



Department
of Health &
Social Care

The High Security Psychiatric Services (Arrangements for Safety and Security) Directions and associated guidance

A consultation on safety and security arrangements
in the high security psychiatric hospitals

May 2018

DH ID box
Title: A consultation on The High Security Psychiatric Services (Arrangements for Safety and Security) Directions and associated guidance
Author: Secure Services Policy Team, Mental Health and Disability
Document Purpose: Consultation
Publication date: May 2018
Target audience: High security psychiatric services providers Patient, users of services, families and their representatives High Security Commissioning Team, NHS England The medical Royal Colleges Third sector and voluntary organisations
Contact details: Secure Services Policy Team Mental Health and Disability Quarry House Leeds LS2 7UE Email address: HSHConsultation@dh.gsi.gov.uk

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

© Crown copyright

Published to gov.uk, in PDF format only.

www.gov.uk/dhsc

The High Security Psychiatric Services (Arrangements for Safety and Security) Directions and associated guidance

A consultation on safety and security arrangements in the high security psychiatric hospitals

Contents

1. Executive summary.....	5
2. Introduction.....	6
3. Summary of proposed changes to the Directions.....	8
4. Equalities analysis.....	15
5. Summary of the questions.....	16
Questions which relate to the hospitals.....	16
Questions which relate to patients.....	16
Questions which relate to staff.....	16
Questions which relate to specific Directions.....	16
General questions.....	17
6. How to respond to this consultation.....	18
Consultation principles.....	18
Comments on the consultation process itself.....	18
Confidentiality of information.....	18
Summary of consultation.....	19

1. Executive summary

- 1.1. The safety and security arrangements for the three high security psychiatric hospitals in England (Ashworth, Broadmoor and Rampton) are set out in the High Security Psychiatric Services (Arrangements for Safety and Security) Directions 2013¹ (hereafter referred to as “the Directions”), and associated guidance.
- 1.2. The Directions and guidance, together with NHS England’s Clinical Security Framework, set out the minimum required standards of safety and security in the high security hospitals. This includes both the physical environment and the operational practice of staff. The Directions do not relate directly to the therapeutic aspects of the hospitals’ work, but they contribute to the provision of a safe environment for patients and staff, and thereby enhance the therapeutic activities of the hospitals.
- 1.3. The Directions and associated guidance were first introduced in 2000 following a Government commissioned review into safety and security practices within the high security hospitals by Sir Richard Tilt (Tilt Review). Since then, the Directions have been reviewed periodically with the current version being published in 2013.
- 1.4. This latest review of the Directions aims to:
 - Promote and protect the rights of patients;
 - Protect the safety of patients, staff and visitors, recognising the important role of the Directions in maintaining high standards of security;
 - Ensure the Directions remain fit for purpose given advances in technology and best practice since they were introduced in 2000;
 - Give the hospitals more flexibility to determine how they put the principles set out in the Directions into practice through the implementation of local safety and security policies; and
 - Ensure that safety and security policies are consistent across the three hospitals.
- 1.5. The Government is consulting on proposed changes to the Directions (any changes to the Directions will be reflected in the associated guidance). These changes have been developed in full partnership with the three high security hospitals, following a comprehensive review of the existing arrangements, which included significant stakeholder involvement.
- 1.6. This consultation provides those responding with the opportunity to provide their views on the proposed revisions. In particular views are welcomed on:
 - Whether the changes will have a positive or negative impact on patients’ daily activities and routines;
 - Whether the changes will have a positive or negative impact on staff working within the hospital;
 - Whether the changes maintain the same standards of safety and security.
- 1.7. Following analysis of the consultation responses, a formal consultation response will be published on the www.gov.uk/dh website.

¹ <https://www.gov.uk/government/publications/high-security-psychiatric-services-directions>

2. Introduction

- 2.1 High security psychiatric services assess and treat individuals with a mental disorder or neuro-development disorder who are detained under the Mental Health Act 1983 and whose risk of harm to others and risk of escape from hospital cannot be managed safely within other mental health settings. Most patients in high security psychiatric services will have had contact with the criminal justice system and will have been transferred from prison or directly from court.
- 2.2 The three high security hospitals each have in place a range of physical, procedural and relational security measures to ensure effective treatment and care whilst providing for the safety of the individual and others.
- 2.3 The High Security Psychiatric Services (Arrangements for Safety and Security) Directions 2013 (hereafter referred to as “the Directions”) and their associated guidance, together with NHS England’s Clinical Security Framework are intended to provide a framework to establish and regulate robust safety and security arrangements in high security psychiatric services. These arrangements should strike the right balance between not being unnecessarily restrictive for patients and enabling effective management of risk. The framework will allow NHS England (as the commissioner of high security psychiatric services) and the Care Quality Commission (as their regulator) to monitor and assure security and safety arrangements.
- 2.4 The Secretary of State for Health and Social Care (SofS) has powers of direction and oversight in relation to high security psychiatric services. Section 4 of the NHS Act 2006 provides that:
 - NHS England must arrange for the provision of high security psychiatric services;
 - The Secretary of State must approve providers of high security psychiatric services before those services can be provided;
 - The Secretary of State may give directions to providers in relation to their provision of high security services; and
 - The Secretary of State may give directions to NHS England about the exercise of their functions in relation to high security services.
- 2.5 The SofS has issued the following Directions to NHS England and the three high security hospitals:
 - High Security Psychiatric Services (Arrangements for Safety and Security) Directions 2013;
 - High Security Psychiatric Services (Arrangements for Visits by Children) Directions 2013; and
 - High Security Psychiatric Services (National Health Service Commissioning Board) Directions 2013.
- 2.6 The Safety and Security Directions set out the arrangements required by the high security hospitals with regard to ‘relational security’ (interaction between staff and patients), ‘procedural security’ (process and arrangements around security protocols), and ‘physical security’ (locks, keys, perimeter fence/wall). The Directions do not relate to clinical procedures or treatment provided to patients.

- 2.7 The Clinical Security Framework was developed in 2009 to replace the Manual of High Secure Practice which was drawn up in response to the recommendations of the Tilt Review. The Clinical Security Framework sets out in more detail how each of the Directions should be implemented to provide a consistent approach across the three hospitals where procedures should be the same. There will be some procedures which differ because of differing services being provided. This document is not published as it contains sensitive information relating to security procedures at the high security hospitals.
- 2.8 Following a series of serious security concerns in the high security hospitals in the late 1990s, the Government commissioned Sir Richard Tilt to undertake a review of security practices at the hospitals and make recommendations (the 'Tilt Review'). The Government accepted all of the recommendations of the Tilt Review and revised the arrangements required at the high security hospital for safety and security through the Safety and Security Directions, published in 2000.
- 2.9 The high security hospitals are assessed and held to account (by the Department of Health and Social Care, NHS England and the National Oversight Group for the High Secure Hospitals) against their compliance with the Directions along with the Mental Health Act 1983 and the Mental Health Act Code of Practice 2015. This is relevant for Care Quality Commission inspections, the annual prison service audits of each hospital and the reauthorisation of service providers.
- 2.10 Although there have been periodic reviews of the Directions, the most recent to include arrangements for locking patients in their room at night, this is the first full review of the Directions and guidance since they were introduced.
- 2.11 Following agreement by Department of Health and Social Care Ministers, the review was undertaken in 2015, by the Independent Clinical Advisor to the National Oversight Group for the High Secure Hospitals. The review group comprised clinicians and Security Directors at the high security hospitals, the Independent Security Advisor to the high secure hospitals' National Oversight Group, the commissioning lead for high secure services at NHS England, and officials at the Ministry of Justice (HM Prison and Probation Service).
- 2.12 The Directions were introduced at a moment in time when there were significant failures in safety and security at the high security hospitals but changes in context since that time mean they no longer need to be as restrictive. The review group considered wide ranging changes to the Directions, but recognised that the Directions remained a positive tool for ensuring safety and security and so didn't recommend substantial changes. The review group recognised that the Directions need to evolve to meet developments in best practice and to embrace new technology, for example, advances in digital and wireless technology for the benefits of staff and patients. Those changes are reflected in the revised Directions which are the subject of this consultation.
- 2.13 All consultation responses will be analysed and considered by the review group who will decide whether further revisions to the Directions and associated guidance are needed. A formal response to the consultation will be published on the www.gov.uk/dh website. It is envisaged that the revised Directions and associated guidance will come into force from summer 2019.

3. Summary of proposed changes to Directions and associated Guidance

- 3.1 This section sets out the proposed changes to the Directions and provides the rationale for those changes. Changes to the associated guidance will also be made to ensure consistency with the revised Directions themselves.
- 3.2 Directions which are not listed have not been changed as part of these revisions to the Directions. The regulations issued by the Care Quality Commission (CQC) in relation to these Directions have also not been changed. The CQC regulations will require amendment as a consequence of the revised final version of the Directions.

Interpretation (Direction 2)

- 3.3 This Direction provides definitions for some of the terms used in the Directions.
- 3.4 We have introduced a specific definition of “escape” to the Directions. This is to support the new Direction 44, which defines the secure perimeter as the boundary outside which a patient may be considered to have escaped.
- 3.5 The definition of “chief executive” has been updated to make it clear it applies to both NHS Trusts and NHS Foundation Trusts.
- 3.6 The definition of an illicit substance has been updated to include psychoactive substances to keep pace with current legislation.

Promotion of safety and security (Direction 3)

- 3.7 This Direction sets out the current guidance that the high security hospitals must comply with, in the running their services. It also details the organisations that must be informed if the high security hospitals are not compliant with that guidance.
- 3.8 Direction 3 (2) Promotion of safety and security introduces a new requirement that providers of high security services must have regard to the Clinical Security Framework in exercising their functions. This new requirement has been introduced to increase the flexibility of the high security hospitals to implement security policies and procedures locally, whilst ensuring a consistent approach across the three high security hospitals.
- 3.9 Direction 3 (3) - Promotion of safety and security introduces a new requirement for providers of high security services to report any derogation from the Clinical Security Framework to NHS England, the NHS Trust Development Authority and Monitor (NHS Trust Development Authority and Monitor function under the operating name of NHS Improvement). This is in addition to existing requirements to report any derogation from any guidance issued by SofS. This Direction also introduces a new requirement for providers of high security services to report (to the organisations above) the action being taken to return to compliance with any guidance issued by the SofS or the Clinical Security Framework.

3.10 These changes put in place more robust arrangements for reporting and monitoring when a service provider is not fully complying with the Directions and relevant guidance.

Rub downs, and searches of patients and their rooms and lockers (Directions 5-13)

- 3.11 Directions 5 to 13 set out the processes which are to be followed for different types of security searches. This covers the searching of patients, their rooms and lockers, ward areas, staff members, and visitors. The Directions state when a search must / or may be undertaken and by who.
- 3.12 Direction 5 (14) Requirements for conducting a rub-down search of a patient has been reworded to clarify that a patient may be subject to a rub-down search where they may not have consented if a member of staff has “reasonable grounds” for believing the patient possesses an item which poses an immediate risk to the patient or the safety of another patient. Where a decision is referred to the Medical Director to authorise a rub-down search, the Direction has now been revised to include “the security of the hospital” as one of the considerations they must take into account.
- 3.13 The changes clarify and provide a tangible reason for the exception on “reasonable grounds”, which also increases the protection of patients’ rights.
- 3.14 It was also important to include “the security of the hospital” as a consideration when authorising a rub-down search to ensure the overall safety of patients, staff and visitors and not compromise the security of the hospital by allowing the entry of a dangerous item into the secure hospital environment.
- 3.15 Direction 6(18) Searches of patients that involve the removal of clothing other than outer clothing has been reworded to clarify that a patient may be subject to a search involving the removal of clothing where they have not consented if a member of staff has “reasonable grounds” for believing that patient possesses an item which poses an immediate risk to the patient or the safety of another patient. See Direction 5 (15) for the rationale.
- 3.16 Direction 7, Searches of patients, rooms and lockers, the Direction has been simplified to provide greater flexibility to the hospitals to conduct searches at critical points determined by and in line with the Clinical Security Framework. The revised direction places the emphasis on “reliable intelligence” for exceptional searches of patients’ rooms and lockers.
- 3.17 The revision will allow a consistent approach across the three hospitals which will be set out in the Clinical Security Framework.
- 3.18 Direction 8, Searches when patients move around in the secure area, the Direction has also been simplified to provide greater flexibility to the hospitals whilst still setting out minimum requirements in the Clinical Security Framework. Again, this will allow a consistent approach across the three hospitals.
- 3.19 Direction 9, Searches of ward areas and other areas, (a) has been reworded to clarify that searches of ward areas must be conducted “**at least once a week**” and (b) has been reworded to clarify that searches of other areas must be conducted “**at least once every three months**”.

- 3.20 Direction 11, (c) Searches of members of staff, has been reworded to clarify that any items “in the possession of staff” are x-rayed and physically inspected prior to entry into the secure area when they are subject to a random search.
- 3.21 Direction 12 (3), Arrangements in respect of visitors and visiting children, has been reworded to clarify that tobacco is not allowed on site to reflect that the high security hospitals are smoke free environments.
- 3.22 Direction 12 (9) has been reworded to clarify that a “child arrangements order” must be made under Section 10 of the Children Act 1989 (as amended by the Children and Families Act 2014) to permit a visiting child access to the secure area. This is to ensure that current legislation is referenced within the Directions.

Supply of food by staff to patients (Direction 14)

- 3.23 This Direction sets out the arrangements for the supply of food by staff to patients and who can authorise this.
- 3.24 Direction 14(1) clarifies that “no member of staff” may bring food into the secure area for the consumption by a patient unless authorised to do so.
- 3.25 Direction 14(2) now states it is the Security Director rather than the Chief Executive that can authorise a staff member to bring food to a patient. The revision sets out that any staff member may now be authorised, previously this was restricted to catering staff and porters. These changes are intended to improve decision making, for example when food is being used for therapeutic purposes.

Checks of vehicles (was Directions 15 and 16 now Direction 15)

- 3.26 This Direction sets out that each hospital must have a policy for vehicle checks entering and leaving the secure area.
- 3.27 Directions 15 and 16 have been revised and combined to give greater flexibility to the hospitals to determine local policies and procedures for vehicle checks whilst in-line with the Clinical Security Framework.

Control of prescribed drugs (Direction 17(2)(a))

- 3.28 This Direction details the instructions that each hospital must provide to its staff which sets out processes for transporting, storing, and the distribution of prescribed drugs.
- 3.29 This has been reworded to ensure policies are expanded to include the transportation of drugs between the pharmacy and “ward area”, the current Direction simply states “ward”. The revision ensures that all relevant parts of the ward are covered by the policy.

Written records of certain searches and tests (Direction 18)

- 3.30 This Direction details which searches and tests a written or electronic record must be kept for e.g. searches of possessions and testing for illicit substances.
- 3.31 This has been reworded to clarify that records of certain searches and tests may be kept in “written or electronic” form, this allows the hospitals to now also keep electronic records.

Security information (Directions 19(1) and (2))

- 3.32 This Direction sets out the arrangements for gathering information on maintenance and security. This covers what types of security information, who the information should be shared with, and ensures that staff are made aware of what must be reported.
- 3.33 This Direction has been reworded to clarify that records may include “written or electronic” security records. This change takes into account that the hospitals each have sophisticated processes for gathering security information and this enables them to be flexible in their implementation.

Patients’ possessions (Direction 20)

- 3.34 This Direction details the arrangements for storing patient’s personal possessions, when patients can access their possessions, when access may be refused, and the timeframes for doing so.
- 3.35 This has been revised to give hospitals more flexibility to develop policies for patients' possessions, with the "aim" to provide patients with timely access to their possessions. This removes the specified time limits in the current Direction, which due to logistical challenges was often unachievable.

Items delivered or brought to hospital premises for patients (Direction 21(6))

- 3.36 This Direction sets out what will happen to any items brought to the hospital for a patient. This includes the processes of examination and the reason why the item may be withheld from the patient.
- 3.37 The Direction has been reworded to clarify that it does not apply to incoming postal packets addressed to a patient”. Directions 25 and 27 set out the arrangements for patient’s incoming post and internal post respectively.

Patients' access to computer equipment and games consoles (Direction 22)

- 3.38 This Direction has been retitled Patients’ access to computer equipment, games consoles and other digital and communications technology. The Direction sets out that each hospital must have a policy for the control of patient’s access to computer equipment and games consoles. It details the processes by which access may be granted, for example, following a thorough risk assessment, and how the use of such equipment will be monitored. The Direction also places restrictions on what patients can and cannot have access to.
- 3.39 It has been revised and extended to set out how risks associated with computer equipment, games consoles and other digital and communication technology must be mitigated, but also to give greater flexibility to the hospitals to develop local policies which balance such security risks with the need to give patients access to modern technology to improve their lives, and to enable the hospitals to use new technologies. The intention is to enable the hospitals to keep pace with technological developments and for patients to access new technologies where they have been robustly risk assessed and authorised by the hospital.

Internal post (Direction 27(5)(b))

3.40 This Direction states that there must be a policy for inspecting and if required withholding internal post. This will set out who can open and inspect the post, and that reasons for withholding any post must be clearly recorded.

3.41 This Direction has been revised to clarify that it relates to internal post “between patients and staff of the hospital where the patient is detained.” This revision simply ensures consistency of terminology between the Direction and associated guidance.

Mobile telephones (Direction 29)

3.42 The Direction states that patients are not allowed mobile telephones in the hospitals. Staff and contractors may be allowed a mobile telephone in the secure area if it has been authorised by the Security Director.

3.43 The Direction has been revised to enable the Security Director to authorise possession of a mobile phone by members of staff in the secure environment. The current direction only allows the Security Director to use discretion in exceptional circumstances. The revised Direction recognises that the three hospitals have different policies for certain members of staff. The Direction also allows contractors to carry a mobile telephone with the approval of the Security Director.

Security risk assessments (Direction 32)

3.44 This Direction ensures that the hospitals have a policy for risk assessments of patients. It sets out when the assessment should be undertaken, by whom, and what the assessment must include. It also provides details of the risk management plan which must be drawn up and under what circumstances it should be reviewed.

3.45 The scope of the Direction has been revised to focus only on security risks. This means security risk assessments will not include other risks related to a patient’s clinical presentation such as risk of harming others, suicide or being assaulted which are addressed through other clinical risk assessments.

3.46 Direction 32 (8)(d) has been added to make the link between risk assessments and leave of absence clearer, and to improve the robustness of processes.

3.47 Direction 32 (9)(a) has been reworded to focus only on security risks. These changes make the purpose of the high risk register clearer in that they relate to security risks and not clinical risks.

Grounds Access (Direction 35) and Grounds Access Committee (Direction 36)

3.48 Direction 35 sets out that a patient must have grounds access, and this must be risk assessed, and granted by the Grounds Access Committee. Direction 36 states that each hospital must operate a Grounds Access Committee and who it will be chaired by.

3.49 These Directions have been redrafted to strengthen the rights of patients to have access to outdoor spaces and fresh air as part of a treatment plan, which is subject to agreement by the Grounds Access Committee. The current Directions are worded that the hospitals should ensure that “patients are not granted grounds access” unless by permission of the

Committee. The revised direction makes it clear that every patient should be eligible for grounds access as part of a treatment plan.

Functions of the Grounds Access Committee (Direction 37(5))

- 3.50 This Direction sets out details of the grounds access requests which the committee must consider, and on what basis they may refuse a request.
- 3.51 The new **37(5)** has been added so that the hospitals are required to put in place a policy to enable patients to request a review of decisions made by the Grounds Access Committee. This strengthens patients' rights as the current Direction only allows appeals to be made by the clinical team on the patient's behalf.

Review of decision of the Grounds Access Committee (Direction 38(2)(a))

- 3.52 This Direction sets out that the Medical Director can review a decision made by the Grounds Access Committee where it feels that this would impede the patient's treatment.
- 3.53 The new **38(2)(a)** has been added to require the Medical Director to take account of the views of the Security Director in reviewing a decision made by the Grounds Access Committee, this ensures consistency of approach to safety and security across the Directions.

Leave of absence (Direction 39)

- 3.54 The Direction states that before a patient is given leave of absence, the responsible clinician must produce a risk assessment, and the patient's clinical team must produce a management plan which the Security Director must approve.
- 3.55 This now states at paragraph 1(a) that the responsible clinician, having consulted the patient's clinical team, must produce a risk assessment that complies with Direction 32 (security risk assessments) to make this link between leave of absence and security risk clearer.

Security audits (Direction 42)

- 3.56 The Direction has been reworded to reference the "High Security Psychiatric Services (National Health Service Commissioning Board) Directions 2013" which sets out requirements for annual and "any other assessment" of compliance with the Directions and other relevant guidance.

Provision of training (Direction 43)

- 3.57 This Direction sets out that each hospital should have a policy for regular staff training in safety and security. It sets out who should receive the training and what it should cover.
- 3.58 This has been amended to ensure that providers of high security services have arrangements in place for providing training it considers appropriate on a regular basis to staff and any person who may be allocated keys at the hospital. The intention is to give the hospitals greater flexibility in developing local policies for training with a need for training programmes to be regularly updated. It also widens the scope of staff who are considered to be eligible for the training.

Perimeter security (Direction 44)

3.59 This is a new Direction, it sets out that each hospital provider must now implement perimeter security arrangements with the aim of, as far as is practically possible, preventing an escape by a patient.

Other directions

3.60 The following Directions have also all been revised to give hospitals more flexibility with certain arrangements for each to be set out in local policies and through the Clinical Security Framework:

- **Monitoring telephone calls (direction 34)**
- **Escorting patients (direction 41)**

4. Equalities Analysis

- 4.1 The Department of Health and Social Care is subject to the Equality Act 2010, and specifically, the Public Sector Equality Duty.
- 4.2 As part of this consultation we would welcome your views on whether you believe anything set out in this document might have a beneficial or adverse impact on any equality issue; in particular, on the protected characteristics as defined in Section 149 of the Equality Act 2010.
- 4.3 The Duty covers the following protected characteristics:
- Age;
 - Disability;
 - Gender reassignment;
 - Marriage and civil partnership;
 - Pregnancy and maternity;
 - Race (includes ethnic or national origins, colour or nationality);
 - Religion or belief (includes lack of belief);
 - Sex;
 - Sexual orientation.
- 4.4 There are three parts to the Duty and public bodies must, in exercising their functions, have due regard to them all. They are:
- The need to eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under the Equality Act 2010;
 - Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;
 - Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.
- 4.5 In light of the revisions to the Directions and if necessary due to the outcome of this consultation, we will undertake an analysis of equality issues in line with the Secretary of State's duties under the Public Sector Equality Duty.

5. Summary of Questions

- 5.1 The questions below seek views on the proposed changes to the High Security Psychiatric Services (Arrangements for Safety and Security) Directions. Any changes made to the Directions will also be reflected in the associated guidance.
- 5.2 The question responses are either Yes or No, or multiple choice; there is also the opportunity to provide further comments to support your answers.
- 5.3 All responses will be analysed and used to inform the final version of the Directions and associated guidance.

Questions which relate to the hospitals

- 5.4 Do you think the proposed changes to the Directions provide the hospitals with sufficient flexibility and autonomy to make appropriate decisions, while ensuring adherence to best practice and common standards?
Yes / No / Not sure - If No or Not sure, please give your reason(s) why

Questions which relate to patients

- 5.5 Do you think the proposed changes to the Directions and associated guidance promote the rights of patients, for example through improved access to technology and grounds access?
Yes / No / Not sure – If No or Not sure, please give your reason(s) why
- 5.6 Do you think the proposed changes to the Directions and associated guidance will have a positive or negative impact on patient's daily activities and routines?
Positive / Negative / I'm not sure - If you would like to, please give your reason(s) why
- 5.7 Do you agree that the changes to the Directions and associated guidance will continue to protect patient's safety and security within the high security hospitals?
Yes I agree / No I don't agree / I'm not sure - If you would like to, please give your reason(s) why

Questions which relate to staff

- 5.8 Do you think the proposed changes to the Directions and associated guidance will have a positive or negative impact on staff working within the hospitals?
Positive / Negative / I'm not sure - If you would like to, please give your reason(s) why
- 5.9 Do you agree that the proposed changes to the Directions and associated guidance will continue to protect staff safety and security within the high secure hospitals?
Yes I agree / No I don't agree / I'm not sure - If you would like to, please give your reason(s) why

Questions which relate to specific Directions

- 5.10 Do you agree that the proposed changes to Direction 3(3) will ensure more robust arrangements for reporting and monitoring when a service provider is not fully complying with the Directions and relevant guidance?
Yes I agree / No I don't agree / I'm not sure - If you would like to, please give your reason(s) why

- 5.11 Do you agree that the proposed changes to Direction 5(15) and 6(19) will ensure staff must have good reasons for conducting a rub-down search, or search which removes clothing without the consent of the patient?
Yes I agree / No I don't agree / I'm not sure - If you would like to, please give your reason(s) why
- 5.12 Do the proposed changes to Direction 9 make it clear how often searches of ward areas and other areas should occur?
Yes / No / Not sure – If No or Not sure, please give your reason(s) why
- 5.13 Do you agree that the proposed changes to Direction 22 will allow the high security hospitals to keep pace with technological developments in electronic media for the benefit of patients?
Yes I agree / No I don't agree / I'm not sure - If you would like to, please give your reason(s) why
- 5.14 Do you agree that the proposed changes to Directions 35 and 36 will strengthen the rights of patients and ensure that every patient is eligible for grounds access as part of their treatment plan?
Yes I agree / No I don't agree / I'm not sure - If you would like to, please give your reason(s) why
- 5.15 Do you agree that the addition of Direction 37(5) strengthens the rights of patients by allowing them to appeal a Grounds Access Committee decision themselves?
Yes I agree / No I don't agree / I'm not sure - If you would like to, please give your reason(s) why

General questions

- 5.16 Do you agree that the proposed changes to the Directions and associated guidance will continue to protect visitor's safety and security within the high security hospitals?
Yes I agree / No I don't agree / I'm not sure - If you would like to, please give your reason(s) why
- 5.17 Do you have any comments on any of the other specific Directions or as a whole?
Yes / No – If Yes, please provide your comment(s) below
- 5.18 If you answered No / No I don't agree / I'm not sure / or Negative to any of the questions, what more could be done to improve things?

6. How to respond to this consultation

- 6.1 This consultation begins on the Thursday 31st May and will close on the Thursday 23rd August 2018.
- 6.2 It will help us to better analyse the responses if respondents complete the online consultation response document, which can be found at:
<https://consultations.dh.gov.uk/high-security-hospitals/hsp-Directions>
- 6.3 Or you can contact us via: HSHConsultation@dh.gsi.gov.uk

Consultation principles

- 6.4 General consultation principles can be found on the Cabinet Office's website at:
<https://www.gov.uk/government/publications/consultation-principles-guidance>
- 6.5 The principles inform Government departments of the considerations that should be made during a consultation. These include consideration of subjects of consultations, the timing and duration of a consultation, making information useful and accessible, and transparency and feedback.

Comments on the consultation process itself

- 6.6 If you have any concerns or comments which you would like to make relating specifically to the consultation process itself please contact:
- 6.7 Consultation Coordinator
Department of Health and Social Care
2 South Quarry House
Leeds
LS2 7UE
- 6.8 Or e-mail: consultations.co-ordinator@dh.gsi.gov.uk
- 6.9 Please do not send consultation responses to this address.

Confidentiality of information

- 6.10 We manage the information you provide in response to this consultation in accordance with the Department of Health and Social Care's Information Charter.
- 6.11 Information we receive, including personal information, may be published or disclosed in accordance with the access to information regimes (primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004).
- 6.12 If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality

disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

6.13 The Department will process your personal data in accordance with the DPA and in most circumstances this will mean that your personal data will not be disclosed to third parties.

Summary of the consultation

6.14 A summary of the responses to this consultation will be made available before or alongside any further action, and will be placed on the www.gov.uk/dh website.