Brief guides are a learning resource for CQC inspectors. They provide information, references, links to professional guidance, legal requirements or recognised best practice guidance about particular topics in order to assist inspection teams. They do not provide guidance to registered persons about complying with any of the regulations made pursuant to s 20 of the Health and Social Care Act 2008 nor are they further indicators of assessment pursuant to s 46 of the Health and Social Care Act 2008.

Brief guide: the use of ‘blanket restrictions’ in mental health wards

Context and policy

The Mental Health Act Code of Practice defines blanket restrictions as “rules or policies that restrict a patient’s liberty and other rights, which are routinely applied to all patients, or to classes of patients, or within a service, without individual risk assessments to justify their application.” The Code’s default position is that “blanket restrictions should be avoided unless they can be justified as necessary and proportionate responses to risks identified for particular individuals”. The Code does allow that secure services will impose blanket restrictions on their patients.

Where blanket restrictions are identified as necessary and proportionate there should be a system in place which ensures these are reviewed within a regular time frame, with an overall aim at the reduction of restrictive practices.

Appendix 1 sets out normative expectations regarding blanket restrictions at different levels of security. It is only a guide. When making a specific judgement, inspectors must take account of factors specific to the unit/service. For example, it might be appropriate for staff on an acute admission ward to search all patients returning from leave, as a temporary measure, if drugs are coming onto the ward and staff suspect that patients are being coerced into bringing drugs in for others.

Appendix 2 lists of items that are likely to be prohibited or restricted on mental health wards. It also describes the principles of risk assessment and personalised care applied to restricted items.

Appendix 3 summarises the powers to monitor and intercept telephone calls and postal items in the High Security Hospitals

Evidence required

As well as checking that the provider has a policy on blanket restrictions that acknowledges the principle of least restriction, inspectors must establish whether the service can give a cogent account of why any blanket restriction is necessary and proportionate, and can demonstrate that:

- there is a systematic, regular review of any blanket restriction that is not an inherent part of the ward security;
• where the blanket restriction is an inherent part of the ward security, staff are permitted to consider relaxing it when it is inappropriate to the care of an individual patient and will not compromise the overall security of the service; and

• the ward takes a systemic approach to identify and challenge its practices that may amount to blanket restriction, with a view to ensuring that care and treatment is provided according to the principle of using the least restrictive option and maximising independence (Code of Practice, Chapter 1).

On wards where staff prohibit or restrict patients’ access to items, and especially to items that would not normally be prohibited or restricted, the service should have a set of auditable standards for:

• How items are identified and what risk assessment is required
• What information about the restrictions and reasons is provided to patients and visitors
• How adherence is monitored (training, monitoring, managing breaches)
• Arrangements for audit and review

**Reporting**

1. In the ‘assessing and managing risk to patients and staff’ section of ‘safe’ state what blanket restrictions are in place, whether any are unwarranted, and/or whether there is a systematic, regular review of any blanket restriction that is not an inherent part of the ward security.

2. Under ‘good governance’ in ‘well-led’ report on the quality of the provider’s oversight of its blanket restrictions and the support provided to staff to actively review and manage these. No form of blanket restriction should be implemented unless expressly authorised by the hospital managers on the basis of the organisation’s policy and subject to local accountability and governance arrangements (Code of Practice 8.9).

**Link to regulations**

The relevant regulations are regulation 13 and regulation 17.

Where CQC has evidence that the blanket restrictions in place are not necessary or proportionate as a response to the risk of harm posed to the service user or another individual this is likely to be a breach of regulation 13 (1) (4) (b) (c) and (5) .

Where CQC finds evidence that the blanket restrictions policy is not regularly reviewed, not authorised appropriately by the hospital managers and is not part of the provider’s governance arrangements then this is likely to breach regulation 17(1) (2) (a) and (b)
Appendix 1: Normative expectations regarding blanket restrictions at different levels of security

<table>
<thead>
<tr>
<th>Security level</th>
<th>General (acute)</th>
<th>PICU</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Banned items</strong></td>
<td>All services will have banned and restricted items: alcohol, weapons, illicit drugs (see appendix 2).</td>
<td>All services will have banned and restricted items in addition to those found in general (acute) ward policies (see appendix 2).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Random or routine searching</strong></td>
<td>Not without specific cause (see appendix 2)</td>
<td>Policy on searching should require clear rationale given on the purpose of any search.</td>
<td>Random searching likely, may be routine at times in response to specific issues</td>
<td>Routine searching likely, Pre-discharge recovery wards may have random searching.</td>
<td>Expected to be routine due to inherent risk of population.</td>
</tr>
<tr>
<td><strong>Access to mobile phones and the internet.</strong></td>
<td>Wards should provide personal access to the internet and mobile phones, particularly to communicate with friends and family. Restrictions on access should be individually justified and not be a blanket measure. Wards may provide non-camera phone handsets and arrange for safe charging of patients’ electronic items (electrical leads can be a ligature risk), e.g. with short-lead chargers or charging in the nursing office.</td>
<td>Some units are piloting access to mobile phones. Dependent on the risk profile of the patient group.</td>
<td>All access to internet likely to be supervised and restricted as part of ward security.</td>
<td>All access to internet will be supervised and restricted as part of ward security.</td>
<td></td>
</tr>
<tr>
<td><strong>Access to money</strong></td>
<td>Restrictions on access to money should be based upon individual risk assessment, and justifiable on grounds of best interests.</td>
<td>Restrictions on access to money will be part of security fabric of ward.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Buying takeaway food</strong></td>
<td>No restrictions</td>
<td>Restrictions on take away food may be in place to ensure that therapeutic activity of the ward environment is not undermined.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Food restrictions</strong></td>
<td>During inpatient care staff should review the physical health of the patient as well as the mental health. Advice and encouragement should be given to patients to have a healthy well balanced diet. Restrictions of access to certain food should not be part of this and can be viewed as a blanket restriction.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Smoke free</strong></td>
<td>NHSE have issued guidance on mental health units becoming smoke-free. This should be considered to be as a blanket restriction that is justifiable.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>incoming or outgoing mail</strong></td>
<td>Staff have no legal powers to interfere with postal items but may withhold outgoing post from a detained patient where addressee has requested that this be done (MHA s.134(1)(a)). Staff may ask patients to open mail in front of them if there are concerns over contraband items or the patient's likely reaction to mail. Staff should justify as necessary and proportionate to an identified risk. It should not amount to an interference with the postal item itself. Staff should not read patients' mail in such arrangements.</td>
<td></td>
<td></td>
<td></td>
<td>Security directions allow monitoring and interference with postal items (see appendix 3).</td>
</tr>
<tr>
<td><strong>Telephone monitoring</strong></td>
<td>No legal powers to monitor patients' telephone calls. Patients should expect privacy when using the telephone. In exceptional cases (e.g. when a patient makes nuisance or unwarranted emergency service calls) access to the telephone might be restricted.</td>
<td></td>
<td></td>
<td></td>
<td>Security directions allow monitoring of phone calls (see appendix 3).</td>
</tr>
</tbody>
</table>
Appendix 2: Prohibited and restricted items in mental health wards

Prohibited items
All mental health inpatient services have some prohibited or ‘contraband’ items. Inspectors should not challenge the enforcement of such prohibitions as a blanket restriction. The following are typically banned in all inpatient services:
- Alcohol and drugs or substances not prescribed (including illicit and legal highs)
- Items used as weapons (firearms- real or replica, knives or others sharps, bats)
- Fire hazard items (flammable liquids, matches, incense)
- Pornographic material
- Material that incites violence or racial/cultural/religious/gender hatred
- Clingfilm, foil, chewing gum, blue tack, plastic bags, rope, metal clothes hangers
- Laser pens
- Animals
- Equipment that can record moving or still images (camera, web cameras)

Although CQC encourages secure services to adopt the least restrictive approach to IT items commensurate with the security requirements of the unit, secure mental health units may also prohibit:
- Mobile phones (though may be allowed in some rehabilitation low secure units)
- Computers, tablets, games devices with hard drives or sharing capabilities
- Items with voice recording capabilities
- Other items with enabled WiFi/internet capabilities
- Items considered as an escape aid

Restricted items
Restricted items are items where the access is controlled and may be directed according to policy and individual risk assessment. Examples of items that may fall into this category include:
- Disposable cigarette lighters
- Toiletries- aerosols, razors
- Identity documents, bank cards, items of stationery
- Cutlery, tinned materials, glassware

Risk assessments and personalised care related to restricted items
Access to items will depend on many factors, some of which may be fixed and others subject to change. The risk assessment and ensuing management of access to security items should take a procedural and individualised approach, where possible in collaboration with the patient, which avoids the implementation of unreasoned blanket bans. For items that may be considered suitable only for restricted use, staff

---

1 This appendix is adapted from a paper ‘Developing a Security Item Assessment and Management Process: A Review of Prohibited, Restricted and Special Measures Items in Medium and Low Secure Services’, by Dr Catherine Marshall, Specialist Registrar in Forensic Psychiatry, East London NHS Foundation Trust.
should complete a thorough risk assessment and provide the patient with a transparent rationale that explains the management outcome. A dynamic and personalised risk assessment considers:

1. **Personal risk**: individual’s historical risk and current mental state
2. **Interpersonal risk**: direct risk to others- patients and staff
3. **Environmental risk**: ward dynamics; general service safety (level of security, rehabilitative/acute)
4. **A common sense consideration** of the item in question

Items can then be categorised:

**GREEN**- access to the item can be facilitated with a collaboratively formed care plan in place with the patient. A service may choose to have a standardised approach for the item which can then be adapted to the individual’s need.

**AMBER**- with the information provided and risk assessment completed so far, it is inconclusive whether access to the item can be safely facilitated. Refer the issue for further assessment and discussion to the MDT/ward round or security liaison nurse.

**RED**- personalised risk assessment has determined that access to the item cannot be safely facilitated. The patient is provided with an explanation for the restriction, and if applicable a timeframe for when the access can be reviewed.
Appendix 3: Powers to monitor and intercept telephone calls and postal items in the High Security Hospitals (HSH)

Withholding of mail

HSH managers have no authority to censor correspondence; i.e. to strike out any parts in a letter or other document. However, they may withhold items from packages whilst allowing the remainder to be delivered if any of the following criteria apply.

<table>
<thead>
<tr>
<th>Type of item</th>
<th>Criteria for withholding the item</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outgoing post</td>
<td>• The addressee has requested that post from the patient should be withheld; or</td>
</tr>
<tr>
<td></td>
<td>• the managers consider the item is likely to cause distress to the addressee or to any other person (not being on the staff of the hospital); or</td>
</tr>
<tr>
<td></td>
<td>• the managers consider the item is likely to cause danger to any person.</td>
</tr>
<tr>
<td>Incoming post</td>
<td>• In the interests of the safety of the patient; or</td>
</tr>
<tr>
<td></td>
<td>• for the protection of other persons³.</td>
</tr>
<tr>
<td>Other items delivered or brought to hospital premises for patients</td>
<td>The item:</td>
</tr>
<tr>
<td>(i.e. not postal packages)</td>
<td>• is one which the patient has asked to be withheld; or</td>
</tr>
<tr>
<td></td>
<td>• is likely to cause distress to the person to whom it is addressed or to any other person; or</td>
</tr>
<tr>
<td></td>
<td>• may cause a danger to any person; or</td>
</tr>
<tr>
<td></td>
<td>• may prejudice the safety of any person; or</td>
</tr>
<tr>
<td></td>
<td>• may prejudice security in the hospital⁴.</td>
</tr>
<tr>
<td>Internal post</td>
<td>• The recipient has asked for internal post from another patient to be withheld; or</td>
</tr>
<tr>
<td>(i.e. post between patients within the same hospital or from a patient to a member)</td>
<td>• it is likely in the opinion of the Trust to cause distress to any person (not being a member of staff); or</td>
</tr>
<tr>
<td></td>
<td>• it is likely in the opinion of the Trust to cause danger to any person; or</td>
</tr>
<tr>
<td></td>
<td>• it is necessary to do so in the interests of the safety of the patient or for the protection of any</td>
</tr>
</tbody>
</table>

² Mental Health Act 1983, s.134(1)
³ Mental Health Act 1983, s.134(2)
⁴ The High Security Psychiatric Services (Arrangements for Safety and Security at Ashworth, Broadmoor and Rampton Hospitals) Directions 2011, paragraph 22(3)
| of staff in the hospital where the patient is detained ⁵ | other person.⁶ |

⁵ The High Security Psychiatric Services (Arrangements for Safety and Security at Ashworth, Broadmoor and Rampton Hospitals) Directions 2011, paragraph 27(5)
⁶ The High Security Psychiatric Services (Arrangements for Safety and Security at Ashworth, Broadmoor and Rampton Hospitals) Directions 2011, paragraph 27(3)
If an item is addressed to or from any person or body identified in section 134(3) of the 1983 Act, the item may only be opened where it is necessary to confirm its destination or origin and must not be further inspected if the intended recipient or author is a person or body identified in that section. Section 134(3) includes a Minister of the Crown or member of either House of Parliament; any judge or officer of the Court of Protection; the Health Service Ombudsman; CQC; The Tribunal; PALs services; IMHA and IMCA services; hospital managers; a legally qualified person instructed by the patient to act as a legal adviser; and the European Commission or Court of Human Rights. Incoming items from these bodies or people may not be withheld. Outgoing items to these bodies or people may only be withheld if that person has requested that communication to him/her should be withheld. The persons or bodies include the Scottish, Welsh or Northern Ireland equivalents which may be relevant where patients have been admitted or transferred having been ordinarily resident in these relevant parts of the U.K.

If an item, or anything contained within it, is withheld (except where outgoing post has been withheld at the request of its intended recipient), within seven days the hospital managers are required to notify the patient. The notice should be given in writing. Except where the intended recipient of outgoing mail has requested that such mail should be withheld, the hospital must also notify the intended recipient in writing. This notification must also inform the patient (or intended recipient) of their right to request CQC to review the managers’ decision.

Monitoring of telephone conversations
Patients in high security hospitals may be subjected to telephone monitoring if a risk assessment concludes that:
• a patient presents a high risk of escaping or organising action to subvert safety and security; or
• there is a need to protect the safety and security of the patient or of others.

Telephone calls between a patient and any person or body identified in section 134(3) of the 1983 Act may not be monitored or recorded. Neither may any telephone call made to the Samaritans.

The patient can make an application for review of telephone monitoring to CQC in writing within 6 months of receiving the notification of the manager’s decision. CQC may accept applications by other means where this is in the interests of justice. The hospital managers should retain monitoring records for at least six months to enable proper determination of any application to review the monitoring.

For the full CQC policy on HSH interception of mail and telephones see:

---

7 This list is not exhaustive: see Mental Health Act 1983 s.134(3) for the full list.
8 Mental Health Act 1983 s.134(6). The duty to notify the person to whom an outgoing package was being sent only applies where the identity of that person is known.
9 Mental Health Act 1983 s.134(6)
10 The High Security Psychiatric Services (Arrangements for Safety and Security at Ashworth, Broadmoor and Rampton Hospitals) Directions 2011, paragraph 34(2), (3). See the discussion on withholding of mail above for main organisations included in the list at s.134(3).