<table>
<thead>
<tr>
<th><strong>Title:</strong></th>
<th>Guidance on the High Security Psychiatric Services (Arrangements for Safety and Security) Directions 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author:</strong></td>
<td>Andrew Herd SCLGCP / MHD&amp;E / FMH&amp;OH / Cost centre: 11160</td>
</tr>
<tr>
<td><strong>Document Purpose:</strong></td>
<td>Guidance</td>
</tr>
<tr>
<td><strong>Publication date:</strong></td>
<td>December 2013</td>
</tr>
<tr>
<td><strong>Target audience:</strong></td>
<td>Providers of high security services (Rampton, Broadmoor and Ashworth).</td>
</tr>
</tbody>
</table>
| **Contact details:** | Andrew Herd  
High Secure Services  
Department of Health  
Quarry House  
Quarry Hill  
Leeds  
LS2 7UE  
Email: andrew.herd@dh.gsi.gov.uk |

You may re-use the text of this document (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit [www.nationalarchives.gov.uk/doc/open-government-licence/](http://www.nationalarchives.gov.uk/doc/open-government-licence/)

© Crown copyright

Published to gov.uk, in PDF format only.

[www.gov.uk/dh](http://www.gov.uk/dh)

Prepared by Andrew Herd
Summary

1. This guidance accompanies the High Security Psychiatric Services (Arrangements for Safety and Security) Directions 2013, which apply to providers of high security psychiatric services.

2. This document contains:
   i) general information (paragraphs (3) to (5)) about the High Security Psychiatric Services (Arrangements for Safety and Security) Directions 2013;
   ii) specific guidance about the implementation of certain of the requirements contained in the directions (paragraph (6));
   iii) general guidance on the manner in which policies (including procedures and protocols) should be produced, and promulgated to staff, within the high security hospitals (paragraphs (7) to (12));
   iv) annexes A & B: protocols for the identification and management of ‘high risk’ patients and locking patients in their rooms at night;
   v) attachment 1: the decision tree for risk management of ‘high risk’ patients; and
   vi) attachment 2: the management strategies supporting the decision making for the risk management of ‘high risk’ patients.

Status of directions and guidance

3. The Directions are issued by the Secretary of State for Health and providers of high security psychiatric services must comply with them. This guidance is not mandatory, but providers must have regard to it. Direction 3 sets out reporting requirements where a provider does not follow, or intends not to follow the guidance.

4. The High Security Psychiatric Services (Arrangements for Safety and Security) Directions 2013 should be read alongside the High Security Psychiatric Services (Arrangements for Visits by Children) Directions 2013 (due to reference in this guidance to visits by children) and providers of high security psychiatric services must comply with them.

Human rights and equality

5. When implementing the Directions and guidance, providers are responsible for doing so in a way which takes issues of human rights and equalities into consideration to ensure they comply with:
   i) The Human Rights Act 1998;
   ii) The Equality Act 2000; and
   iii) Health inequalities duties as set out in the Health and Social Care Act 2012.

6. They should take a similar approach to equality in terms of religion and belief, age and sexual orientation.
Specific guidance on certain Directions

7. This section of the guidance is specifically about the implementation of certain of the requirements contained in the Directions.

**Direction 2: Interpretation.**
In addition to the interpretations as specified within direction 2, this guidance defines the following:

i) “admission facility” – for the purposes of direction 6(14) an “admission facility” should include suitable facilities to carry out a search involving the removal of clothing other than outer clothing whilst maintaining the patient’s dignity and privacy;

ii) “responsible clinician” - this will include any person appointed by the provider to provide cover in the absence of the “responsible clinician” (e.g. during non-working hours, annual leave etc);

iii) "visitor" - any person aged 18 or over who proposes to enter the secure area of the hospital and is not a member of staff is included within this definition. It will, for example, thus include Care Quality Commissioners, Mental Health Review Tribunal personnel, the police, health professionals and solicitors; and

iv) “security director” – this includes the person nominated to undertake delegated responsibilities and duties by the security director that the security director would undertake.

**Direction 3: Promotion of safety and security**
In order to comply with the requirements in paragraph (3) of this direction to report non-compliance without delay, initial contact may be made by telephone. However, providers of high security psychiatric services must also report non-compliances in writing to NHS England and the NHS Trust Development Authority.

Providers will implement arrangements for the management of safety and security in accordance with the additional detailed advice available within the Clinical Security Framework. If a provider decides to implement arrangements other than in accordance with the content of the Clinical Security Framework they must notify NHS England.

The Directions and guidance, together with the Clinical Security Framework, cover minimum physical and operational standards of safety and security. They do not focus on the therapeutic aspects of the work of the hospitals. However, by supporting a safe environment for patients and staff, the arrangements should enhance the therapeutic activities of the hospitals.

It is not the purpose of the Directions and guidance or the Clinical Security Framework to cover every aspect/area of policies which providers should have in place. Each provider should determine what other areas need to be covered by policies. In addition, some of this will be governed by legislation, for example the Mental Health Act 1983; the Human Rights Act 1998; equality, health inequalities and employment legislation and legislation relating to drugs management and misuse.
**Direction 5: Requirements for conducting a rub-down search of a patient**

A rub-down search must be a search of a type at least equivalent to a Level B rub-down search as described in Function 3 (outcome 3.2) of the Clinical Security Framework.

The Directions state that rub-down searches must, unless there are exceptional circumstances, be carried out by members of staff who are of the same sex as the person being searched. If this is not possible, there should always be a member of staff of the same sex present when the search is carried out.

If a search without consent is authorised, or the search is being undertaken under paragraph 15 of this direction, a further attempt should be made to obtain the patient’s consent before proceeding with a search without consent.

Where searches of patients are conducted without consent, the minimum of force needed to complete the search should be used.

It is recommended that patients be made aware of the searching processes that affect them.

**Direction 6: Searches of patients that involve the removal of clothing other than outer clothing**

"Outer clothing" means a top coat and any other items of clothing (e.g. jacket, cardigan) that are bulky and inhibit a proper search being conducted.

Each provider should provide instructions to staff regarding the detailed arrangements for conducting a search of a patient that involves the removal of clothing. These instructions should include:

i) measures aimed at providing privacy and protecting the dignity of the patient;

ii) identification of the limited circumstances where a search of this type may be used; and

iii) the arrangements for authorising a search of this type.

If a search without consent is authorised, or the search is being undertaken under paragraph (19) of this direction, a further attempt should be made to obtain the patient’s consent before proceeding with a search without consent.

Where searches of patients are conducted without consent, the minimum of force needed to complete the search should be used.

It is recommended that patients be made aware of the searching processes that affect them.

**Direction 7: Searches of patients, rooms and lockers**

Unless circumstances dictate otherwise, a patient should be present when their room and locker are searched. This may be clinically beneficial for the patient and witnessing thorough searches may act as a deterrent in future.

Providers should consider whether room searches are most appropriately carried out by ward staff, dedicated search teams, or both.

In the interests of protecting staff from any allegations of inappropriate action, it is advisable for room searches to be undertaken by more than one member of staff.
If items belonging to a patient are removed, the patient should be given a receipt for the items and informed why the items have been removed and where they are being kept. A receipt is not required where items of rubbish, such as discarded packaging or items of food waste, are removed and if this is the case, the patient should be informed.

The requirement to carry out a rub-down search immediately before and after a visit in paragraph (6) of this direction includes carrying out a rub-down search if a patient leaves or re-enters the visit area during a visit.

The exemption in paragraph (10) of this direction is made on the understanding that the requirements for the patient’s management include continuous observation and minimal contact with other patients.

It is recommended that patients be made aware of the searching processes that affect them.

**Direction 8: Searches when patients move around in the secure area**

The exemption in paragraph (4) of this direction is made on the understanding that the requirements for the patient’s management include continuous observation and minimal contact with other patients.

It is recommended that patients be made aware of the searching processes that affect them.

**Direction 9: Searches of ward areas and other areas**

The requirement to search therapy, workshop, recreation and leisure facility areas, and other non-ward areas which a patient may visit in the secure area, has been set at no less than once every three months. Existing arrangements for the searching and supervision of patients, checking of tools before and after sessions and controls on patients’ access, should already minimise the risk of illicit items being hidden in those areas. However, these searches should not be limited to once every three months but should be searched whenever a credible risk is identified.

**Direction 10: Security of tools, equipment and materials**

Providers should abide by the contents of Function 1 (outcome 1.5) of the Clinical Security Framework when developing policies for members of staff regarding the control of tools, equipment and materials in secure areas of the hospital.

**Direction 11: Searches of members of staff**

What constitutes a rub-down search is contained (above) in the guidance to direction 5 “Requirements for conducting a rub-down search of a patient.”

A member of staff who refuses to be searched or to permit his/her possessions to be searched, must be denied entry to the secure area. A member of staff who refuses to be searched or to allow their possessions to be searched on the way out of the secure area cannot, however, be prevented from leaving. Providers must include within their policies arrangements for managing such refusals.

Only visitors who have had a Disclosure Barring Service (DBS) check and completed the appropriate training detailed in direction 44(3) can be key holders.
Direction 12: Arrangements in respect of visitors and visiting children
What constitutes a rub-down search is contained (above) in the guidance to direction 5 “Requirements for conducting a rub-down search of a patient.”

Bringing and sending food items in to the hospital presents risks in terms of checking for concealed illicit items. It also presents potential health hazards. The restrictions on bringing and sending food in to the hospital, other than in limited and carefully controlled circumstances, are intended to address these concerns. Providers should ensure a sufficiently varied range of food is available on site to cater for differing tastes among patient/visitor groups.

The security director should be informed of any decision to allow a visitor to bring food into the hospital under paragraph (5)(b) of this direction.

There is no legal power to routinely require a visitor to submit to a search but if a search is refused, the provider is entitled to refuse that person entry. Applying restrictions to visitors who refuse to submit to searches on their way out of the hospital is more problematic because visitors cannot be prevented from leaving the hospital. However, searches of visitors on entry and searches of the patient prior to the visit, if carried out thoroughly, should minimise the risk of inappropriate items being passed between the patient and the visitor. Nevertheless, if there is reason to believe that a visitor may be carrying an inappropriate item out of the hospital, and they refuse to submit to a search, consideration should be given to contacting the police about the matter, or informing the visitor that entry may be refused on a future occasion.

Care should be taken with regard to obtaining consent to search visiting children of any age. Where children have the capacity to understand the implications, and make an informed decision about being searched, it would be appropriate to seek their consent in addition to, or instead of, the adult who is accompanying them. However, a forced search of a visiting child who is competent to understand and make a decision on the matter, even if carried out with the accompanying adult’s consent, may constitute an assault.

Members of the First-Tier Tribunal (Mental Health) carrying out a judicial function who are exempt from rub-down searches under direction 12(10), should be invited to participate in rub-down searches in the interests of their own safety and that of the safety and security of the hospital. A record should be made on each occasion a tribunal member enters the secure area of the hospital and whether or not they participated in a rub-down search.

Direction 12(13) refers to senior members of the Royal family carrying the style His or Her Majesty (HM) or His or Her Royal Highness (HRH).

Direction 13: Searches of visitors and inspection of possessions
Under normal circumstances, it is expected that both male and female staff will be available to search visitors entering the secure area, and that it will therefore be possible for searching to be carried out by a person of the same sex as the visitor. However, there may be circumstances when searching by a member of staff of the opposite sex is considered to be appropriate, even when staff of the same sex are available. For example, female staff searching male babies. This should only be done at the request of the visitor or with appropriate consent.
It may not be possible to X-ray all property entering the secure area with contractors and it is accepted that they will often need to take into the secure area tools and other equipment which, whilst unacceptable for other visitors, will be needed by contractors to enable them to complete the tasks which they are employed to perform within the hospital. Providers should have suitable arrangements in place for:

i) checking contractors’ tools and other equipment both on arrival and departure from the secure area; and

ii) the supervision of contractors while they are working within the secure area.

Providers must abide by the contents of Function 1 (outcome 1.6) and Function 3 (outcome 3.2) of the Clinical Security Framework when developing their policies for the management of contractors and their property.

**Direction 14: Supply of food by staff to patients**
These restrictions are intended to prevent staff in direct contact with patients being involved in bringing food into the hospital for consumption by patients. The chief executive’s authority detailed in paragraph (2) of this direction may be given to groups of staff as well as individuals. It may be a standing authority, which would not have to be applied for on each occasion, that these staff bring food into the hospital for patients.

**Direction 15: Checks of vehicles**
Providers must abide by the contents of Function 1 (outcome 1.6) and Function 3 (outcome 3.4) of the Clinical Security Framework when developing policies for members of staff for managing and escorting vehicles within secure areas.

The Direction requires all vehicles to be checked before the vehicle enters or leaves the secure area. It will be impracticable to carry out a detailed search of every vehicle entering and leaving the secure perimeter. It is however, expected that vehicles will be carefully checked for unauthorised persons both on arrival and departure, and that a watch will be kept for illicit or potentially dangerous items which are not required by the occupants of the vehicles for the tasks which they will be performing within the secure area.

**Direction 16: Contractors’ vehicles in the secure areas**
Vehicles should not normally be left in the secure area of the hospital. The security director should only give permission having considered, and approved, both the location and any necessary supervisory arrangements for the vehicle. In making arrangements for the management of contractors’ vehicles in the secure area, providers must abide by the contents of Function 1 (outcome 1.6) of the Clinical Security Framework.

**Direction 17: Testing for illicit substances**
It is recommended that patients are made aware of the requirements within the Directions for providers to carry out these tests.

It is not envisaged that patients should be physically forced to provide a sample for testing. A refusal to co-operate with a request for a sample might raise concern but it is for the provider to consider what action to take in the event of a refusal, taking into account individual circumstances.
**Direction 20: Security information**

Providers must abide by the contents of Function 4 (outcome 4.2) of the Clinical Security Framework when developing policies for the maintenance and use of security information records.

Security records should be developed and maintained to contain:

i) security information relating to each patient; and

ii) other security information relating to the hospital.

Security records should form the basis of an electronic security intelligence system.

Security records and other sources of relevant information should be analysed/assessed for the purpose of developing security intelligence.

Security records and the intelligence developed from them should be used to inform risk assessment and operational practice.

Security intelligence systems should be set up with due regard to legal requirements for protecting patient confidentiality and the disclosure of information. It is recommended that clear protocols are drawn up which cover the need for security and clinical records to be kept as entirely separate entities.

The director of security in discharging their duties under direction 20(4)(d) should ensure they consider any request for disclosing security records and hold the authority for sharing security information.

**Direction 21: Patients’ possessions**

Providers must abide by the contents of Function 1 (outcome 1.11) of the Clinical Security Framework when developing policies for arrangements for managing patients’ property.

Providers should also abide by the following:

i) If a patient is denied access to an item of property under paragraph (3) of this direction they should be given a reason for that refusal if they request it and informed of the process for appealing that decision; and

ii) The possessions in patients' rooms and their personal lockers should be limited to a level and type which are compatible with the facilitation of searching within a defined period of time outlined in hospital policy, the maintenance of security and the reduction of fire hazards. Providers should also manage the risk presented by the potential to misuse technology, particularly that capable of displaying, recording, storing and distributing images and other data.
Arrangements for patient access to electrical and related items within their rooms should include the following arrangements:

i) CDs or items in other approved formats used for the recording of audio material, should be restricted to a maximum of 24 items. This can include a combination of formats but should not include any format capable of recording images.

ii) If permitted, DVDs, videos or items in other approved formats capable of recording images, should be restricted to a maximum of 5 items. These should all be the same format (e.g. a combination of videos and DVDs should not be permitted).

All access to electrical items in patients’ rooms should be thoroughly risk assessed.

If patients are allowed access to electrical items in their rooms, the quantity should be appropriately limited and exclude multiple items of the same type (e.g. they should only have a single television, CD player etc).

Each provider should have a strategy for managing patients’ access to televised and other similar material, which includes appropriate controls over access to unacceptable / clinically harmful material. The strategy should be compliant with the following guidelines:

i) Patients should not be able to access pay-to-view television unless this is controlled by the provider;

ii) Access to equipment capable of recording televised material should only be allowed if the provider has in place effective controls and systems for checking recorded content;

iii) Patients should not have access to equipment capable of making copies of previously recorded material;

iv) Care should be exercised when considering access to new/developing technologies which are designed for or could be used for recording/storing images; and

v) Patients should not be allowed to loan or exchange recorded material amongst themselves unless by prior agreement with a suitably qualified member of nursing/medical staff, who should ensure that any necessary amendments are made to the property inventories of the patients concerned.

Patients should not have access to computer equipment in their rooms, unless this is owned and controlled by the provider and abides by Section 5.2 (b) of the Clinical Security Framework (see paragraph (23) of the Directions and associated guidance).

Patients may have access to any other electrical items that the clinical team, acting on advice from the security department, has agreed the patient may have.

**Direction 22: Items delivered or brought to hospital premises for patients and Direction 26: Patients’ incoming post**

Items delivered or brought to hospital premises for patients include any items of patients’ property arriving at hospital on admission, carried by patients or otherwise and property carried by a patient on return from leave of absence.
Where DVDs, videos or items in other formats intended or capable of recording images are concerned, it is recommended that:

i) Any item delivered or brought into the hospital premises should, on arrival in the hospital, be checked by a member of staff to establish that it is what it is purported to be and then be passed to the clinical team for a decision as to whether or not it is suitable for the patient for whom it is intended. (Bearing in mind that apparently innocent content may be considered inappropriate for some patients); and

ii) No item should be passed to a patient if it is has a classification of 18R.

Providers should have arrangements in place for managing items delivered to the hospital for patients that they are not allowed, either because they breach the Directions or the provider’s policy.

Direction 23: Patients’ access to computer equipment and games consoles
In developing systems and policies for patients’ access to, and usage of, computer equipment and games consoles, providers should ensure that:

i) patients are not allowed access to live internet content, unless in exceptional circumstances such as for exams and this access should be directly supervised;

ii) individual patient’s access to computers is risk assessed, and the risk assessment should determine whether or not access is to be supervised directly, remotely or subject to electronic monitoring;

iii) patients’ access to computers is at least monitored electronically; and

iv) all computer systems must be auditable.

‘Directly supervised’ means the patient is subject to a member of staff sitting with them and directly supervising their access; ‘remote supervision’ means the supervising member of staff is undertaking this supervision via remote location (on another computer); ‘electronic monitoring’ is the active and retrospective monitoring of the computer or information technology by the patient using bespoke software services that can provide individual patient activity reports.

Where computer equipment is allowed in a patient’s room, the computer equipment must be owned and controlled by the provider. It should not only be electronically monitored but capable of remote supervision at the discretion of the provider.

Direction 25: Role of patients in managing or working in patients’ shops and other specified employment
When identifying any suitable employment opportunities for patients in the hospital, providers should consider the risks associated with these opportunities.

Where the level of risk is considered to be similar or higher than that presented by working in a patients’ shop, these work placements should be classified as ‘specified employment’ opportunities. It is for the provider to decide what work falls within the definition of ‘specified employment’.
Referrals to the grounds access committee should only be made where a patient’s clinical team has undertaken a risk assessment and proposes that working in a patients’ shop or in ‘specified employment’ should be included as part of the patient’s treatment plan.

**Direction 27: Internal Post**
Post between patients and members of their clinical team should not be opened routinely under this direction. Post between patients and staff should only be opened in response to security or other concerns.

**Direction 29: Incoming post addressed to members of staff**
Postal packets addressed to staff should not be opened and inspected for security reasons unless the addressee is present and has given their consent.

Staff should be informed that a postal packet addressed to them may be withheld and not allowed into the secure area if they refuse to allow it to be opened and inspected following an x-ray.

If a postal packet is withheld the member of staff must be informed of the following:

i) the reasons for withholding it;

ii) that they can request that the Chief Executive review the decision to withhold it; and

iii) that they can take the postal packet when they leave the secure area.

**Direction 31: Patients’ outgoing telephone calls**
Where a provider decides to include patient contact with the Samaritans within its policy on telephone use by patients, it should agree its policy proposals, and the detailed arrangements, with the Samaritans prior to making the service available to patients.

Contact with the Samaritans should be on an individual patient basis, be risk assessed and included within the patient’s treatment plan.

**Direction 32: Patients’ incoming telephone calls**
Pre-arranged incoming calls should only be authorised when the caller is not in a position to receive a call from the patient e.g. where the caller is a patient in another high security hospital or another establishment which restricts incoming calls.

**Direction 33: Risk assessments and Direction 35: Security at night**
Each provider should have a policy on the circumstances in which a patient can be locked in their room at night. This policy should include the requirement to consider locking the room of a patient, considered to be ‘high risk’ as set out in direction 33(4) and for this to be included in their risk management plan, following a risk assessment under direction 33. It should also include any arrangements for locking other patients in their rooms at night under direction 35.

There is a distinction between night-time confinement under these directions and seclusion. Locking the room of a patient at night under direction 35 is not the same as seclusion.
Paragraph 15.43 of the Mental Health Act 1983 Code of Practice (‘the Code of Practice’), defines seclusion as "the supervised confinement of a patient in a room, which may be locked. Its sole aim is to contain severely disturbed behaviour which is likely to cause harm to others." Seclusion is a therapeutic response to a patient’s immediate disturbed behaviour and should be used as a last resort and for the shortest possible time. Seclusion should not be used as a punishment or threat. It should not be used as part of a treatment programme, or because of a shortage of staff or where there is any risk of suicide or self-harm (paragraph 15.45 of the Code of Practice).

By contrast, night-time confinement under the Directions is the routine, pre-determined locking-in of patients as set out in direction 35, and not a reaction to a patient's immediate behaviour. Night-time confinement in accordance with the Directions should be pre-determined and only permitted under direction 35, if a full risk assessment has been carried out under direction 33 and a risk management plan prepared, which must include any decision (including a date on which that decision must be reviewed) to lock the room of a patient at night in accordance with direction 35.

Longer-term segregation as described in paragraph 15.63 of the Code of Practice is also not the same as night-time confinement under the directions. Longer-term segregation of a patient should follow guidance in paragraphs 15.63 to 15.66 of the Code of Practice.

Annex A provides an example of a protocol to meet the requirement for an individual risk assessment of each patient. The protocol incorporates arrangements for considering whether high risk patients should or could be locked in their rooms at night as part of their risk management plan made under the directions.

Annex B provides an example of a protocol which sets out the requirements for making decisions regarding the locking of other patients (under direction 35) in their rooms at night.

Direction 34: Monitoring telephone calls
The identification of telephone calls for recording under paragraph (7) of this direction should be based on a random selection.

Where a provider decides to retain a record under paragraph (8) (b) of this direction, it should record the reason for that decision.

Direction 36: Grounds Access
Further to the interpretation and definition of 'grounds access' within direction 2, this does not include unescorted patient access into ward garden areas if:
  i) the garden area is only accessible from the patient’s ward;
  ii) the garden area is bounded by a barrier (fence or wall) which effectively separates it from adjacent areas and which cannot easily be defeated; and
  iii) access is approved by the patient’s clinical team following individual documented risk assessment.

Direction 38: Functions of the Grounds Access Committee
When granting grounds access the grounds access committee must identify the area or areas of the hospital premises to which the grounds access applies.
It is recommended that the grounds access committee should, as part of its responsibilities, keep under review the question of the total number, and the mix, of patients who should be permitted grounds access at any one time.

**Direction 40: Leave of Absence**
When developing policies for the management of leave of absence, providers must ensure they are compliant with Ministry of Justice guidance to responsible clinicians and guidance within Function 1 (outcome 1.3) of the Clinical Security Framework. They should also consider the following:

i) Child protection issues should be a central consideration in leave of absence planning. Contact between patients and named children during leave of absence must be approved following the principles outlined in the High Security Psychiatric Services (Arrangements for Visits by Children) Directions 2013;

ii) When leave of absence is used for rehabilitation purposes, it should be written into a care plan and have clear objectives;

iii) Whilst the responsible clinician has statutory power to grant leave of absence (subject to Ministry of Justice consent where necessary), the chief executive has a responsibility to consider and advise on safety issues, which is reflected in the requirement of the security director to approve all leave of absence management plans. Leave of absence should not take place unless the management arrangements are approved; and

iv) Unescorted leave of absence is only likely to be appropriate in exceptional circumstances.

**Direction 41: Escorting patients**
When developing policies for members of staff on carrying out escorting duties, including the appropriate use of handcuffs and escorting chains, providers must abide by the contents of Function 1 (outcome 1.3) of the Clinical Security Framework.

**Direction 42: Security of keys and locks**
When developing policies for members of staff on the security of keys and locks, providers must abide by the contents of Function 7 (outcome 7.6) of the Clinical Security Framework.

**Direction 44: Provision of training**
Providers should be guided by advice from NHS Protect, when developing training on the non-physical management of violence and aggression for members of staff and other key holders.

**General guidance on policies**
8. Providers are required by Direction 4 to cooperate with other providers for the purpose of making arrangements in respect of safety and security. However, it is for each provider to develop its policies around the Directions, guidance and the content of the Clinical Security Framework. This includes deciding whether to apply more rigorous arrangements either across the hospital as a whole, in particular areas of the hospital or with regard to specific patients or patient groups.
9. Providers should consider the requirements of the whole hospital environment when developing organisational policies. It will often be appropriate for them to have a separate or supplementary policy framework to effectively meet all of these needs. Providers should also ensure that these policies can only be changed with clearance at the highest management level.

10. When developing, reviewing, amending and implementing these policies, providers should fulfil their responsibilities regarding human rights and equality outlined in paragraphs (4) and (5) above.

11. Providers should ensure that each policy clearly states:
   i) the objective that it is intended to achieve;
   ii) how that objective is to be achieved;
   iii) the key staff group(s) to be involved in its implementation and operation;
   iv) what, if any, scope there is for staff discretion in its operation - it being accepted that within the framework of hospital policies there may be a number of clearly defined areas where clinical units/directorates and clinical teams may exercise discretion to interpret policies to reflect the distinctive needs of a particular patient group;
   v) how and when the policy will be reviewed; and
   vi) who has lead responsibility for the policy.

12. To ensure effective implementation, providers should have appropriate arrangements in place to inform, educate and train staff about the existence of, and reasons for, each policy, together with an efficient audit mechanism.

13. It is recommended that:
   i) all hospital staff have access on request, or direct access, to the Clinical Security Framework;
   ii) an up to date record of all relevant policies is easily and readily available to all ward staff and its location and contents are known by all ward staff;
   iii) the full policy documents are clear, concise. Staff should be required to know the contents of all relevant policies and have become familiar with them before being deployed on a ward. They should be asked to confirm that they have read them and to re-confirm this regarding any changes made to them;
   iv) any changes to policies are immediately recorded in the policies record and communicated to all staff in advance of implementation by an agreed method, such as regular team briefings;
   v) where staff are permitted to use discretion in the exercise of a policy, the reasons for exercising that discretion are recorded;
   vi) the number of policies is maintained at a manageable level so that staff are not overwhelmed and have a realistic prospect of becoming familiar with them. A single page summary attached to each policy, highlighting key principles and instructions for staff, may be useful in this respect.

14. It is recommended that providers share copies of their main policies with each other to encourage sharing good practice and achieving a generally consistent approach across the high secure hospitals. However, it is accepted that there may be some variation in the approach of each provider to reflect their different local circumstances.
Annex A

Protocol for:

i) **risk assessment and management (direction 33);**
ii) **identification and management of ‘high risk’ patients in high security hospitals; and**
iii) **locking these patients in their rooms at night (direction 35).**

Introduction

1. This protocol is designed to ensure that the public, staff and patients in hospitals are protected from harm by addressing systematically the risks that patients may present. It enables the identification of all patients who present high levels of risk in specific areas (see direction 33(4)) and suggests options for the safe management of these risks. It includes consideration as to whether locking patients in their rooms at night should be included within risk management plans in accordance with direction 35 and associated guidance.

2. The mental disorder which led to a patient’s admission to hospital may have a profound effect on the presentation of risk, causing it to fluctuate (often frequently) over time and producing different types of risk in combination. Consideration should be given to the interdependencies of all risks within the risk management plan, and the impact of mitigating action on each risk, to ensure safety is not compromised.

3. This protocol should be used to assess patients at 6-monthly intervals, at least, but the frequency of assessment should be set for individual patients in the light of their clinical condition and security intelligence (see direction 33(9)).

4. For reasons including, but not confined to, their mental disorder, some patients may be unwilling or unable to cooperate with arrangements for managing risks. When developing risk management plans for vulnerable patients, consideration must be given to their capability of making appropriate decisions to protect themselves.

5. Good practice requires the management of patients and identified risks includes the development of a multi-disciplinary care plan, alongside a risk management plan, as a key component of risk reduction is the effective treatment of the patient’s mental disorder.

6. **Model protocol for risk assessments, the determination of ‘high risk’ (direction 33) and the development of risk management plans including whether these should include locking patients in their rooms at night (direction 35).**

7. A comprehensive multi-disciplinary risk assessment must be undertaken and recorded to ensure that all risks are identified (see direction 33). This risk assessment must be used to make a judgment as to whether the patient presents a ‘high risk’ in any of five main categories:
   i) risk of harm to others;
   ii) risk of harm to self (suicide or self-injury);
   iii) risk of being assaulted (i.e. high vulnerability);
   iv) risk of escaping or absconding; and
   v) risk of subverting safety and security, or organising action to subvert safety and security.
8. A management plan for each identified risk should be agreed and documented by the multi-disciplinary team (see direction 33(5)).

9. Review dates should be agreed and documented for each identified risk and its associated management plan (see direction 33(8)). In some instances the review frequency may be determined by the policies governing the specific interventions deployed (e.g. seclusion, close observation etc).

10. In any category, risk may range from ‘no risk’ to ‘high risk’ and this is a matter of clinical judgement. The underpinning reasons for the conclusion must be documented if the patient is assessed as ‘high risk’ in any of the main categories (see direction 33(8)(a)).

11. The clinical team should consult a member of the security department when drawing up the management plan and must do so if the patient is assessed as ‘high risk’. (see direction 33(7)).

12. A decision tree has been designed to standardise the development of risk management plans for each identified risk (see Attachment 1). The use of this and the decisions made should be documented in the patient’s notes.

13. Where the patient is identified as ‘high risk’ such plans could include any one or all of the procedures noted in the decision tree, determined in the light of all relevant clinical factors. Where following this protocol would suggest a patient should be locked in their room at night but this is not pursued, the reasons for not doing so should be recorded.

14. The provider’s policy should include a requirement that, before a decision is taken to include locking a patient in their room in their risk management plan, the patient’s clinical team must first consider whether there are clinical or psychosocial grounds for not locking the patient up at night. For example, this may be a consideration for patients assessed as at risk of taking their own life or self-harming. These risks should be balanced with other risks as outlined in paragraph (2) above.

15. The provider’s policy should include arrangements for reviewing any decision to include locking a patient in their room at night as part of their risk management plan. This should include both a requirement for regular reviews and reviews whenever assessed risk levels change (see direction 33(9)).

16. Locking of patients’ rooms at night, where they have been assessed as ‘high risk’, may contribute to maintaining the safety of patients, staff, public and the overall security of the establishment.

17. Locking a patient into their room at night must only take place if the room has integral sanitation and a staff call system or the patient is continuously observed by a member of staff (see direction 35(2)).

18. Locking a patient in their room at night must be supervised containment and frequent monitoring and review of the patient will be necessary. The local seclusion procedures should be referred to as a model of good practice in this respect, thus ensuring any necessary changes in the patient’s management are made in a timely manner to address changes in the patient’s clinical presentation.
19. Most patients are asleep in their rooms at night. Supervision of corridors is crucial to detecting patient movement, which may be an indication of increasing risk and hence a need to upgrade the risk management plan. Corridor supervision can be enhanced by deploying increased levels of staff. This should be considered as part of the overall risk management policy for the hospital. However, consideration should also be given to deploying technologies (e.g. CCTV monitoring of corridors, video motion detectors, infra-red detectors, bedroom door alarms) to provide technological support to clinical management and enhance risk management by ensuring the untoward movement of any patient will be identified, even when not anticipated.
Protocol for making decisions regarding locking patients in their rooms at night where this is not part of a risk management plan to manage ‘high risk’ (direction 33)

Introduction

1. This protocol sets out the requirements for providers wishing to include arrangements in their policies for locking individual patients, or groups of patients, in their room(s) at night (direction 35) where this is not part of a risk management plan to manage their ‘high risk’ (direction 33), nor patients locked in their rooms as part of local seclusion policies.

2. Providers may include these arrangements within their policies but these should only be put in place where it is considered that this will maximise therapeutic benefit for patients, as a whole, in the hospital. For example, confining a group of patients at night may release staff to facilitate greater therapeutic input for patients during the day.

3. No patient should be locked in their room at night if it is considered this would have a detrimental effect on their well-being (see paragraphs (5) & (6) below).

4. Groups of patients should only be locked in their rooms at night following discussion and approval at Board level. These arrangements should be reviewed on a regular basis.

5. Paragraphs (5) & (6) concern the periodic review of whether individual patients should routinely be locked in at night. The provider’s policy should include a requirement that, before a decision is taken to lock a patient in their room at night, the patient’s clinical team must consider whether there are clinical or psychosocial grounds for not taking this action.

6. Arrangements should also be made for reviewing decisions if there are circumstances, for example the risk of suicide or self-harm, which would indicate that locking the patient in their room at night might have a detrimental effect on their well-being or be unsafe.

7. Locking a patient in their room at night must only take place if the room has integral sanitation and a staff call system or the patient is continuously observed by a member of staff (see direction 35(2)).

8. Locking a patient in their room at night must be supervised containment and frequent monitoring and review of the patient will be necessary. This is to ensure that any necessary changes in the patient’s management are made in a timely manner to address changes in the patient’s clinical presentation. Locked-in patients should not be left unsupervised at night, and there must be capacity to unlock them at any time if clinically indicated.
Attachment 1

Decision Tree for Risk Management of 'high risk' Patients
(including decisions about locking them in their rooms at night to manage risk)

All Patients

**YES**

High risk of suicide or self harm?

- These patients **should not** normally be locked in their rooms. Management strategies to consider include those listed in box 1 & box 6 (Attachment 2)

**NO**

Also consider

- High risk of being assaulted?

**YES**

Also consider

- High risk of escape?

**YES**

Also consider

- High risk of immediate harm to others?

**YES**

Also consider

- High risk of subverting Security?

**YES**

These patients **should** be locked in their rooms at night unless deployment of other measures reduces the risk. Management strategies to consider include those listed in Box 4 & Box 6 (Attachment 2)

**NO**

These patients **may** be locked in their rooms. Management strategies to consider include those listed in Box 2 & Box 6 (Attachment 2)

- These patients **should** be locked in their rooms at night unless deployment of other measures reduces the risk. Management strategies to consider include those listed in Box 3 & Box 6 (Attachment 2)

- These patients **should** be locked in their rooms at night unless deployment of other measures reduces the risk. Management strategies to consider include those listed in Box 5 & Box 6 (Attachment 2)

These patients **should** be locked in their rooms at night unless deployment of other measures reduces the risk. Management strategies to consider include those listed in Box 6 (Attachment 2)
Attachment 2

Management Strategies Supporting the Decision Making for the Risk Management of ‘High Risk’ Patients

Box 1

**High Risk Suicide / Self Harm**

- specific treatment focussed on suicide/self-harm for the individual;
- reduced access to risk items;
- enhanced levels of observation (refer to the hospital’s observation policy);
- enhanced emotional support; and
- occasionally a suicidal/self-harming patient is also violent and prone to assaulting others and in this situation the patient may be locked in their room at night in conjunction with enhanced levels of observation[^3].

Box 2

**High Risk of Being Assaulted**

- enhanced levels of observation (refer to the provider’s observation policy);
- geographical manipulation i.e. consider moving the patient away from individual(s) posing risk or restrict access to such individual(s);
- voluntary locking into room for periods of day or night. Many of these patients will co-operate with measures to enhance their safety, including agreeing to remain in their rooms for specified periods. But consideration must be given to the patient’s ability / willingness to protect themselves; and
- Voluntary exit from rooms should be maintained if possible but locking into room for identified ‘high risk’ periods only (e.g. night-time)[^3] may be considered.
**Box 3**

**High Risk of Escape or Absconding**

- locking in room for identified ‘high risk’ periods (e.g. night time);  
- geographical manipulation i.e. consider moving the patient to a higher staffed location, or restrict access to a more confined area of the ward;  
- enhanced monitoring of visits (including closed visits) or temporary suspension of visits;  
- enhanced monitoring of mail and telephone calls;  
- enhanced precautions for leave of absence from hospital (refer to policy);  
- enhanced escorting (to be specified precisely) for movement within hospital’s secure perimeter;  
- enhanced levels of observation (refer to the provider’s observation policy);  
- enhanced restrictions on access to risk items;  
- enhanced search/drug screening procedures.

**Box 4**

**High Risk of Immediate Harm to Others**

- locking in room until judged safe to end such locking in – in accordance with seclusion policy;  
- locking in room for identified ‘high risk’ periods only (e.g. night time);  
- Longer term segregation should be considered if the risk is continuous and other management strategies are not considered sufficient to manage the risk;  
- geographical manipulation i.e. consider moving the patient to a higher staffed location or away from provocation, or restrict access to a more confined area of the ward;  
- enhanced levels of observation (refer to the provider’s observation policy);  
- enhanced restrictions on access to risk items;  
- enhanced search/drug screening procedures;  
- enhanced monitoring of visits (including closed visits) or temporary suspension of visits.
Box 5

**High Risk of Subverting Security**

- locking in room for identified ‘high risk’ periods (e.g. night time);  
- geographical manipulation i.e. consider moving the patient to a higher staffed location, or restrict access to a more confined area of the ward;  
- enhanced monitoring of visits (including closed visits) or temporary suspension of visits;  
- enhanced monitoring of mail and telephone calls;  
- enhanced precautions for leave of absence from hospital (refer to policy);  
- enhanced escorting (to be specified precisely) for movement within hospital’s secure perimeter;  
- enhanced levels of observation (refer to the provider’s observation policy);  
- enhanced restrictions on access to risk items;  
- enhanced search/drug screening procedures.

Box 6

**Corridor Supervision at Night**

Corridor supervision can be enhanced by increasing levels of staff and this should be considered as part of risk management. Consideration should also be given to deploying technology to enhance corridor supervision. Appropriate technology would include CCTV monitoring of corridors, video motion detectors, infra-red detectors, and door alarms. These can all be used to give early warning of untoward patient movement.

*Note 1:* if these measures do not reduce the risk of escape in the view of the clinical team and security department, then locking in for ‘high risk’ periods will be necessary (see paragraphs (33) & (35) of the Directions).

*Note 2:* a decision not to lock a patient in their room at night in accordance with the protocol should be clearly documented in the notes.

*Note 3:* locking patients in their rooms at night should be supervised (see paragraph (15) of the protocol).