

Health, Safety and Wellbeing Partnership Group  
Health and Safety at Work Act 1974

Management of Health and Safety at Work Regulations 1999

Care Quality Commission, ‘Guidance for providers on meeting the regulations’, Regulations 18 and 19
http://www.cqc.org.uk/sites/default/files/20150210_guidance_for_providers_on_meeting_the_regulations_final_01.pdf
Prevent and Deter

Standard 3.2

The organisation ensures that staff whose work brings them into contact with NHS patients are trained in the prevention and management of clinically related challenging behaviour, in accordance with NHS Protect’s guidance. Training is monitored, reviewed and evaluated for effectiveness.

Rationale

It is important that staff feel safe in their working environment. Training in the management of clinically related challenging behaviour in accordance with NHS Protect’s guidance will help achieve such a safe and controlled working environment.

Ratings

Organisation does not meet the standard

There is little or no evidence the organisation ensures that staff whose work brings them into contact with NHS patients are trained in the prevention and management of clinically related challenging behaviour.

A risk-based approach is not taken when deciding on the level of training to be delivered to staff. This results in staff receiving insufficient training for their level of interaction with NHS patients who may display clinically related challenging behaviour.

Where training is delivered, this does not follow current NHS Protect guidance.

Organisation partially meets the standard

The organisation ensures that staff whose work brings them into contact with NHS patients are trained in the prevention and management of clinically related challenging behaviour.

In accordance with NHS Protect guidance, a risk-based approach is taken when deciding on the level of training to be delivered. Staff receive a level of training which is equal to or greater than that specified within NHS Protect guidance.

The training delivered follows current NHS Protect guidance.

The organisation does not regularly review and evaluate the training delivered to ensure it is effective.

Organisation meets the standard

The organisation ensures that staff whose work brings them into contact with NHS patients are trained in the prevention and management of clinically related challenging behaviour.

In accordance with NHS Protect guidance, a risk-based approach is taken when deciding on the level of training to be delivered. Staff receive a level of training which is equal to or greater than that specified within NHS Protect guidance.

The training delivered follows current NHS Protect guidance.

The organisation regularly reviews and evaluates the training delivered to ensure it is effective. Where necessary, findings lead to improvements being made.
**Guidance, supporting documentation and evidence**

Organisations should consider the following (the list is not exhaustive):

- NHS Protect document ‘Meeting needs and reducing distress: Guidance on the prevention and management of clinically related challenging behaviour in NHS settings’
- Skills for Health document ‘UK Core Skills Training Framework’, subject 4
- Skills CFA document ‘Prevention and Management of Violence in the Workplace: National Occupational Standards’
- Reported Physical Assaults (RPA) statistics
- Training needs analyses
- Risk assessments
- Management of violence & aggression policy
- Lesson plan
- Training materials
- Training records
- Training evaluation
- Delegate feedback analyses
Prevent and Deter
Standard 3.3

The organisation assesses the risks to its lone workers, including the risk of violence. It takes steps to avoid or control the risks and these measures are regularly and soundly monitored, reviewed and evaluated for their effectiveness.

Rationale

It is essential that staff feel safe and secure, so that they can perform their duties free from the fear of violence. They must also be confident that the organisation is committed to taking effective action and providing support if they find themselves in a threatening environment and need help. This should be backed up by robust procedures.

Due to the nature of their work, lone workers need to be provided with additional support, as well as training, to deal with increased risks. At the same time the organisation should empower staff to take a greater degree of responsibility for their own safety and security.

In NHS Protect’s definition, ‘lone working’ is ‘any situation in which someone works without a colleague nearby, or when someone is working out of sight or earshot of another colleague’.

Ratings

**Organisation does not meet the standard**

There is little or no evidence to demonstrate the organisation assesses the risks to its lone workers.

Where risk assessment work is undertaken, this is not done in a systematic or effective manner.

There is little or no evidence to demonstrate the organisation has taken steps to avoid or control the risks to its lone workers.

**Organisation partially meets the standard**

The organisation assesses the risks to its lone workers.

Risk assessments are undertaken in a systematic and effective manner.

Steps are taken to avoid or control the risks to lone workers.

There is little or no evidence the organisation reviews and evaluates its systems, and the steps taken, to avoid or control the risks to its lone workers.

**Organisation meets the standard**

The organisation assesses the risks to its lone workers.

Risk assessments are undertaken in a systematic and effective manner and steps are taken to avoid or control the risks to lone workers.

The organisation regularly reviews and evaluates its systems to avoid or control the risks to its lone workers. Where necessary, findings lead to improvements being made.

The organisation monitors the steps taken to avoid or control the risks to its lone workers and can demonstrate these are adhered to by staff.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect document ‘Tackling crime against the NHS: a strategic approach’
- NHS Protect document ‘A guide for the better protection of lone workers in the NHS’
- Reported physical assaults on NHS staff figures
- Policies and procedures on lone working
- Strategy for the delivery of training to lone workers across the organisation
- Risk assessment records
- Training needs analyses
- Lone worker learning aims and outcomes
- Lone worker training lesson plans, presentations and training materials
- Delegate feedback
- Training records
- Training evaluation
- Examples of information sharing
- Post incident action, including reporting and reviews
- Use of lone worker devices
- Contingency planning documents

Links

NHS Protect document: Developing a policy for the protection of lone workers
http://www.nhsbsa.nhs.uk/4248.aspx

NHS Lone Worker Protection Service
http://www.nhsbsa.nhs.uk/4248.aspx

Lone working framework agreement

Lone working framework model contract

Lone Worker estate mapping exercise

POSHH document: Improving safety for lone workers: A guide for lone workers

POSHH document: Improving safety for lone workers: A guide for managers

HSE document: Working Alone, Health and guidance on the risks of lone working
http://www.hse.gov.uk/pubns/indg73.pdf
Defra, Dealing with irresponsible dog ownership: Practitioner’s manual

Contract award notice

Lone working framework schedules

British Security Industry Association
http://www.bsia.co.uk/sections/lone-workers.aspx
Prevent and Deter
Standard 3.4
The organisation distributes national and regional NHS Protect alerts to relevant staff and action is taken to raise awareness of security risks and incidents. The process is controlled, monitored, reviewed and evaluated.

Rationale
NHS Protect issues alerts to keep NHS organisations informed of an immediate potential security risk or threat. It is the responsibility of the organisation to ensure alerts are circulated to all relevant staff, so appropriate action can be taken immediately to reduce the organisation’s exposure to the risk or threat.

The process for doing this should be controlled, monitored, reviewed and evaluated regularly to ensure it remains relevant and appropriate.

Ratings

Organisation does not meet the standard
There is little or no evidence that the organisation distributes national or regional NHS Protect alerts to relevant staff.

The organisation may have issued some national or regional NHS Protect alerts to staff, but this does not include all relevant alerts.

Organisation partially meets the standard
There is evidence that the organisation issues all relevant national or regional NHS Protect alerts to staff.
The organisation has a process to identify the appropriate staff to receive the alerts.
The organisation can demonstrate that there is a system in place to control the issue of alerts, which meets statutory requirements.
In addition, NHS Protect guidance in relation to the issue, distribution and withdrawal of alerts has been taken into account.
There is little or no evidence that the organisation has monitored, reviewed or evaluated the issue of national and regional NHS Protect alerts to see whether they have raised awareness of the issues communicated through them.

Organisation meets the standard
The organisation uses sound data to evaluate the success of the alert process and measures the levels of awareness generated by it.
Where appropriate, the results of the evaluation inform the process for issuing alerts in order to maximise its effectiveness.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect strategy document ‘Tackling crime against the NHS: a strategic approach’
- NHS Protect guidance on the request and issue of an NHS security management alert
- Evidence that the organisation has issued all relevant publicity alerts
- Evidence that the organisation has withdrawn relevant publicity alerts
- Process for the identification of relevant staff
- A process for receipt, distribution and withdrawal of NHS Protect alerts which is in line with NHS Protect guidance
- Confidentiality – NHS Code of Practice
- Data Protection Act 1998
- DH guidance on the Data Protection Act 1998
- Compliance Advice – Violent Warning Markers: Use in the Public Sector
- Use and Disclosure of Health Data
- Human Rights Act 1998
- Home Office guidance on publicising anti-social behaviour orders (ASBOs)
- Evaluation of the regional and national alert processes and procedures
- Evidence of where the regional and national alert processes and procedures have been changed to maximise their impact in the light of evaluation
Prevent and Deter

Standard 3.5

The organisation has arrangements in place to manage access and control the movement of people within its properties and any associated grounds.

Rationale

Most NHS properties and grounds are, by their nature, open environments which contain security-sensitive and high risk areas. The risk may arise from the presence of specific patient or client groups, high value items (e.g. medical devices and equipment), medicines, consumables, or patient and staff personal items.

The right combination of access control systems, policies and procedures can enable the organisation to manage how, when and where people can move around properties and grounds. This helps it maintain a secure environment and reduce opportunities for crime. However, a uniform approach to managing access and the movement of people is unlikely to have the desired outcomes; the correct approach is one based on a risk assessment. The outcome of security risk assessments relating to access control should be documented.

Ratings

Organisation does not meet the standard

There is no evidence that the organisation has a way to comprehensively manage access and control the movement of people within its properties and grounds.

There may be some work to manage access and control the movement of people at the organisation’s site(s), but it is not systematic or comprehensive.

There is little or no evidence that the organisation carries out, or documents, risk assessments in this area.

Organisation partially meets the standard

There is evidence of comprehensive arrangements for managing access and controlling the movement of people on the organisation’s properties and grounds.

There is evidence the organisation carries out and documents risk assessments in this area. There is little or no evidence that the organisation reviews or evaluates its arrangements for managing access and controlling the movement of people to bring about improvements in security.

Organisation meets the standard

There is evidence the organisation carries out and documents risk assessments in relation to managing access and controlling the movement of people in its properties and grounds. Where necessary, findings lead to improvements being made.

There is evidence that the organisation regularly evaluates the arrangements for managing access and controlling the movement of people in the organisation’s properties and grounds.

Where appropriate, the results from the evaluation lead to improvements in the arrangements for managing access and controlling the movement of people at the organisation.
**Guidance, supporting documentation and evidence**

Organisations should consider the following (the list is not exhaustive):

- The NHS Security Management Manual (particularly the chapter on access controls)
- NHS Protect guidance found on the Safe and Secure Health Facilities website [http://www.sshf.nhs.uk/sfh](http://www.sshf.nhs.uk/sfh)
- ACPO Secure by Design Initiative
- Organisational access risk assessments
- Meeting minutes, action points and records of their execution
- LSMS, estates and human resources processes for requesting, issuing and returning access control devices
- Evidence of a reduction in security breaches
- Outcomes of staff surveys where an improved sense of security can be shown
- Examples of reviews of arrangements for managing access and controlling the movement of people at the organisation
- Examples of where the results of the evaluation have led to improvements in the arrangements for managing access and controlling the movement of people at the organisation
Prevent and Deter

Standard 3.6

The organisation has systems in place to protect all its assets from the point of procurement to the point of decommissioning or disposal.

Rationale

Procurement may generally be considered under the remit of anti-fraud work. However, certain assets may have in-built security features fitted to them as a result of a proactive request made during the procurement process. By protecting its assets throughout their entire life-cycle – procurement and purchase, delivery, deployment and use, maintenance and repair, decommissioning and disposal – the organisation will reduce the risk of potential losses and interrupted service delivery as a result of theft, loss and damage.

At different stages in its life-cycle an asset is likely to be subject to different security risks; these need to be properly understood and managed.

Ratings

**Organisation does not meet the standard**

The organisation is unable to provide evidence of comprehensive and systematic arrangements for the protection of assets from the point of procurement to the point of decommissioning or disposal.

There may be some work by the organisation to protect its assets, but it is not comprehensive or systematic and/or it does not cover the entire life-cycle of the asset from procurement to decommissioning or disposal.

**Organisation partially meets the standard**

There is evidence that the organisation has comprehensive and systematic arrangements for the protection of its assets from the point of procurement to the point of decommissioning or disposal.

There is little or no evidence that the organisation has reviewed or evaluated its arrangements for the protection of assets to determine how they could be improved.

**Organisation meets the standard**

There is evidence that the organisation regularly evaluates its arrangements for the protection of its assets to ensure they are effective.

Where appropriate, evaluation results lead to improvements in the arrangements to protect assets at the organisation.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect guidance on the security and management of NHS assets, including Appendix 1 – Checklist for assessing risks to NHS assets
- The organisation’s policies and procedures which describe security measures to be applied when assets are delivered
- ‘Goods in’ instructions and protocols to ensure the security of assets from the point of manufacture to the point of delivery to the purchasing department
- Allocation of responsibility for the security of assets to the nearest appropriate member of staff (for example a departmental manager)
- Meeting minutes, action points and records of their execution
- Inclusion of goods worth £5,000 or more in the asset register
- Organisational arrangements to ensure that disposal or decommissioning of an item is carried out in line with current legislation
- A process for ensuring that assets that are still usable but no longer required by the organisation are subject to appropriate due diligence checks before being given as a gift to charitable organisations, to ensure that they are not used in a way that could compromise the organisation
- The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
- Data Protection Act 1998
- Evidence of a reduction in items going missing
- Examples of reviews of the arrangements for the protection of the organisation’s assets
- Examples of the results of evaluation leading to improvements in the arrangements for the protection of the organisation’s assets
- Examples of risk assessments that have been carried out

Links

Care Quality Commission, ‘Guidance for providers on meeting the regulations’, Regulation 15
http://www.cqc.org.uk/sites/default/files/20150210_guidance_for_providers_on_meeting_the_regulations_final_01.pdf
Prevent and Deter
Standard 3.7
The organisation has departmental asset registers and records for business critical assets worth less than £5,000.

Rationale
The loss, theft or damage of high risk, business critical assets of any value can have a critical impact on the delivery of patient care, on business continuity and on the reputation of the organisation.

Although this is not stipulated as a requirement in standing orders or standing financial instructions, NHS Protect has produced guidance to encourage healthcare providers to adopt departmental asset registers and records for business critical assets under £5,000 as part of good governance arrangements. The aim is to ensure that organisations have records of high risk, business critical assets.

Ratings

Organisation does not meet the standard
There is little or no evidence that the organisation has departmental asset registers and records for high risk, business critical assets worth less than £5,000.

There may be evidence of some arrangements in place to record high risk, business critical assets worth less than £5,000, but any asset registers created as a result are not current, comprehensive or systematically used across the organisation.

Organisation partially meets the standard
There is evidence that the organisation has departmental asset registers and records for high risk, business critical assets worth less than £5,000.

The departmental asset registers and records are current, comprehensive and systematically used across the organisation.

There is little or no evidence that the organisation has regularly and soundly audited or evaluated departmental asset registers and records to ensure they are effective.

Organisation meets the standard
There is evidence that the organisation undertakes regular and sound evaluations or audits of departmental asset registers and records for high risk, business critical assets worth less than £5,000.

Where appropriate, the results from the evaluations or audits lead to improvements in departmental asset registers and records.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect Guidance on the security and management of NHS assets, including Appendix 1 - Checklist for assessing risks to NHS assets
- Policies and procedures for departmental asset registers and records for high risk assets under £5,000, including protocols for allocation of responsibility to ensure that the register remains current
- Copies of current departmental asset registers and records for high risk assets under £5,000
- Evidence that all high risk, business critical assets under £5,000 in value are appropriately recorded in departmental asset registers and records
- Evidence that all departments adhere to the requirement, for example this may be recorded in policies and procedures
- Learning aims and outcomes of training on the departmental asset registers and records
- Training records
- Meeting minutes, action points and records of their execution
- Evidence of a reduction in losses
- Examples of reviews and/or audits of departmental asset registers carried out to ensure their effectiveness
- Examples of the results of the evaluation and/or audits leading to improvements in departmental asset registers and records
- Evidence that the asset registers are available for audit purposes at all times
- Policies making heads of department responsible for asset registers and records for high risk assets under £5,000
- Audit reports on control of assets worth under £5,000
- Risk assessments to determine which high risk assets under £5,000 are critical to business operations
Prevent and Deter

Standard 3.8

The organisation has clear policies and procedures in place for the security of all medicines and controlled drugs.

Rationale

Good governance and security arrangements in relation to the safe management of all medicines and controlled drugs (CDs) and medical gas cylinders should exist in all healthcare settings. This requirement is set out in legislation, for example in The Controlled Drugs (Supervision of Management and Use) Regulations 2013. NHS Protect’s medicine security self-assessment toolkit for providers builds on existing legislation to support organisations in their assessment of the secure management and storage of medicines and CDs.

Ratings

**Organisation does not meet the standard**

There is no evidence that the organisation has clear policies and procedures in place for the security of medicines and controlled drugs.

The organisation may have some arrangements in place for the security of medicines and controlled drugs, but they do not comply with current legislation and NHS Protect guidance.

**Organisation partially meets the standard**

There are clear policies and procedures in place for the security of medicines and controlled drugs, and they are supported by the organisation’s executive board or equivalent body.

The policies and procedures are up to date and comply with current legislation and NHS Protect guidance.

There is little or no evidence that the organisation regularly and soundly reviews or evaluates the safe and secure management of medicines and controlled drugs.

**Organisation meets the standard**

There is evidence that the organisation regularly and soundly evaluates its policies and procedures for the safe and secure management of medicines and controlled drugs to ensure they are effective.

The organisation has assurance on the security arrangements for all its medicines and controlled drugs.

Where appropriate, the results of evaluation lead to improvements in the organisation’s policies and procedures for the safe and secure management of medicines and controlled drugs.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect guidance ‘Security standards and guidance for the management and control of controlled drugs in the ambulance sector’
- NHS Protect guidance ‘Guidance on the security and storage of medical gas cylinders’
- NHS Protect checklist ‘Security of medical gas cylinders – General Checklist’
- NHS Protect checklist ‘Security of medical gas cylinders – Physical security and storage checklist’
- NHS Protect toolkit ‘Medicine security self-assessment tool’
- NHS Protect toolkit ‘Medicine security – Pharmacy checklist’
- NHS Protect toolkit ‘Medicine security – Ward/ department checklist’
- NHS Protect toolkit ‘Medicine security – Action plan template’
- NHS Protect guidance ‘Security of prescription forms guidance’
- NHS Protect guidance ‘Aide Memoire – Area Teams’
- NHS Protect guidance ‘Aide Memoire – Prescribers’
- NHS Protect guidance ‘Aide Memoire – Practice managers’
- The organisation’s policies and procedures for the management of medicines and controlled drugs
- Records of the Controlled Drugs Accountable Officer, as required in the Controlled Drugs (Supervision of Management and Use) Regulations 2013
- Job description of the Controlled Drugs Accountable Officer
- Meeting minutes, action points and records of their execution
- Examples of reviews of policies and procedures on the safe and secure management of medicines and controlled drugs
- Examples of evaluation results leading to improvements in the policies and procedures on the safe and secure management of medicines and controlled drugs
- Examples of assurance that the organisation complies with relevant legislation and guidance

Links


The Misuse of Drugs and Misuse of Drugs (Safe Custody) (Amendment) Regulations 2007

The Misuse of Drugs Regulations 2001 (SI 2001 No 3998)

Misuse of Drugs Act 1971

National Prescribing Centre, Handbook for controlled drugs Accountable Officers in England (March 2011)

Royal Pharmaceutical Society, Professional Standards for Hospital Pharmacy


Safer Management of Controlled Drugs – A guide to good practice in secondary care (2007)
http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/documents/digitalasset/dh_079591.pdf (this document has been archived but you may still find it useful to refer to it)

Safer Management of Controlled Drugs (Guidance on Standard Operating Procedures for Controlled Drugs)
http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_064828.pdf (this document has been archived but you may still find it useful to refer to it)

The Controlled Drugs (Supervision of management and Use) Regulations 2006

Care Quality Commission, ‘Guidance for providers on meeting the regulations’, Regulation 12
http://www.cqc.org.uk/sites/default/files/20150210_guidance_for_providers_on_meeting_the_regulations_final_01.pdf
# Prevent and Deter

## Standard 3.9

The organisation has policies and procedures in place to ensure prescription forms are protected against theft and misuse. These policies and procedures are reviewed, evaluated and updated as required.

## Rationale

NHS Protect has issued guidance on the security of prescription forms. Good governance and security arrangements should be in place for the security, distribution and storage of these items. In addition, local policies and procedures should specify the actions that staff should take when these items are lost or stolen, including reporting in line with NHS Protect guidance.

## Ratings

**Organisation does not meet the standard**

There is little or no evidence the organisation has policies and procedures in place to ensure prescription forms are protected against theft and misuse.

Policies and procedures may be in place but these are not systematically applied across the organisation.

Prescription forms are not protected against theft and misuse.

**Organisation partially meets the standard**

The organisation has policies and procedures in place to ensure prescription forms are protected against theft and misuse.

These are applied systematically across the organisation and are effective in protecting prescription forms against theft and misuse.

The policies and procedures are not regularly reviewed and evaluated.

**Organisation meets the standard**

The organisation has policies and procedures in place to ensure prescription forms are protected against theft and misuse.

These are applied systematically across the organisation and are effective in protecting prescription forms against theft and misuse.

The policies and procedures are regularly reviewed and evaluated. Where necessary, findings lead to improvements being made.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect guidance ‘Security of prescription forms guidance’
- NHS Protect guidance ‘Aide Memoire – Area Teams’
- NHS Protect guidance ‘Aide Memoire – Prescribers’
- NHS Protect guidance ‘Aide Memoire – Practice managers’
- NHS Protect toolkit ‘Medicine security self-assessment tool’
- NHS Protect toolkit ‘Medicine security – Action plan template’
- The organisation’s policies and procedures for the management and distribution of prescription forms
- Examples of reviews of policies and procedures on the secure management and distribution of prescription forms
- Examples of evaluation results leading to improvements in the secure management and distribution of prescription forms
- Examples of assurance that the organisation complies with relevant legislation and guidance

Links

Care Quality Commission, ‘Nigel’s surgery 23: Security of blank computer prescription forms’
http://www.cqc.org.uk/content/nigels-surgery-23-security-blank-computer-prescription-forms
Prevent and Deter
Standard 3.10
Staff and patients have access to safe and secure facilities for the storage of their personal property.

Rationale
While staff and patients should take care to make sure their property is safe and secure, organisations should provide them with secure facilities to store their personal belongings.

Where patients’ property has been handed in for safekeeping, the storage facilities should be suitable for their purpose, suitably located and secure. The management of patients’ property should be supported by specific policies and procedures that address all phases of the patient’s stay. NHS Protect has issued guidance on protecting patients’ property.

Ratings

Organisation does not meet the standard
There is little or no evidence of arrangements for the security of staff and patients’ property.

The organisation has not implemented NHS Protect’s guidance for NHS organisations on the secure management of patients’ property.

There may be evidence of some arrangements in place to provide staff and patients with safe and secure facilities for the storage of their personal property. However, these arrangements are not comprehensive or systematically applied across the organisation and do not follow the relevant NHS Protect guidance.

Organisation partially meets the standard
There is evidence that the organisation has systematically implemented comprehensive arrangements for the security of staff and patients’ property.

NHS Protect’s guidance for NHS organisations on the secure management of patients’ property has been fully implemented by the organisation.

There is little or no evidence that the organisation has soundly reviewed, audited or evaluated the effectiveness of its arrangements for the security of staff and patients’ property.

Organisation meets the standard
There is evidence that the organisation regularly and soundly evaluates and audits its arrangements for the security of staff and patients’ property to ensure they are effective.

Where appropriate, the results from the evaluation and audits lead to improvements in the organisation’s arrangements for the security of staff and patients’ property.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect document ‘Guidance for NHS organisations on the secure management of patients’ property’, including the Managing patients’ property flowchart
- Policy on staff and patients’ property
- Procedures for the security of staff and patients’ property
- Evidence that the organisation has developed its own policy for the secure management of patient property using the policy template provided by NHS Protect
- Examples of communications to staff and patients on the secure storage facilities that are available for their property
- Arrangements for the secure storage of staff and patients’ property which are proportionate to the need, rely on appropriately maintained facilities and are governed by policies that are regularly reviewed.
- Meeting minutes, action points and records of their execution
- Evidence of a reduction in losses relating to staff and patients’ property
- Examples of reviews and/or audits of secure storage for staff and patients’ property carried out to establish its effectiveness
- Examples of the results of the evaluation/or audits leading to improvements in the secure storage of staff and patients’ property

Links

Care Quality Commission, ‘Guidance for providers on meeting the regulations’, Regulations 13 and 15
http://www.cqc.org.uk/sites/default/files/20150210_guidance_for_providers_on_meeting_the_regulations_final_01.pdf
Prevent and Deter
Standard 3.11
The organisation records all security related incidents affecting staff, properties and assets in a comprehensive and systematic manner. Records made inform security management priorities and the development of security policies.

Rationale
Organisations need to learn from incidents in order to make improvements in security. They should therefore have a comprehensive and systematic process for learning lessons from individual incidents or investigations. This should include not just recording the incident itself, but also identifying its underlying causes and the changes to policies and procedures the organisation can introduce in order to reduce the risk of recurrence. This information can also be used to help the organisation identify any particular crime patterns or trends.

Ratings

Organisation does not meet the standard
There is little or no evidence that the organisation maintains a detailed record of security related incidents affecting staff, properties and assets.

The organisation maintains some records of security related incidents affecting staff, properties and assets, but they are not comprehensive, systematically made or updated in a timely manner.

There is no evidence that the organisation has sought to use the records to inform security management priorities and develop security policies.

Organisation partially meets the standard
There is evidence that the organisation records security related incidents staff, properties and assets in a comprehensive and systematic manner.

There is little or no evidence that the organisation regularly and soundly reviews or evaluates its systems for recording security related incidents affecting its staff, properties and assets.

Organisation meets the standard
The organisation can demonstrate that data from its security related incidents affecting staff, properties and assets informs security management priorities.

The organisation is able to demonstrate a link between reporting and improvements in the level of security related incidents affecting staff, properties and assets.

There is evidence that the organisation regularly and soundly evaluates the effectiveness of its reporting system on security related incidents affecting staff, properties and assets. Where appropriate, the findings contribute to improvements in the management of security within the organisation.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- Reports arising from the organisation’s security incident reporting system
- Crime pattern analysis
- Risk management reports
- Internal processes, policies and procedures for the organisation’s security incident reporting system
- A manual for, or written processes relating to, the reporting system
- Learning aims and outcomes of training on the reporting system
- Training records
- Evidence of changes to policies or procedures that can be linked to incident reporting
- Meeting minutes, action points and records of their execution
- Additions to risk matrices
- Risk management group minutes
- Examples of reviews and audits of the organisation’s security incident reporting system affecting staff, properties and assets to establish its efficiency and effectiveness
- Examples of, where appropriate, the results of the evaluation or audits resulting in improvements to the organisation’s security incident reporting system affecting staff, property and assets
- Supporting evaluation or audit reports
- SIRS input in relation to theft/damage of the organisation’s properties or assets

Links

Care Quality Commission, ‘Guidance for providers on meeting the regulations’, Regulation 17
http://www.cqc.org.uk/sites/default/files/20150210_guidance_for_providers_on_meeting_the_regulations_final_01.pdf
Prevent and Deter

Standard 3.12

The organisation takes a risk-based approach to identifying and protecting its critical assets and infrastructure. This is included in the organisation’s policies and procedures.

Rationale

Certain parts of the organisation’s operations constitute its critical assets and infrastructure: if they are lost or compromised, this could lead to catastrophic consequences for services and business continuity.

It is therefore essential to understand key threats faced by the organisation’s critical assets and infrastructure and take appropriate mitigating action to reduce them. This must be included in the organisation’s policies and procedures, so that the relevant staff know exactly which are the organisation’s critical assets and how to protect them.

Ratings

Organisation does not meet the standard

There is little or no evidence that the organisation applies a risk-based approach to identifying and protecting its critical assets and infrastructure.

There is little or no evidence that the protection of critical assets and infrastructure is included in the organisation’s policies and procedures.

Organisation partially meets the standard

There is evidence that the organisation, as part of its business continuity work, has identified its critical assets and infrastructure, has risk assessed them and put in place the appropriate control measures.

There is little or no evidence that the organisation has reviewed or evaluated its work to identify and protect its critical assets and infrastructure, or that the risk-based approach is influencing relevant organisational policies.

Organisation meets the standard

There is evidence that, using its risk-based approach to identifying and protecting its critical assets and infrastructure, the organisation makes improvements to relevant policies.

The organisation can demonstrate that it regularly evaluates its approach to identifying and protecting its critical assets and infrastructure and that, where appropriate, evaluation results lead to improvements.

The organisation tests its business continuity response through rehearsals and table top exercises in critical areas, and the outcomes lead to changes in training, policy and processes where necessary.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Commissioning Board Business Continuity Management Framework
- Evidence of risk assessments carried out of critical assets, buildings and other infrastructure
- Business continuity plan
- Business continuity training
- Training learning aims and outcomes
- Records of rehearsal and desk top exercises
- Risk management reports
- Risk management group minutes
- Additions to risk matrices
- Action cards
- Plans
- Reviews
- Debriefs
- Audit and monitoring criteria
- Meeting minutes, action points and records of their execution
- Evidence of changes to policies or procedures that can be linked to the risk-based approach to protecting the organisation’s critical assets and infrastructure
- Examples of reviews and/or audits of the organisation’s protection of its critical assets carried out to establish its efficiency and effectiveness
- Examples of the results of the evaluation/or audits leading to improvements in the organisation’s policies relating to the protection of its critical assets and infrastructure
- Evidence of work conducted as part of the Prevent element of the government’s counter-terrorism strategy
Prevent and Deter

Standard 3.13

In the event of increased security threats, the organisation is able to increase its security resources and responses.

Rationale

The security threats an organisation faces, and their severity, change over time. In some cases a new or emerging threat is suddenly identified, in others an existing threat can escalate. Security threats can also diminish.

Organisations must be able to adapt rapidly to such changes, particularly in the event of an increased security threat. Organisations must have arrangements to ensure the appropriate level of security response to an increased security threat.

Ratings

**Organisation does not meet the standard**

The organisation is unable to demonstrate that, in the event of increased security threats, it is able to increase its security resources and responses in a timely manner using a risk-based approach.

The organisation may be able to increase its security resources and responses but this cannot be shown to be appropriate for the level of risk.

**Organisation partially meets the standard**

The organisation can demonstrate that it has taken a risk-based approach to security threats and is able to increase and deploy its resources in a timely manner in response to those threats.

There is little or no evidence that the organisation regularly and soundly evaluates its ability to deploy appropriate resources in a timely manner in the event of increased security threats.

**Organisation meets the standard**

The organisation is able to demonstrate that arrangements for increasing its security resources and responses following an increase in security threats receive an appropriate level of executive and management support and are included in the organisation’s risk processes.

The impact of the risk-based approach to responding to increased security threats is regularly and soundly evaluated and relevant policies and processes are updated as required.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- Risk assessments of critical assets and infrastructure
- Business continuity plan
- Business continuity training
- Major incident action plan with security roles and responsibilities
- Risk management reports
- Risk management group minutes
- Additions to risk matrices
- Action cards
- Emails
- Plans
- Reviews
- Debriefs
- Audit and monitoring criteria
- Internal processes, policies and procedures on increasing the organisation’s security resources and responses as a result of increased security threats
- Meeting minutes, action points and records of their execution
- Evidence of the ability to increase resources as the security threat increases
- Evidence of policies or procedures being updated as a result of reviewing the organisation’s response to increased security threats
Prevent and Deter

Standard 3.14

The organisation has suitable lockdown arrangements for each of its sites, or for specific buildings or areas.

Rationale

Lockdown is the process of controlling access and the movement of people (staff, patients and visitors) around a site or specific building or area in response to an identified threat or hazard.

The aim of lockdown is to ensure that the organisation can continue to deliver as much of its service as possible during such events. This is achieved by controlling access and by diverting staff, patients and members of the public to alternative sites. There are different types of events that may require a lockdown, but having suitable arrangements in place is critical to any organisation’s business continuity planning and to protecting staff, patients, members of the public and property.

Ratings

Organisation does not meet the standard

There is little or no evidence that the organisation has suitable lockdown arrangements in place.

The organisation may have some lockdown arrangements in place, for example covering only some of the appropriate sites but not all.

Organisation partially meets the standard

The organisation is able to demonstrate that it has lockdown arrangements in place for each of its sites or for specific buildings or areas.

There is little or no evidence that the organisation regularly and soundly evaluates the effectiveness of its lockdown arrangements.

Organisation meets the standard

The organisation is able to demonstrate that its lockdown arrangements are regularly and soundly evaluated and any findings lead to improved arrangements.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect guidance on lockdown – Project Artemis
- Organisational policies and procedures relevant to lockdown
- Risk assessments
- Training learning aims and outcomes
- Training records
- Records of rehearsals and their evaluation
- Risk management reports
- Risk management group minutes
- Additions to risk matrices
- Action cards
- Templates
- Emails and other staff communications
- Plans
- Reviews
- Debriefs
- Meeting minutes, action points and records of their execution
- Evidence that procedures are regularly tested and reviewed, such as post event reports
- Evidence that findings lead to improvements in procedures

Links

Core Standards For Emergency Preparedness, Resilience and Response (EPRR)
Prevent and Deter
Standard 3.15
Where applicable, the organisation has clear policies and procedures to prevent and respond to a child or infant abduction. These are regularly tested, monitored and reviewed.

Rationale
This standard applies to organisations delivering maternity, neonatal, paediatric and specialist perinatal mental health services (in-patient mother and baby units).

Fortunately it is rare for a child or infant to be abducted from a provider’s properties. However, because of the trauma and inevitable publicity surrounding an abduction, organisations should (where applicable) have comprehensive measures in place to prevent and respond to such an incident.

Security measures in this area should be robust, practical, proportionate to the level of risk and easy for all staff, patients and visitors to understand and comply with. They should be supported by policies and procedures that are tested, monitored and reviewed at regular intervals to ensure they remain robust. If weaknesses in the measures are found, it is important that they are addressed as soon as possible.

Ratings

Organisation does not meet the standard
There is no evidence that the organisation has clear policies and procedures to prevent and respond to a child or infant abduction.

There may be some policies and procedures in place in this area, but they are insufficient and do not follow NHS Protect guidance.

Organisation partially meets the standard
The organisation is able to demonstrate that it has developed and implemented clear policies and procedures to prevent and respond to a child or infant abduction.

The organisation’s policies and procedures are in line with NHS Protect guidance.

There is little or no evidence of regular and sound evaluation of the effectiveness of the organisation’s policies and procedures for preventing and responding to a child or infant abduction.

Organisation meets the standard
The organisation regularly tests, monitors, evaluates and reviews its policies and procedures for preventing and responding to a child or infant abduction. Where necessary, findings lead to improvements being made.

The organisation is able to demonstrate that its policies and procedures in relation to child and infant abduction have resulted in a decrease in the number of incidents, where applicable.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- The NHS Security Management Manual, in particular the chapter on security in maternity, neonatal and paediatric services
- The organisation’s child and infant abduction policy
- Evidence that is the organisation’s child and infant abduction policy is tested, monitored and reviewed
- Meeting minutes, action points and records of their execution
- Risk assessments
- Training learning aims and outcomes
- Training records
- Records of rehearsals and their evaluation
- Risk management reports
- Risk management group minutes
- Additions to risk matrices
- Specific measures in maternity, neonatal, paediatric and specialist perinatal mental health services (in-patient mother and baby units) in response to risk assessment, such as specific access control measures or baby tagging
- Changes to the security system and related documentation
- Communications to staff
- Layout and design changes to buildings and copies of related building plans
- Evidence of police engagement in line with the organisation’s policies and procedures (including on related roles and responsibilities)
- Evidence of a decrease in incidents as a result of implementation of the policies and procedures
- Increase in the perception of safety – measured by surveys
- Evidence that the policies and procedures are regularly tested and reviewed
- Evidence that findings lead to improvements in the policies and procedures
Key Principle 3: Hold to Account

A **red** rating means non-compliance with the standard.

An **amber** rating means partial compliance with the standard. While the organisation has done work to meet the standard, this work has not been evaluated or it has not had a demonstrable impact.

A **green** rating means full compliance with the standard. The organisation has not only done work to meet the standard, but it has also evaluated the outcome of this work or can demonstrate its impact.

**Hold to Account**

**Standard 4.1**

The organisation has arrangements in place to ensure that security related incidents are investigated in a timely and proportionate manner and these arrangements are monitored, reviewed and evaluated.

**Rationale**

All investigations into security related incidents should be carried out in a timely and proportionate manner, so that evidence is preserved and any witnesses can recall facts more accurately. The investigation process should be documented, and arrangements for investigations should be monitored, reviewed and evaluated: this helps ensure that investigations are carried out to the highest possible standard, and that the organisation learns from its investigations.

**Ratings**

**Organisation does not meet the standard**

There is little or no evidence the organisation has arrangements in place to ensure that security related incidents are investigated in a timely and proportionate manner.

Investigations may be carried out, but they are not conducted in line with relevant legislation and NHS Protect guidance.

**Organisation partially meets the standard**

The organisation systematically and effectively carries out investigations into security related incidents in a timely and proportionate manner. These are conducted in line with relevant legislation and NHS Protect guidance.

Investigations are carried out appropriately, either internally or involving the police.

Investigation findings are not used to improve policies and procedures, where necessary, to prevent security related incidents from reoccurring.

There is little or no evidence the organisation monitors, reviews and evaluates the effectiveness of its arrangements to investigate security related incidents.

**Organisation meets the standard**

The organisation systematically and effectively carries out investigations into security related incidents in a timely and proportionate manner. Where these are carried out internally, they are conducted in line with
Standards for providers 2017-18: Security management

Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect strategy document ‘Tackling crime against the NHS: a strategic approach’
- NHS Protect guidance on Investigating security incidents and breaches
- Relevant supporting legislation
- NHS Protect/accreditation board records
- NHS Protect CPD training records
- Organisational policies, e.g. allocation of cases
- Other relevant policies and procedures
- Evidence of joint working arrangements with local police, including (where applicable) an incident response plan
- Records of police liaison and action taken as a result
- Records of all cases and case closures
- Policy changes resulting from investigative work
- Summary reports to committees
- Case conferences
- Meeting minutes, action points and records of their execution
- Incident investigation reports
- Records of related police work
- Evidence that investigative arrangements are regularly evaluated
- Evidence that findings from evaluations lead to improvements in investigative arrangements
**Hold to Account**

**Standard 4.2**

The organisation is committed to applying all appropriate sanctions against those responsible for security related incidents.

**Rationale**

When investigating security related incidents, it is important that the organisation considers the full range of possible sanctions. At the end of the investigation, where wrongdoing is identified, the organisation should seek to apply the most appropriate sanctions against the individual(s) involved. However, due to medical or clinical factors it may not be appropriate to apply sanctions in certain cases. This should be considered on a case by case basis.

A failure to apply sanctions may negatively affect the organisation’s reputation and its ability to deter others from committing similar offences.

**Ratings**

**Organisation does not meet the standard**

There is little or no evidence the organisation is committed to applying all appropriate sanctions against those responsible for security related incidents.

A commitment to applying all appropriate sanctions may be apparent in some cases, but this is not systematically applied to each security related incident.

**Organisation partially meets the standard**

The organisation is committed to applying all appropriate sanctions against those responsible for security related incidents. Policies and procedures are in place which support this commitment.

The organisation seeks to apply the full range of sanctions available and, where appropriate, works with NHS Protect’s Legal Protection Unit to ensure sanctions are applied.

Where a decision is taken not to apply a sanction, the advice received about this, and the reasons for the decision, are documented.

The organisation does not regularly review and evaluate the effectiveness of its arrangements for applying all appropriate sanctions against those responsible for security related incidents.

**Organisation meets the standard**

The organisation is committed to applying all appropriate sanctions against those responsible for security related incidents. Policies and procedures are in place which support this commitment.

The organisation seeks to apply the full range of sanctions available. Where a decision is taken not to apply a sanction, the advice received about this, and the reasons for the decision, are documented.

The organisation regularly reviews and evaluates the effectiveness of its arrangements for applying all appropriate sanctions against those responsible for security related incidents. Where necessary, findings lead to improvements being made.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS England’s Serious Incident Framework
- Health & Safety at Work Act 1974
- Care Quality Commission Regulations 2014
- NHS Litigation Authority
- NHS England – Patient Safety (for the purposes of child abduction as an SIs)
- NHS Protect strategy document ‘Tackling crime against the NHS: a strategic approach’
- NHS Protect guidance ‘Applying appropriate sanctions consistently’ (April 2013)
- NHS Protect guidance on clinically-related challenging behaviour
- The organisation’s security policy, including any measures on applying sanctions
- Other relevant policies and procedures
- Minutes from board or senior management meetings where sanctions are discussed
- Correspondence with NHS Protect’s Legal Protection Unit
- Evidence of joint working arrangements with local police, including (where applicable) an incident response plan
- Successful prosecutions in relation to security incidents at the organisation
- Publicity on successful prosecutions
- Meeting minutes, action points and records of their execution
- Communications to staff
- Police engagement over investigations and sanctions
- Evidence that the sanctions arrangements are regularly evaluated
- Evidence that findings from evaluations are lead to improvements in the arrangements
- Injunctions to prevent nuisance or annoyance
- Police cautions
- Non-criminal sanctions, including internal disciplinary sanctions, civil redress, fines, voluntary recoveries, acceptable behaviour agreements, withholding of treatment sanctions, written warnings and ASBO
Hold to Account
Standard 4.3
The organisation has a communications strategy which allows for appropriate publicity of sanctions following security related incidents.

Rationale
An organisational communications strategy which allows for publicising sanctions successfully applied following security incidents demonstrates the organisation’s commitment to tackling crime and taking appropriate action to bring perpetrators to justice. It can also act as a suitable deterrent to others who may be considering committing similar crimes. However, in some instances, due to medical or clinical factors it may not always be appropriate to pursue a sanction or publicise it. This must be reviewed on a case by case basis. Publicity of all sanctions, criminal or otherwise, should be considered.

Ratings

Organisation does not meet the standard
The organisation does not have a communications strategy which allows for the publicity of sanctions successfully applied following security related incidents to be considered on a case by case basis.

There is little or no evidence that the organisation publicises sanctions successfully applied following security related incidents.

The organisation may publicise some sanctions, but this is not done in a comprehensive and systematic manner.

Organisation partially meets the standard
The organisation has a communications strategy which allows for the publicity of sanctions successfully applied following security related incidents to be considered on a case by case basis.

The organisation publicises sanctions successfully applied following security related incidents. This is done in a comprehensive and systematic manner.

Where publicity is sought through the media, the organisation’s media policy is adhered to. Due regard is given to media handling guidance from NHS Protect. Where a decision is taken not to publicise a sanction, for example due to extenuating clinical factors, the rationale behind this decision is recorded.

There is little or no evidence that the organisation regularly reviews and evaluates its arrangements for publicising sanctions successfully applied following security related incidents.

There is little or no evidence the organisation has evaluated the impact of publicising sanctions as a deterrent.

Organisation meets the standard
The organisation has a communications strategy which allows for the publicity of sanctions successfully applied following security related incidents to be considered on a case by case basis.

The organisation publicises sanctions successfully applied following security related incidents. This is done in a comprehensive and systematic manner.

(continues on next page)
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect strategy document ‘Tackling crime against the NHS: a strategic approach’
- NHS Protect guidance on applying sanctions following security incidents
- NHS Protect guidance on clinically-related challenging behaviour
- NHS Protect guidance on developing a pro-security culture
- The organisation’s security policy, including any measures on publicising successful sanctions and redress
- Relevant organisational policies and procedures
- Communications strategy in relation to security management
- Relevant meeting minutes, action points and records of their execution
- Examples of publicising successful sanctions
- Corporate communications and media policy
- Staff surveys
- Increase in reporting after publicity in a certain area
- Reductions in particular crimes after publicity in a certain area
- Evidence that findings from evaluations lead to improvements in publicity arrangements
Hold to Account

Standard 4.4

The organisation has a clear policy on the recovery of financial losses incurred due to security related incidents and can demonstrate its effectiveness.

Rationale

The organisation should take all necessary steps to recover financial losses due to security related incidents. As custodians of public resources, NHS organisations should ensure that any money lost in this way is recovered and reinvested to deliver the best outcomes for patients.

Organisations should have a policy for the recovery of financial losses due to security related incidents, and should be able to demonstrate its effectiveness.

Ratings

Organisation does not meet the standard

There is no evidence that the organisation seeks to recover financial losses due to security related incidents.

There may be some work to recover financial losses, but it is not carried out in a comprehensive, systematic or timely manner and there is not a clear policy in place in this area.

Organisation partially meets the standard

The organisation has a clear policy for the comprehensive, systematic and timely recovery of financial losses incurred due to security related incidents.

There is little or no evidence that the organisation regularly and soundly evaluates the effectiveness of this policy.

Organisation meets the standard

The organisation can demonstrate that it has a policy which enables it to consider recovery of financial losses due to security related incidents on a case by case basis.

The impact of the recovery of financial losses due to security related incidents is regularly monitored and soundly evaluated and, where appropriate, improvements are made to the organisation’s policy on recovery.
Guidance, supporting documentation and evidence

Organisations should consider the following (the list is not exhaustive):

- NHS Protect strategy document ‘Tackling crime against the NHS: a strategic approach’
- NHS Protect guidance on redress
- Data on sanctions and how they relate to recovery of financial losses
- Monitoring data
- Records of decisions on whether to undertake recovery of financial losses and reasons given for/against recovery
- Committee reports
- The organisation’s policy for the recovery of financial losses due to security related incidents
- Other relevant policies and procedures
- Minutes from board or senior management meetings where recovery of financial losses was discussed
- Correspondence with NHS Protect’s Legal Protection Unit
- Evidence of successful recovery of financial losses by the organisation
- Publicity around successful recovery of financial losses
- Meeting minutes, action points and records of their execution
- Communications to staff
- Evaluation of the impact of successful recovery of financial losses
- Evidence of an increase in reporting after publicity around successful recovery of financial losses
- Reductions in relevant crimes after publicity
- Evidence that the arrangements for recovery of financial losses are regularly evaluated
- Evidence that findings from evaluations lead to improvements in the arrangements
## Appendix 1

### Quality assurance programme - Reasonable expectations of the parties

<table>
<thead>
<tr>
<th>Your reasonable expectations of us and how we will work with you.</th>
<th>Our reasonable expectations of organisations and how they will work with us.</th>
</tr>
</thead>
<tbody>
<tr>
<td>All parties will engage in a professional and polite manner at all times.</td>
<td></td>
</tr>
<tr>
<td>We will be consistent, fair and transparent, taking a constructive and supportive approach.</td>
<td>The Self Review Tool will be completed and signed off by the relevant organisational representative and sent to NHS Protect within the required deadline.</td>
</tr>
<tr>
<td>We will give organisations a minimum of four weeks’ notice of an assessment site visit, our evidence requirements and necessary arrangements in relation to relevant staff interviews and site visit requirements.</td>
<td>The site visit is comprehensively organised and communicated to the Quality and Compliance team in line with our evidence requirements and all other necessary arrangements by the due date provided in line with the requirements of standard 1.2. All advance evidence requested must be supplied to the SQCI by the due date. Failure to comply with deadlines may mean that the organisation is in breach of standard 1.2.</td>
</tr>
<tr>
<td>Organisations will be assigned a named representative, usually a Senior Quality and Compliance Inspector, and provided with their full contact details, to provide support in relation to the quality assurance programme.</td>
<td>A timely notification of a named organisation representative with full contact details to assist in assessment site visit arrangements should be submitted promptly.</td>
</tr>
<tr>
<td>We will provide comprehensive and timely feedback on all questions raised.</td>
<td>Any questions are fully raised at the earliest opportunity.</td>
</tr>
<tr>
<td>The assessment will be completed and initial feedback provided at the closing meeting.</td>
<td>Access to the organisation’s staff as requested, including senior managers, in order to facilitate the assessment process.</td>
</tr>
<tr>
<td>We shall provide organisations with a copy of the final report no later than four weeks after the completion of the assessment visit.</td>
<td>The organisation’s response to the final report recommendations will be sent to the assigned Quality and Compliance representative within four weeks of receipt of the final report.</td>
</tr>
<tr>
<td></td>
<td>The organisation will comply with NHS Protect’s documented review process, responding to any queries and submitting requested documentation on time in line with standard 1.2.</td>
</tr>
</tbody>
</table>
The security management quality assurance programme

1. LIAISON
2. YEARLY ASSURANCE
   - WORKPLAN
   - SELF REVIEW TOOL SENT TO NHS PROTECT
3. DOCUMENTS EVALUATED FOR INTELLIGENCE AND RISK
4. ASSESSMENT REQUIRED OR DUE?
   - YES
     - SENIOR QUALITY AND COMPLIANCE INSPECTORS REQUEST AND REVIEW REQUIRED EVIDENCE ON ASSESSMENT TYPE (THEMATIC, FULL OR FOCUSED)
     - ARRANGE DATE WITH ORGANISATION FOR SITE VISIT (PERSONAL CONTACT)
     - SITE VISIT / ASSESSMENT (PERSONAL CONTACT)
     - DISCUSS FINDINGS WITH ORGANISATION
     - PRODUCE REPORT
     - ISSUE REPORT (ORGANISATION, NHS PROTECT, AREA SECURITY MANAGEMENT SPECIALIST)
     - LIAISON
5. NO
   - NO FURTHER ACTION
6. NHS PROTECT AND NATIONAL PRIORITIES
7. LOCAL RISK AND/OR NEEDS
8. NHS PROTECT AND REGULATORY INFORMATION
9. LINK TO STANDARDS
10. NATIONAL REPORT
11. BENCHMARKING

The security management quality assurance programme

Standards for providers 2017-18: Security management
Summary of changes for 2017-18

<table>
<thead>
<tr>
<th>Standard</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Rationale amended.</td>
</tr>
<tr>
<td>1.2</td>
<td>No change.</td>
</tr>
<tr>
<td>1.3</td>
<td>No change.</td>
</tr>
<tr>
<td>1.4</td>
<td>Green rating amended.</td>
</tr>
</tbody>
</table>
| 1.5      | Renumbered 1.2.  
Headline standard, rationale and ratings, all amended. |
| 2.1      | Merged with 2.3 and renumbered. Headline standard, rationale and ratings, all amended. |
| 2.2      | Renumbered 2.1. |
| 2.3      | Merged with 2.1. |
| 2.4      | No change. |
| 2.5      | No change. |
| 2.6      | No change to standard. Pilot status changed to permanent. |
| 3.1      | No change. (check) |
| 3.2      | No change. |
| 3.3      | No change. |
| 3.4      | No change. |
| 3.5      | Changes to….? |
| 3.6      | No change. |
| 3.7      | Deleted. |
| 3.8      | Renumbered to 3.7. |

(continues on next page)
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9</td>
<td>Renumbered to 3.8.</td>
</tr>
<tr>
<td>3.10</td>
<td>No change.</td>
</tr>
<tr>
<td>3.11</td>
<td>Renumbered to 3.10.</td>
</tr>
<tr>
<td>3.12</td>
<td>Renumbered to 3.11.</td>
</tr>
<tr>
<td>3.13</td>
<td>Renumbered to 3.12.</td>
</tr>
<tr>
<td>3.14</td>
<td>Renumbered to 3.13.</td>
</tr>
<tr>
<td>3.15</td>
<td>Renumbered to 3.14.</td>
</tr>
<tr>
<td>3.16</td>
<td>Renumbered to 3.15.</td>
</tr>
<tr>
<td>4.1</td>
<td>No change.</td>
</tr>
<tr>
<td>4.2</td>
<td>No change.</td>
</tr>
<tr>
<td>4.3</td>
<td>Headline standard, rationale and ratings have been amended.</td>
</tr>
<tr>
<td>4.4</td>
<td>No change.</td>
</tr>
</tbody>
</table>