Department of Health

Guidance on the High Security Psychiatric Services (Arrangements for Safety and Security at Ashworth, Broadmoor and Rampton Hospitals) Directions 2011

DH INFORMATION READER BOX

Policy
HR / Workforce
Management
Planning /
Clinical
Estates
Commissioning
IM & T
Finance
Social Care / Partnership Working

Document Purpose	Policy
Gateway Reference	16188
Title	Guidance on the High Security Psychiatric Services (Arrangements for Safety and Security in Ashworth, Broadmoor and Rampton Hospitals) Directions 2011
Author	Mental Health and Disabilities Division, DH
Publication Date	24 Jun 2011
Target Audience	High secure psychiatric services providers
Circulation List	
Description	Guidance on the safety and security directions and safety and security arrangements in the high secure hospitals
Cross Ref	N/A
Superseded Docs	Guidance on the Safety and Security Directions 2001
Action Required	Implementation of guidance on new directions
Timing	**Directions come into force on 1 August 2011**
Contact Details	Helen Causley Secure Services Department of Health 133-155 Waterloo Road, London SE1 8UG 020 79724757
For Recipient's Use	

Guidance on the High Security Psychiatric Services (Arrangements for Safety and Security at Ashworth, Broadmoor and Rampton Hospitals) Directions 2011

Prepared by Helen Causley and Chris Sharpe

First published July 2011
Published to DH website, in electronic PDF format only.
http://www.dh.gov.uk/publications

The High Security Psychiatric Services (Arrangements for Safety and Security at Ashworth, Broadmoor and Rampton Hospitals) Directions 2011

1. The Secretary of State has revised the Safety and Security Directions originally given to the Ashworth, Broadmoor and Rampton Hospital Authorities under cover of [HSC 1999/150 published on 28 June 1999. The revised Directions come into force on 1 August 2011. Mersey Care NHS Trust, West London Mental Health NHS Trust, and Nottinghamshire Healthcare NHS Trust are required to ensure that the new Directions are implemented with effect from those dates.

New issues covered by the revised Directions include:-

- A duty upon the Trusts to co-operate with each other in developing security arrangements.
- Searching of patients involving the removal of clothing
- Specified employment opportunities
- Provision of Training

In addition, changes to issues covered in the previous Directions include:-

- More rigorous reporting requirements
- The introduction of a limited exemption from patient searches in exceptional circumstances
- The removal of the Chief Executives' authority to permit vehicles and their occupants to be exempt from search requirements
- Improved requirements for the management of vehicles within the secure area.
- Improved requirements for the management of Patients' property including improved access to property in storage.
- Removal of the ban on patients accessing the internet and introduction of detailed arrangements governing how access to computers and games consoles should be controlled and managed
- Improved controls on mobile phones
- Provision to allow telephone contact with the Samaritans
- More rigorous risk assessment requirements
- Changes to the arrangements for locking patients in their rooms at night
- Extended requirements for the management of Leaves of absence

2. This document contains:-

i. general information (paragraphs 3 to 5.) about The High Security Psychiatric Services (Arrangements for Safety and Security at Ashworth, Broadmoor and Rampton Hospitals) Directions 2011

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).

Action

3. The Directions are issued by the Secretary of State for Health and are mandatory upon the Trusts, which run the high security hospitals. The Guidance contains recommendations, which are not mandatory, but the Directions set out reporting requirements should a Trust choose to deviate from them.

Human Rights and Equality

4. When implementing these Directions and when considering this and other related guidance each Trust is responsible for doing so in a way which takes issues of Human Rights into consideration and :-

i) eliminates unlawful discrimination on grounds of race, gender and disability; and promotes equality of opportunity between racial groups, men and women, and disabled and other people.

ii) promotes equality and eliminates discrimination.

5. They should take a similar approach to equality in terms of religion and belief, age and sexual orientation.

Specific guidance on Directions

6. This section of the Guidance is specifically about the implementation of certain of the requirements contained in The High Security Psychiatric Services (Arrangements for Safety and Security at Ashworth, Broadmoor and Rampton Hospitals) Direction 2011.

Direction 2: Interpretation.

Definition of “admission facility” – for the purposes of Direction 6 (4) an “admission facility” should include suitable facilities to carryout a search involving the removal of clothing other than outer clothing whilst maintaining the patient’s dignity and privacy.

Definition of “grounds access” - this does not include unescorted patient access into ward garden areas if;

- the garden area is only accessible from the patient’s ward,
- 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

- access is approved by the patient's clinical team following individual documented risk assessment

Definition of "postal packet" - "Postal packet" has the meaning given in the Mental Health Act 1983, and is defined in the Postal Services Act 2000 as a "letter, packet or other article transmitted by post".

Definition of "responsible clinician" - This will include any person appointed by the Trust to provide cover in the absence of the "responsible clinician" (e.g. during non-working hours, annual leave etc)

Definition of "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.

<u>Direction 3:</u> 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 by phone. Trusts should, however, always report non-compliances in writing.

In addition to the requirement to comply with the Directions and to have regard to this guidance and the associated reporting requirements, Trusts have agreed to implement arrangements for the management of safety and security in accordance with the additional detailed advice available within the Clinical Security Framework. If a Trust decides to implement arrangements other than in accordance with the content of the Clinical Security Framework they should notify the Strategic Health Authority responsible for the area in which the Trust is located.

The Directions and Guidance together with the advice within 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 hospital authorities. The intention is, however, that their implementation will, in contributing to the provision of a safe environment for patients and staff, enhance rather than provide a barrier to 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 the Trusts should have in place. Each individual Trust 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 and employment legislation and legislation relating to drugs management and misuse.

<u>Direction 5:</u> Requirements for conducting a rub-down search of a patient

It is recommended that a rub-down search should 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.

As the Directions state, rub-down searches should, 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 (eg jacket, cardigan) that are bulky and inhibit a proper search being conducted.

Each Trust 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.

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

It is recommended that, 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 might deter patients witnessing thorough searches from attempting to conceal illicit items.

The Trusts 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.

The requirement to carryout a rub-down search immediately before and immediately 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 searching of therapy, workshop, recreation and leisure facility areas, and other non-ward areas which a patient may visit in the secure area, has been limited to not less than once every three months in the expectation that the arrangements for searching and the supervision of patients, checking of tools before and after sessions and the nature of the patients' access will minimise the risk of illicit items being hidden in those areas.

Direction 10: Security of tools, equipment and materials

In drawing up their instructions for members of staff regarding the control of tools, equipment and materials in the secure areas of the hospitals, it is recommended that the Trusts should be guided by the contents of Function 1 (outcome 1.5) of the Clinical Security Framework.

Direction 11: Searches of members of staff

Guidance on what constitutes a rub-down search is contained above, in the guidance to Direction 5 ‘Requirement for conducting a rub-down search of a patient.

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

Only visitors who have had a CRB 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

Guidance on what constitutes a rub-down search is contained in the guidance to Direction 5 ‘Requirement for conducting a rub-down search of a patient.

The bringing and sending of food items into the hospital presents great difficulties in terms of checking for concealed illicit items. It also presents potential health hazards. The restrictions on bringing and sending food into the hospitals other than in limited and carefully controlled circumstances is intended to address these concerns. The hospitals will need to have a sufficiently varied range of food available on site to cater for differing tastes among the patient/visitor group. The restriction on people bringing or sending tobacco products into the hospitals is because of the difficulty in checking such products for the presence of drugs.

The Security Director should be informed of any decision to allow a visitor to bring food into a hospital under paragraph 5 (b) of this Direction.

There is no legal power to routinely require a visitor to submit to a search. However, other than in the case of the limited exceptions identified in this Direction the hospital authority is entitled to refuse admission to anybody who refuses to be searched. Requiring visitors to submit to searches on their way out of the hospital is more problematic because visitors cannot be prevented from leaving the hospital. There should, however, be no need to search visitors on leaving since they will have been searched on entry and, as long as the search of the patient prior to the visit has been properly carried out, it should not have been possible for the patient to pass any inappropriate items to the visitor. If there is nevertheless 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 perhaps informing the visitor that entry may be refused on a future occasion.

Care will need to be taken with regard to the obtaining of consent to the searching of 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. 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 search under Direction 12 (10) should be invited to participate in rub-down search in the interests of their own safety and that of the safety and security of the hospital. On each occasion where a Tribunal member enters the secure area of the hospital they should be invited to participate in the rub-down search and a record should be made of whether or not they have participated.

Senior members of the Royal family are those 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. There may however be some circumstances, in which 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 always be possible to X-ray all the 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 hospitals. The Trusts will, however, need to have in place suitable arrangements for:-

i. the checking of contractors’ tools and other equipment both on arrival at, and departure from, the secure area,

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

It is also recommended that the Trusts should be guided 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

Care will need to be taken with regard to the obtaining of consent to the searching of 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. 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.

There is no legal power to routinely require a visitor to submit to a search. However, other than in the case of the limited exceptions identified in this Direction the hospital authority is entitled to refuse admission to anybody who refuses to be searched. Requiring visitors to submit to searches on their way out of the hospital is more problematic because visitors cannot be prevented from leaving the hospital. There should, however, be no need to search visitors on leaving since they will have been searched on entry and, as long as the search of the patient prior to the visit has been properly carried out, it should not have been possible for the patient to pass any inappropriate items to the visitor. If there is nevertheless 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 perhaps informing the visitor that entry may be refused on a future occasion.

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 and 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

In drawing up their instructions for members of staff managing and escorting vehicles within the secure areas of the hospitals, it is recommended that the Trusts should be guided by the contents of Function 1 (Outcome 1.6) and Function 3 (outcome 3.4) of the Clinical Security Framework.

This Direction requires all vehicles to be checked before they enter or exit 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 supervision arrangements for the vehicle.

In making its arrangements for the management of contractors' vehicles in the secure area, it is recommended that the Trusts should also be guided 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 be made aware of the requirements within the Directions for Trusts 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 be seen as an indication that the patient has something to hide but it will be for the Trusts to decide what action to take in the event of a refusal in the light of the pertaining circumstances.

Direction 20: Security information

When developing their policies regarding the maintenance and use of their security information records, it is recommended that the Trusts be guided by the contents of Function 4 (outcome 4.2) of the Clinical Security Framework. Trusts should also be guided by the following:

Security records must be developed and maintained on-

i) security information relating to each patient; and

ii) other security information relating to the Hospital

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

The 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 need to be set up with due regard to rules surrounding patient confidentiality and 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.

Direction 21: Patients' possessions

When developing their policy on the arrangements for managing patients' property, it is recommended that the Trusts be guided by the contents of Function 1 (Outcome 1.11) of the Clinical Security Framework. Trusts should also be guided by the following:

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.

The possessions in patients' rooms and their personal lockers need to be limited to a level and type which are compatible with the facilitation of searching, the maintenance of security and the reduction of fire hazards. There is also a need to manage the risk presented by the potential to misuse technology, particularly that capable of displaying, recording, storing and distributing images and other data.

With these objectives in mind, it is recommended that, as far as patient access to electrical and related items within their rooms is concerned, Trusts should include the following arrangements:-

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

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, this 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 hospital should have a strategy for managing patient 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 hospital.

ii) Access to equipment capable of recording televised material should only be allowed if the hospital 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.

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. Restrictions also apply to most games machines (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, have agreed that the patient may have.

<u>Direction 22</u>: Items delivered or brought to hospital premises for patients and <u>Direction 26:</u> 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.)

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

Hospitals will need to have arrangements for managing items delivered to the hospital for patients that the patient is not allowed, either because they breach the directions or hospital policy.

<u>Direction 23</u>: Patients' access to computer equipment and games consoles

When developing their systems and policies for patient access to, and usage of, computer equipment and games consoles trusts are advised that;

a) Patient accessible IT must be connected to a dedicated network.

b) There must be secure separation of staff and patient networks. Where this is achieved by virtual as opposed to physical separation, the configuration and management arrangements should be independently health-checked by an expert. It is the responsibility of the Hospital Senior Information Risk Owner to ensure that these health checks are made at least annually and the results recorded.

c) Patients should only access either 'thin client' terminals or a PC configured as a thin or virtual desktop client with read/write access to the local drive blocked. Where a Trust allows access to PCs configured as thin or virtual desktop clients, the arrangements should be independently health-checked by an expert. It is the responsibility of the Hospital Senior Information Risk Owner to ensure that these health checks are made at least annually and the results recorded.

d) All processing capability and software should be on a remote server that is not in a patient area.

e) Patients should not have access to removable / transportable media e.g. recordable or re-writeable CDs, DVDs, memory sticks etc or any CD ROMs etc.

f) There should be a rigorous documented approval process for a patient's access to computers, applications, software and Internet material etc. This process must be patient specific and must include:

- identification of the reason for access
- a thorough risk assessment which includes individual assessments of:
  - access to the computer and any other hardware

    - applications, software etc that it is intended the patient should use e.g. access to software packages such as word processing, spreadsheets, etc
    - access to any internet sites.
- approval by the patient's clinical team for all applications for access.
- consideration and authorisation by a multidisciplinary group chaired by the Security Director.

g) Other than the exception below, there should be no live access to the Internet. Access will normally be limited to cached material.

h) Live access to the Internet should be an exceptional event which should only be allowed where absolutely essential e.g. participation in an educational examination which is only available on line and must be completed live. Any live access to the Internet must be supervised on a one to one basis.

i) All Internet access must be managed via a 'white list'. All permitted sites must be rigorously vetted and patient access must be individually approved.

j) All patient access must be directly supervised

k) There must be live remote monitoring capability from the supervisor's PC

l) All patients approved for access must have a unique log on which is not known to them.

m) Patients must be logged on to a terminal remotely by the supervisor using the supervisor's PC.

n) The management system must have access control levels which should be set up to prevent those staff supervising patients from making changes to a patient's access rights.

o) Adjustments to patients' access rights should only be made by an authorised member of staff. This member of staff should not be involved in direct supervision of patients.

p) The system must use electronic activity and behaviour monitoring systems to detect abuse / misuse by the patients.

q) The system must use appropriate filtering systems.

r) The system should not allow live email communication and any communication using electronic media must be examined as if it were a letter.

s) It is not appropriate to allow privileged communication to be sent electronically.

t) The system must be comprehensively auditable i.e. all changes to the system set up must be auditable and must be regularly audited by staff not in direct contact with patients.

u) Detailed records must be maintained of all patient access to IT.

v) There must be a comprehensive audit of all patient access onto the system. This must include:

- A review of patient activity, including review of the reports produced by the activity and behaviour monitoring systems, by those supervising the access, as soon as practicable following a session.
- A review of patient activity, system reports and supervisor monitoring activity by those managing the system

w) Regular reports should be provided to clinical teams on their patients' access rights and use of IT.

x) Aggregated information should be provided to hospital managers to enable them to monitor IT access by patients.

Direction 25: Role of patients in managing or working in patients' shops and other specified employment

To identify whether any employment opportunities open to patients in their hospital should be managed under this Direction the Trust should consider the risks associated with all work placements available to patients.

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 trust 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 propose that working in a patients' shop or one of these 'specified employment opportunities' should be included as part of that 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 reasons for withholding it,

- that they can request that the Chief Executive review the decision to withhold and
- that they can take the postal packet when they leave the secure area.

Direction 31; Patients' outgoing telephone calls

Where a Trust 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. the caller is a patient in another high security hospital or other establishment which restricts incoming calls.

Direction 33: Risk assessments and Direction 35: Security at night

Each Trust 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 of matters 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 thing as seclusion.

Paragraph 15.43 of the Mental Health Act 1983 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 disturbed behaviour and its purpose is to control severely disturbed behaviour in the here and now. Seclusion 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, because of 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 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. Long-term segregation is similarly for a different purpose. Night-time confinement in accordance with the directions is something that is pre-determined and will only be 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.

Annex A provides an example of a protocol which should be followed in order 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.

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

Direction 38: Functions of the Grounds Access Committee

When granting Grounds Access the Grounds Access Committee should 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 their responsibilities, keep under review the question of the total number, and the mix, of patients who should be permitted ground access at any one time.

Direction 40: Leave of Absence

When developing their policies for the management of leaves of absence, Trusts should ensure that they are compliant with the Ministry of Justice guidance to responsible clinicians on the subject and the guidance within Function 1 (Outcome 1.3) of the Clinical Security Framework. They should also consider the following:

- Child protection issues should be a central consideration in leave of absence planning. Contact between patients and named children during a leave of absence should be approved following the principles outlined in the Visits by Children to Ashworth Broadmoor and Rampton Hospitals Directions.
- When leave of absence is used for rehabilitation purposes, it should be written into a care plan and have clear objectives.
- Whilst the responsible clinician has statutory power to grant leave of absence (subject to Ministry of Justice consent where necessary), there is a managerial responsibility on the Chief Executive to consider and advise on safety issues which is reflected in the requirement for the Security Director to approve all leave of absence management plans. Leaves of absence should not take place unless the management arrangements are approved.
- Unescorted leave of absence from a high security hospital is only likely to be appropriate in exceptional circumstances.

Direction 41: Escorting patients

In drawing up instructions to members of staff on carrying out escorting duties, including the appropriate use of handcuffs and escorting chains, it is recommended that the Trusts should be guided by the contents of Function 1 (outcome 1.3) of the Clinical Security Framework.

Direction 42: Security of keys and locks

In drawing up their instructions for members of staff on the security of keys and locks, it is recommended that the Trusts should be guided by the contents of Function 7 (Outcome 7.6) of the Clinical Security Framework

Direction 44: Provision of training

When developing training on the non physical management of violence and aggression for members of staff and other key holders, Trusts should be guided by advice from the Security Management Service.

General guidance on policies

7. Whilst the Trusts are required by Direction 4 to work together to develop safety and security arrangements; it will be for each individual Trust to develop its policies around the Directions, Guidance and the content of the Clinical Security Framework and to decide 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.

8. Trusts should consider the requirements of the high security hospital for which they are responsible when developing Trust Policy. It will often be appropriate for them to have a separate or supplementary policy to effectively meet the needs of the high security hospital.

9. When developing, reviewing, amending and implementing policies Trusts should pay due regard to their responsibilities regarding equality outlined in paragraphs 4 and 5 above.

10. Trusts should ensure that the high secure hospital for which they are responsible has clear hospital-wide policies which cannot be changed except at the highest management level and that each policy should clearly state:-

- the objective that it is intended to achieve,
- how that objective is to be achieved,
- the key staff group(s) to be involved in its implementation and operation,
- 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,
- at what frequency the policy will be reviewed and
- who has lead responsibility for it

11. In order to ensure effective implementation, the Trusts will need to 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.

It is recommended that:-

- at all times an up to date record of all relevant policies should be easily and readily available to all ward staff, and its location and contents should be known by all ward staff;

- the full policy documents should be clear, concise and easily available to all staff in a single file. Staff should be required to know the contents of all relevant policies and to have read and be aware of them before they start working on a ward. They should be asked to confirm that they have read them and to re-confirm regarding any changes made to them;

- any changes to policies should be made known to all staff in advance by an agreed method, such as regular team briefings;

- the changes should immediately be recorded in the policies record before implementation;

- where staff are permitted to use discretion in the exercise of a policy, the reasons for the exercise of that discretion should be recorded;

- while it is clearly important that there should be a comprehensive set of policies, efforts should be made to keep the number of them to manageable proportions so that staff are not overwhelmed by paper and have a realistic prospect of being familiar with them. A single page summary attached to each policy, highlighting key principles and instructions for staff, may be useful in this respect.

12. It is recommended that the Trusts should share copies of their main policies with a view to disseminating good practice and achieving a generally consistent approach. That is not to say that there will not need to be some variations between the hospitals due to different local circumstances.

Annex A

Protocol for:-

(i) risk assessment and management

(ii) the Identification and Management of "High Risk" Patients in High Security Hospitals (Direction 33); and

(iii) locking these patients in their rooms at night (Direction 35)

Introduction

1 This protocol is designed to ensure that the public and the staff and patients in the hospitals are protected from harm by addressing systematically the risks that patients 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 their risks. It includes consideration as to whether locking them in their rooms at night should be included in their risk management plans in accordance with Direction (35) and associated Guidance.

2 The mental disorder which has led to the patient's admission to the 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, such that the preferred way of managing one risk compromises the safe management of another.

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).

3 Good practice requires that the management of patients and the risks they present will include the development of a multi-disciplinary care plan, as a key component of risk reduction is the effective treatment of the patient's mental disorder.

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

5 A comprehensive multi-disciplinary risk assessment will 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:

- risk of harm to others
- risk of harm to self (suicide or self injury)
- risk of being assaulted (i.e. high vulnerability)
- risk of escaping or absconding

- risk of subverting safety and security, or organising action to subvert safety and security.

In any category, risk may range from 'no risk' to 'high risk' and this is a matter for clinical judgement. The underpinning reasons for the conclusion should be documented and **must** be documented if the patient is assessed as 'high risk' (see Direction 33(8) (a)).

6 The risk assessment protocol must be used to assess patients at least 6 monthly but frequencies will be set for individual patients in the light of their clinical condition and security intelligence (see Direction 33(9)).

7 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.

8 A management plan for each identified risk should be agreed and documented by the multi-disciplinary team (see Direction 33(5))

9 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.

10 The hospital policy should include a requirement that, before a decision is taken to include locking a patient in his room at night in a patient's 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. In the case of a patient assessed as at risk of committing suicide or self harm this consideration will take into account these risks. These risks must, however, be balanced with other risks.

11 Hospital policy should include arrangements for reviewing any decision to include locking a patient in his room at night as part of his risk management plan. This should include both a requirement for regular reviews and reviews whenever assessed risk levels change (see Direction 33(9)).

12 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)).

13 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).

14 Locking of patients' rooms at night, where they have been assessed as 'high risk', will contribute to maintaining the safety of patients, staff, public and the overall security of the establishment.

15 Locking a patient into their room at night should 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)).

16 Locking patients into their room at night should 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.

17 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 risk management. 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.

Annex B

Protocol for making decisions regarding the locking in their rooms at night of patients who are not locked in at night as part of a risk management plan to manage their "High Risk" (Direction 33)

Introduction

1 This protocol sets out the requirements for Trusts wishing to include arrangements in their policies for locking individual patients or groups of patients in their rooms at night (Direction 35) who are not patients locked in at night as 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.

Model Protocol for Trusts wishing to include arrangements for locking of patients in their rooms at night for reasons other than the management of "High Risk" or seclusion.

2 Trusts may include within their policies arrangements for patients (other than those locked in their rooms at night as part of a risk management plan to manage their high risk) to be locked in their rooms at night (Direction 35). Arrangements 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 also paragraph 5 & 6 below).

4 Groups of patients should only be locked in their rooms at night following discussion and approval by the Trust Board. This should be reviewed on a regular basis.

5 Paragraph 5 & 6 concern the periodic review of whether individual patients should be subject to routine locking in at night. The hospital policy should include a requirement that, before a decision is taken to lock each patient in their room at night, the patient's clinical team must regularly consider whether there are clinical or psychosocial grounds for not locking the patient up at night.

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.

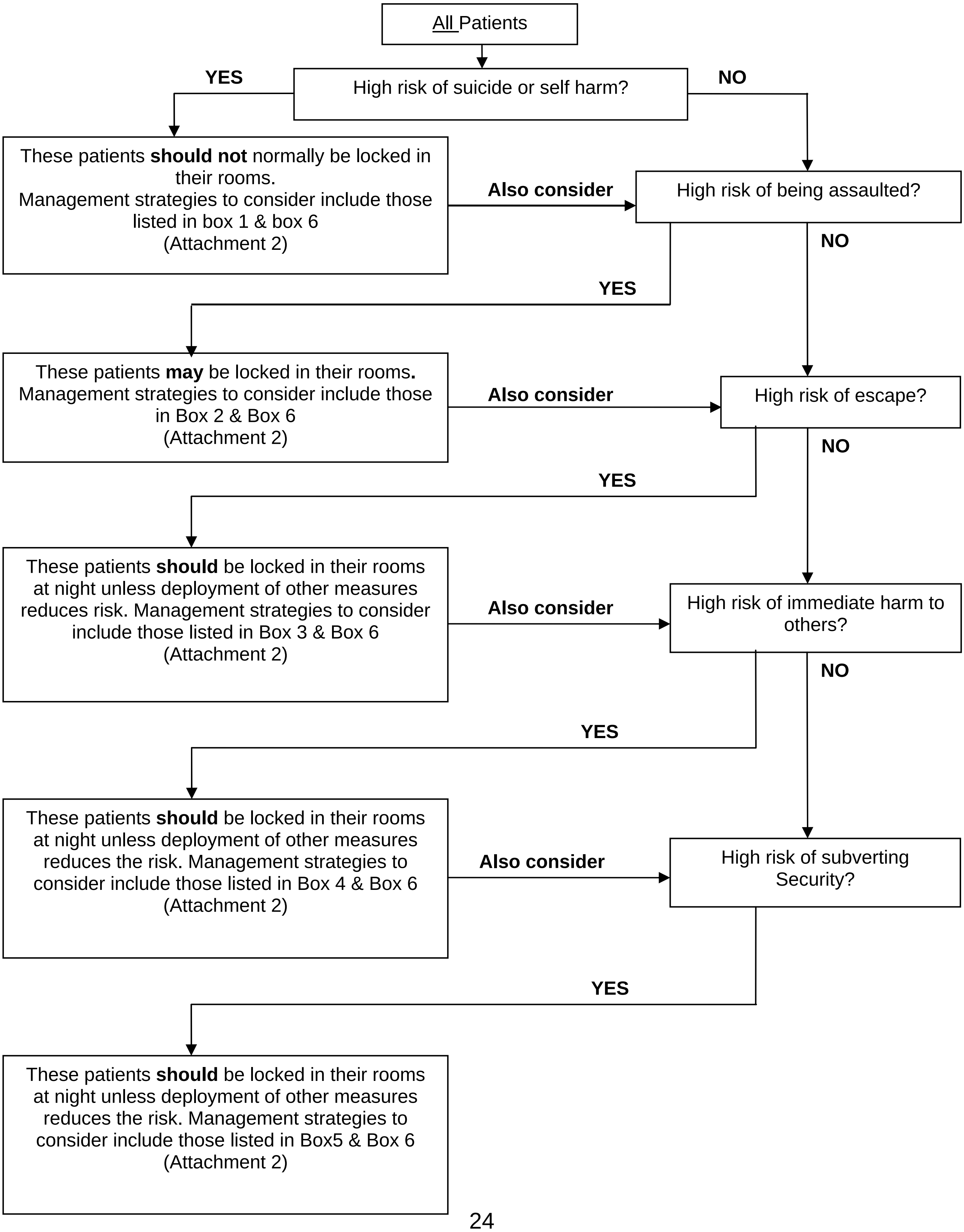
7 Locking a patient into their room at night should only take place if the room has integral sanitation and a staff call system or the patient is continuously observed by a member of staff (see paragraph 35(2) of the Directions).

8 This paragraph is about responding to what happens in the course of a particular night. Locking patients into their room at night should 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

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)

High risk of being assaulted?

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

High risk of escape?

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

High risk of immediate harm to others?

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)

High risk of subverting Security?

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 Box5 & 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
- occasionally a suicidal/self harming patient is also violent and assaultative 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 hospital'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.
- 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 into room for identified high risk periods (e.g. night time) [2] [3]
- geographical manipulation i.e. consider moving the patient to a higher staffed location, or restrict access to a more confined area of the ward[1]
- enhanced monitoring of visits (including closed visits) or temporary suspension of visits[1]
- enhanced monitoring of mail and telephone calls[1]
- enhanced precautions for leave of absence from hospital (refer to policy)[1]
- enhanced escorting (to be specified precisely) for movement within hospital's secure perimeter[1]
- enhanced levels of observation[1] (refer to the hospital's observation policy)
- enhanced restrictions on access to risk items
- enhanced search/drug screening procedures[1]

Box 4

High Risk of Immediate Harm to Others

- locking into room until judged safe to end such locking in – in accordance with seclusion policy
- locking into room for identified high risk periods only (e.g. night time) [2, 3]
- 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[1]
- enhanced levels of observation[1] (refer to the hospital's observation policy)
- enhanced restrictions on access to risk items
- enhanced search/drug screening procedures[1]
- enhanced monitoring of visits (including closed visits) or temporary suspension of visits[1]

Box 5

High Risk of Subverting Security

- locking into room for identified high risk periods (e.g. night time) [2, 3]
- geographical manipulation i.e. consider moving the patient to a higher staffed location, or restrict access to a more confined area of the ward[1]
- enhanced monitoring of visits (including closed visits) or temporary suspension of visits[1]
- enhanced monitoring of mail and telephone calls[1]
- enhanced precautions for leave of absence from hospital (refer to policy)[1]
- enhanced escorting (to be specified precisely) for movement within hospital's secure perimeter[1]
- enhanced levels of observation[1] (refer to the hospital's observation policy)
- enhanced restrictions on access to risk items
- enhanced search/drug screening procedures[1]

Box 6

Corridor Supervision at Night

Corridor supervision can be enhanced by the use increased 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 paragraph 33 & 35 of the Directions).*

NOTE 2: *a decision not to lock a patient in his 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).*