Department
of Health &
Social Care

Guidance on the High Security Psychiatric Services (Arrangements for Safety and Security) Directions 2019

Published 21 June 2019

Contents

1. Introduction 2

2. Status of the Directions and Guidance 3

3. Human Rights and Equalities Legislation 4

4. Guidance on the implementation of specific Directions 5

5. General guidance on policies 21

6. Annex A: Risk assessments, the determination of ‘high risk’ and risk management plans...24

7. Annex B: Protocol for locking non 'high risk' patients in their rooms at night...............27

Attachment 1: Decision tree for risk management of high risk patients 29

Attachment 2: Management strategies 30

1. Introduction

1.1 This guidance accompanies the High Security Psychiatric Services (Arrangements for Safety and Security) Directions 2019, which apply to providers of high security psychiatric services.

1.2 This document contains:

(a) general information (paragraphs (2.1) to (2.2)) about the High Security Psychiatric Services (Arrangements for Safety and Security) Directions 2019;

(b) specific guidance about the implementation of certain requirements contained in the Directions (paragraph (4.1));

(c) general guidance on the way policies (including procedures and protocols) should be produced, and promulgated to staff within the high security hospitals (paragraphs (5.1) to (5.10));

(d) **annexes A & B**: protocols for the identification and management of 'high risk' patients and locking patients in their rooms at night;

(e) **attachment 1**: the decision tree for risk management of 'high risk' patients; and

(f) **attachment 2**: the management strategies supporting the decision making for the risk management of 'high risk' patients.

2. Status of the Directions and Guidance

2.1 The Directions are issued by the Secretary of State for Health and Social Care and providers of high security psychiatric services must comply with them. This guidance is not mandatory, but providers must have regard to it. Providers must also have regard to the NHS England Clinical Security Framework. Direction 3 sets out reporting requirements where a provider is not compliant with the Directions, guidance or the NHS England Clinical Security Framework and any action it is taking to become compliant.

2.2 The High Security Psychiatric Services (Arrangements for Safety and Security) Directions 2019 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. Arrangements for visits by vulnerable adults must be included within the high security hospitals local policies and procedures.

3. Human Rights and Equalities Legislation

3.1 When implementing the Directions and guidance, providers are responsible for doing so in a way which takes human rights and equalities into consideration to ensure they comply with:

(a) The Human Rights Act 1998; and

(b) The Equality Act 2010.

4. Guidance on the implementation of specific Directions

4.1 This section of the guidance is specifically about the implementation of certain requirements contained in the Directions. Only those Directions which required further detailed guidance, clarification, or pose a greater security risk have been included.

Direction 2: Interpretation

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

(a) “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);

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

(c) “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

To comply with the requirements of paragraph (2) of this Direction each provider must have regard to this guidance and the NHS England Clinical Security Framework in addition to complying with the requirements set out in the Directions.

To comply with the requirements in paragraph (3) of this Direction to report non-compliance without delay, initial contact may be made by telephone by an officer of the provider delegated this authority by the Chief Executive. However, the Chief Executive of the relevant provider of high security psychiatric services must also report non-compliances in writing without delay to NHS England and NHS Improvement.

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, 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 rub-down search as described in 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. 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 (2) 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 all patients are made aware of the searching processes that affect them.

A member of staff has the authority to undertake a rub-down search of a patient if they have “reasonable grounds” to believe that the patient possess’ an item which causes an immediate risk to the patient’s own safety or the safety of any other person. This would include any concern about tools, improvised weapons or items, including drugs or prescribed medication, that may be used to either commit deliberate self-harm or harm another person.

“Reasonable grounds” would include situations where a patient is believed to have an improvised a weapon; a tool or implement is known to be missing and has not been accounted for; and, security intelligence provides a reasoned view that a patient has an item or items that may cause an immediate risk to themselves or others.

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:

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

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

(c) the arrangements for authorising a search of this type.

If a search without consent is authorised, or the search is being undertaken under paragraph (2) 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 all patients are made aware of the searching processes that affect them.

“Reasonable grounds” for the searching of a patient under paragraph (2) of this Direction reflects that as required for the decision-making process as set out in this guidance for Direction 5.

“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.

Direction 7: Searches of patients, rooms and lockers

When developing the local hospital policy in respect of the routine searching of patients, their rooms and lockers the provider should have regard to the standards set out in the Clinical Security Framework.

Unless circumstances dictate otherwise, a patient should be present when their room, locker, and possessions 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.

Decisions to undertake a search of a patient’s room and any locker used by that patient pursuant to Direction 7(3) should be based on reliable intelligence and reasonable suspicion that a search maybe required.

A decision to undertake a rub-down search of a patient must meet requirements of Direction 5.

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

Direction 8: Searches when patients move around the secure area

When developing the local hospital policy in respect of the searches of patients who move around in the secure area the provider should have regard to the standards set out in the Clinical Security Framework.

Direction 9: Searches of ward areas and other areas

Each provider in developing their local hospital policy on the searches of ward areas and other areas should have regard to the standards set out in the Clinical Security Framework.

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 to at least 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, searches should also be undertaken whenever a credible risk is identified.

Direction 10: Security of tools, equipment and materials

When issuing written instructions to members of staff, providers should have regard to the standards set out in the Clinical Security Framework regarding the control of tools, equipment and materials in secure areas of the hospital.

Direction 11: Searches of members of staff and key-holders

When developing the local policy for the searching of members of staff and key-holders, providers should have regard to the standards set out in the Clinical Security Framework.

What constitutes a rub-down search is contained in the guidance to Direction 5.

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 an Enhanced Disclosure Barring Service (DBS) check and completed the appropriate training detailed in Direction 43(2) can be key-holders.

Direction 12: Arrangements in respect of visitors and visiting children

What constitutes a rub-down search is contained in the guidance to Direction 5.

Bringing and sending food items into 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 into 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 and dietary requirements 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. 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 title 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 appropriate, even when staff of the same sex are available. For example, female staff searching male babies or infants. 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:

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

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

Providers must have regard to the standards set out in the Clinical Security Framework when developing their policies for the management of contractors and their property.

Direction 14: Supply of food by staff and key-holders to patients

In developing local policy and instructions to staff each provider must have regard to the standards set out in the Clinical Security Framework.

These restrictions are intended to prevent staff and key-holders in direct contact with patients being involved in bringing food into the hospital for consumption by patients. The security director’s authority detailed in paragraph (2) of this Direction may be given to groups of staff or key-holders 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 have regard to the standards set out in the Clinical Security Framework when developing policies for members of staff managing and escorting vehicles, including contractor’s vehicles within secure areas.

The Direction requires any vehicle to be checked before the vehicle enters or leaves the secure area, apart from an emergency services vehicle that is attending to an emergency. 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.

Whilst not a requirement set out within the Directions, it is good operational practice to ensure that vehicles are not normally 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.

Direction 16: Testing for illicit substances

The provider must in developing the local policy for the testing of illicit substances have regard to the standards set out in the Clinical Security Framework.

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 and the Clinical Security Framework.

Direction 18: Written or electronic records of certain searches and tests

The provider must ensure that written and electronic records as required in Direction 18 adhere to the standards set out in the Clinical Security Framework.

Direction 19: Security information

Providers must have regard to the standards set out in 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:

(a) security information relating to each patient; and

(b) other security information relating to the hospital.

Security records may comprise of written and electronic records and 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 security director in discharging their duties under Direction 19(4)(d) should ensure they consider any request for disclosing security records and hold the authority for sharing security information.

Direction 20: Patients' possessions

Providers must have regard to the standards set out in the Clinical Security Framework when developing policies for managing patients’ property.

Providers should also have regard to the following:

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

(b) 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 both the Clinical Security Framework and 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.

Although not a requirement of the Direction, it is good practice to ensure 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:

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

(b) 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;

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

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

(e) 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 may have access to electrical items that the clinical team, acting on advice from the security department, has agreed the patient may have.

Direction 21: Items delivered or brought to hospital premises for patients and Direction 25: Patients' incoming post

Providers should have regard to the standards set out in the Clinical Security Framework when developing policies for managing items delivered or brought to the hospital premises for patients.

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 multi-media devices, DVDs, videos or items in other formats intended for / or are capable of recording images are concerned, it is recommended that:

(a) Any item delivered or brought into the hospital premises should, on arrival in the hospital, be checked by an authorised member of staff to establish that it is what it is purported to be and then, subject to c) below, 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;

(b) No item should be passed to a patient if it has a classification of 18R;

(c) Patient’s access to information technology equipment should be controlled in accordance with Direction 22.

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, the Clinical Security Framework or the provider’s policy.

Direction 22: Patients’ access to information technology equipment and the internet

Providers must have in place policies for controlling patient’s access to, and use of, information technology equipment and the internet. Such policies must have regard to the standards set out in the Clinical Security Framework.

Policies should be underpinned by robust risk assessment to anticipate and mitigate risks associated with introducing rapidly developing technologies and their potential impact on the security of the hospital. These policies should be informed where necessary by independent expert advice.

'Direct supervision' 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).

A patient's access to information technology equipment in their room should only be allowed following risk assessment of the patient.

Direction 24: 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 28: 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 is not allowed into the secure area if they refuse to allow it to be opened and inspected.

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

(a) the reasons for withholding it;

(b) that they can request that the security director review the decision to withhold it; and

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

Direction 29: Mobile telephones

When developing local policies for the management of mobile telephones, the provider must have regard to the standards set out in the Clinical Security Framework. The routine authorisation of mobile telephones for staff use within the secure perimeter is not expected.

Patients are not allowed possession of, or access to mobile telephones within the secure area. Any patient access to a mobile telephone outside of the secure area, such as when on an extended medical leave of absence for compassionate reasons, should be risk assessed and recorded in the Leave of Absence Management Plan and be directly supervised by escorting staff and authorised by the security director.

Direction 30: Patients’ outgoing telephone calls

Providers must have regard to the standards set out in the Clinical Security Framework when developing policies for managing 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 31: Patients’ incoming telephone calls

Providers should have regard to the standards set out in the Clinical Security Framework when developing policies for managing 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 32: Security Risk Assessments

Providers must have regard to the standards set out in the Clinical Security Framework when developing policies for managing security risk assessments of patients.

Providers must ensure that when considering leave of absence for patients, including the preparation required in advance to facilitate an emergency medical leave of absence, the security risk assessment must be reflected in the leave of absence risk management plan for each individual patient and for each individual leave of absence episode.

Direction 35(2) Grounds Access requires that providers must include security arrangements and risk assessments in accordance with Direction 32 to enable a patient to be granted grounds access as part of a treatment plan.

Direction 33: 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) of this Direction it should record the reason for that decision.

Direction 34: Security at night

Each provider should have a policy on the circumstances in which a patient can be locked in their room at night.

There is a distinction between night-time confinement under these Directions and seclusion. Locking the room of a patient at night under Direction 34 is not the same as seclusion.

Paragraphs 26.103 to 26.149 of the Mental Health Act 1983 Code of Practice (‘the Code of Practice’) define seclusion and describe processes for its use.

By contrast, arrangements made by a hospital for patients’ rooms to be locked at night (referred to as night time confinement) refers to the pre-determined locking-in of patients, 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 in accordance with Direction 34. A risk assessment must be carried out under Direction 32 and a risk management plan prepared, which must include any decision (including a date on which the decision must be reviewed) to lock the room of a patient at night in accordance with Direction 34.

Longer-term segregation as described in paragraph 26.150 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 26.150 to 26.160 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 34) in their rooms at night.

Direction 35: Grounds Access

Grounds access is a positive activity that all patients may, following a security risk assessment, be granted by the provider's Grounds Access Committee in accordance with Direction 37 or the medical director in accordance with Direction 38.

A request for grounds access should be made by a member of the clinical team to the Grounds Access Committee and must only be refused if this will adversely affect the safety and security of patients, staff or visitors or the security of the hospital.

Further to the interpretation and definition of 'grounds access' within Direction 2, this does not include unescorted patient access into ward garden areas which are to be treated as part of the ward area if:

(a) the garden area is accessible from the patient's ward;

(b) the garden area is defined by a demarcation line which effectively separates it from adjacent areas; and

(c) access is approved by the patient's clinical team following individual documented risk assessment.

Direction 37: Functions of the Grounds Access Committee

The provider's policy for grounds access must ensure that if the Grounds Access Committee refuse a request for grounds access that the individual patient has the right to request, through their responsible clinician, a review of the decision in accordance with Direction 38.

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 total number, and the mix, of patients who should be permitted grounds access at any one time.

Direction 39: Leave of Absence

The provider must ensure that before a patient is granted leave of absence, or for planning the arrangements to facilitate an emergency medical leave of absence, the responsible clinician, having consulted the patient's clinical team produces a risk assessment in compliance with Direction 39.

When developing policies for the management of leave of absence, providers should ensure they have regard to any relevant Ministry of Justice guidance to responsible clinicians and any guidance within the Clinical Security Framework. They should also consider the following:

(a) 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;

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

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

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

Direction 40: Escorting patients

All staff including drivers involved in the escorting of patients must receive training as appropriate to their role and in accordance with the Clinical Security Framework.

When developing policies for members of staff on carrying out escorting duties, including the appropriate use of handcuffs, escorting chains and other mechanical restraints, providers must have regard to the standards set out in the Clinical Security Framework.

Direction 41: Security of keys and locks

When developing policies for members of staff and other key-holders on the security of keys and locks, providers must have regard to the standards set out in the Clinical Security Framework.

All key-holders will be subject to Enhanced DBS clearance.

Direction 43: Provision of training

All training should have due regard to the standards set out in the Clinical Security Framework.

5. General guidance on policies

5.1 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 standards set out in 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.

5.2 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 these needs. Providers should also ensure that these policies can only be changed with clearance at the highest management level.

5.3 When developing, reviewing, amending and implementing these policies providers should fulfil their responsibilities regarding human rights and equality outlined in paragraph 3.1 above.

5.4 Providers should ensure that each policy clearly states:

(a) the objective that it is intended to achieve;

(b) how that objective is to be achieved;

(c) the key staff group(s) to be involved in its implementation and operation;

(d) 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;

(e) how and when the policy will be reviewed; and

(f) who has lead responsibility for the policy.

5.5 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.

5.6 It is recommended that:

(a) each provider ensures that all patients are informed, where appropriate, of the content of policies that affect them. The Clinical Security Framework provides further instruction to providers on policy content that must be shared with patients as well as policies that must not be shared with patients;

(b) all hospital staff have access on request, or direct access, to the Clinical Security Framework;

(c) 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;

(d) the full policy documents are clear and concise. Staff should be required to know the contents of all relevant policies and have become familiar with them before working within the secure perimeter. They should be asked to confirm that they have read them and to re-confirm this regarding any changes made to them;

(e) 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;

(f) where staff are permitted to use discretion in the exercise of a policy, the reasons for exercising that discretion are recorded;

(g) 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.

5.7 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 security hospitals. However, it is accepted that there may be some variation in the approach of each provider to reflect their different local circumstances.

5.8 Where appropriate, NHS England and providers should consider whether common issues and policies across the hospitals should be addressed through amending and updating the Clinical Security Framework to ensure consistent best practice across all providers of high secure services.

5.9 NHS England must work with providers and through the Clinical Secure Practice Forum to regularly review and update the Clinical Security Framework to ensure it remains up to date with current best practice.

5.10 NHS England must maintain a robust governance framework for monitoring and updating the Clinical Security Framework with oversight from the National Oversight Group for High Secure Services.

6. Annex A: Risk assessments, the determination of ‘high risk’ and risk management plans

Protocol for:

(a) risk assessment and management (Direction 32);

(b) identification and management of ‘high risk’ patients in high security hospitals; and

(c) locking these patients in their rooms at night (Direction 34).

6.1 This protocol is designed to ensure that the public, patients and staff 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 32(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 34 and associated guidance.

6.2 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.

6.3 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 32(9)).

6.4 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 patients, consideration must be given to their capability of making appropriate decisions.

6.5 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 in the effective treatment of the patient’s mental disorder.

6.6 Below is a model protocol for risk assessments, the determination of ‘high risk’ (Direction 32) and the development of risk management plans including whether these should include locking patients in their rooms at night (Direction 34).

(a) A multi-disciplinary risk assessment must be undertaken and recorded to ensure that security risks are identified (see Direction 32). This risk assessment must be used to make a judgment as to whether the patient presents a ‘high risk’ in either of the two main categories:

(i) risk of escaping or absconding; and

(ii) risk of subverting safety and security, or organising action to subvert safety and security.

(b) A management plan for each identified risk should be agreed and documented by the multi-disciplinary team (see Direction 32(5) and **Attachment 2**).

(c) Review dates should be agreed and documented for each identified risk and its associated management plan (see Direction 32(8)). In some instances, the review frequency may be determined by the policies governing the specific interventions deployed (e.g. seclusion, close observation etc).

(d) 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 32(8)(a)).

(e) 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 32(7)).

(f) A decision tree has been designed to standardise the development of risk management plans for each identified risk (see **Attachment 1**).

(g) 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.

(h) 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 the security risks (see **Attachment 1**, and Box 1 in **Attachment 2**).

(i) 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 32(9)).

(j) 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.

(k) 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 34(2)).

(l) 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.

(m) 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.

7. Annex B: Protocol for locking non 'high risk' patients in their rooms at night

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 32)

7.1 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 34) where this is not part of a risk management plan to manage their ‘high risk’ (Direction 32), nor patients locked in their rooms as part of local seclusion policies.

7.2 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.

7.3 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 (7.5) & (7.6) below).

7.4 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 minimum three-monthly basis.

7.5 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.

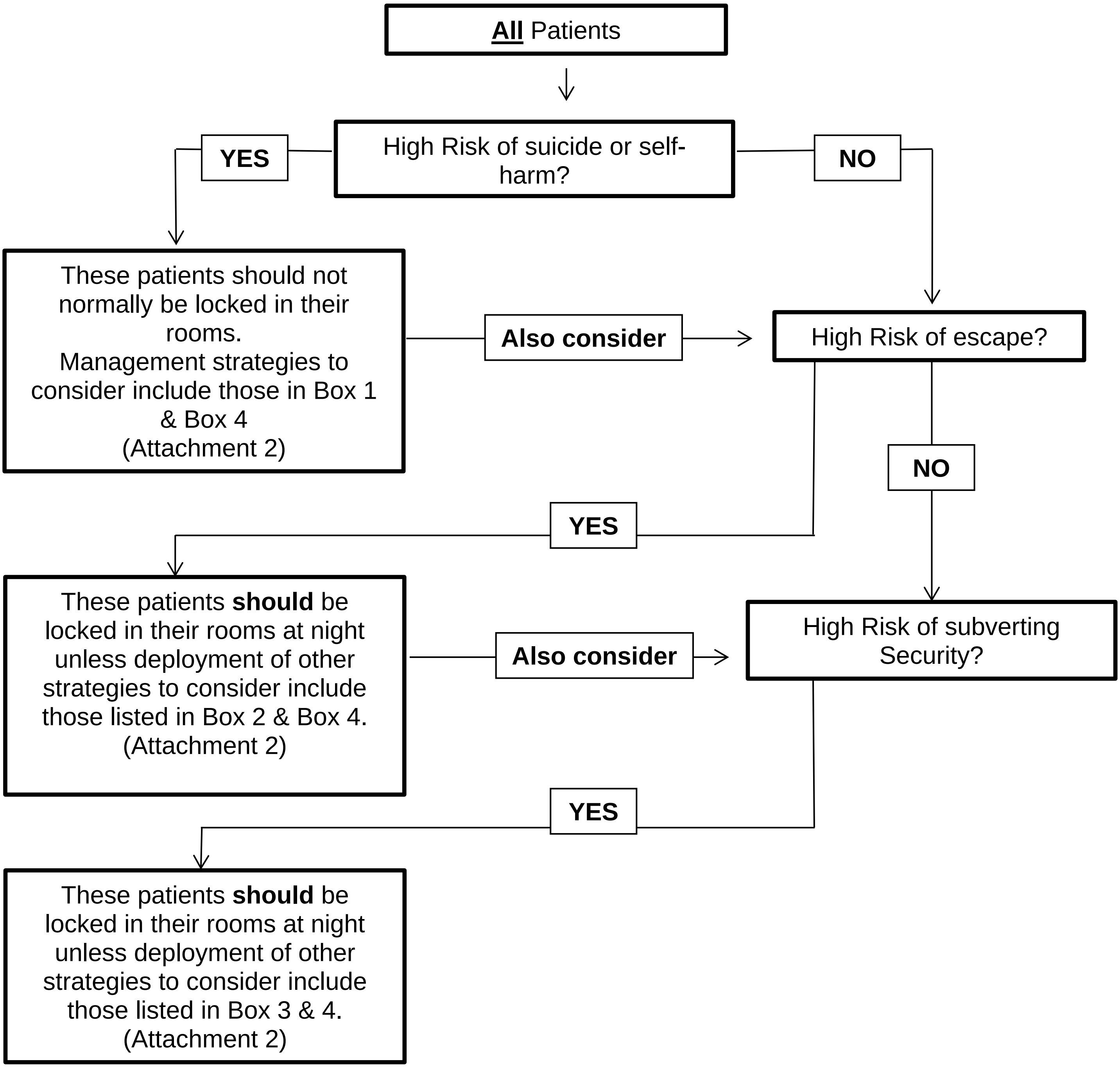
7.6 Arrangements, reflected in the provider policies, should also be made for reviewing decisions if there are circumstances, for example the risk of suicide or self-harm, which would indicate that locking the patient in their room at night might have a detrimental effect on their well-being or be unsafe.

7.7 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 34(2)).

7.8 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

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 in Box 1 & Box 4
(Attachment 2)

High Risk of escape?

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

High Risk of subverting Security?

These patients **should** be locked in their rooms at night unless deployment of other strategies to consider include those listed in Box 3 & 4.
(Attachment 2)

Attachment 2: Management strategies

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 Escape or Absconding

locking in 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 (refer to the provider's observation policy); [1]

enhanced restrictions on access to risk items;

enhanced search/drug screening procedures.[1]

Box 3

High Risk of Subverting Security

locking in 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 (refer to the provider’s observation policy); [1]

enhanced restrictions on access to risk items;

enhanced search/drug screening procedures.[1]

Box 4

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 may be necessary (see paragraphs (32) & (34) 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 6.6(l) **Annex A** & 7.8 of **Annex B***)*.

Published to GOV.UK in pdf format only.

Community and Social Care/Mental Health, Disability and Dementia/Mental Health Policy

www.gov.uk/dhsc