FORENSIC CCQI
QUALITY NETWORK FOR FORENSIC MENTAL HEALTH SERVICES

RC PSYCH
ROYAL COLLEGE OF PSYCHIATRISTS

Physical Security in Secure Care

Quality Network for Forensic Mental Health Services

Publication number: CCQI 350

Editors: Megan Georgiou, Patrick Neville, Jemini Jethwa and Kate Townsend

To be completed by the service:	
Issue number:	
Issue date:	
Review date:	

This publication is available at: www.qnfmhs.co.uk

Any enquiries relating to this publication should be sent to us at: forensics@rcpsych.ac.uk

Artwork displayed on the front cover of the report:

Untitled, River House, South London and Maudsley NHS Foundation Trust.

Contents

Physical security in secure care

Introduction

Physical security has been a central feature of the Quality Network for Forensic Mental Health Services' standards since they were first published for medium secure services in 2007. They have developed over the years and now also encompass low security. They were formulated in accordance with the Environmental Design Guide Adult Medium Secure Services (Department of Health, 2011).

Physical security has been defined as:

> *"...the provision, maintenance and correct application of appropriate equipment and technology by appropriately trained staff. It is important but should not be the sole element of security provided. The security provided should be such as to protect the privacy and dignity of patients, to prevent others passing contraband items and to make escape difficult."* (Department of Health, 2007)

Three levels of security exist across adult secure inpatient services:

- High secure services provide care and treatment to those adults who present a grave and immediate risk to the public and who must not be able to escape from hospital
- Medium secure services provide care and treatment to those adults who present a serious risk of harm to others and whose escape from hospital must be prevented
- Low secure services provide care and treatment who present a significant risk of harm to others and whose escape from hospital must be impeded (NHS England, 2018)[1]

Physical security is just one domain of security within secure services; it works interdependently with procedural (timely, correct and consistent application of effective operational procedures and policies) and relational security (the understanding and use of knowledge about individual patients, the environment and population dynamic). It is essential that all three domains are embedded into service delivery, decision-making and practice.

During the consultation process for the third edition of low and medium secure standards (2019), we received feedback that these standards would be more useful in a physical security document that can be adapted locally.

[1] Please note, this document refers to guidance from NHS England. If your service is situated outside of England, please refer to guidance and commissioning arrangements relevant to your national or geographical location (e.g. NHS Wales, NHS Scotland, Health Service Executive, Health and Social Care Northern Ireland).

The following document has been devised using the physical security standards as a framework. It should be utilised as a 'live' document that is subject to continual review. Some elements are mandatory for all services; however, each area provides you with the opportunity to define how this practice occurs locally.

What is the purpose of this tool?

The purpose of the physical security document is to clearly describe the features of physical security within your service.

The aim of this tool has been defined as the following:

- To act as a standardised tool that can be adapted locally to manage physical security
- To be used as an assessment and compliance tool
- To provide a consistent process of assurance
- To aid training for staff in physical security

It is important to note that all staff have a responsibility to ensure the principles of recovery are maintained and a caring and therapeutic environment is promoted, despite the secure nature of the service.

How to use this document

- Standards are denoted by **navy blue, boldened text** and can be found in each section;
- Complete each of the sections by clearly detailing the practices and procedures in place at your service that relate to the particular standard being requested;
- Detail how each of the items apply locally;
- Where helpful, include clearly labelled images to illustrate the practices in place e.g. the airlock, climbing points, locking systems etc. Images can be included within the relevant section, or within the appendix of this document;
- Reviews of this document should occur when any section has been updated, at a point of any significant learning or breach in security;
- At the rear of this document is space for a procedural security index document (PSID). This should be utilised as an aide memoire for all applicable security policies.

Please note that the **description section** is for services to describe in detail how their service relates to that standard.

In each standard, the **policy section** is to allow for the signposting of where that policy can be found. Do not add the entire policy.

Types of standards

Each standard has been rated to define whether it is essential, expected or desirable in relation to patient care.

All criteria are rated as Type 1, 2 or 3

> **Type 1:** Essential standards. Failure to meet these would result in a significant threat to patient safety, rights or dignity and/or would breach the law.
>
> **Type 2:** Expected standards that all services should meet.
>
> **Type 3:** Desirable standards that high performing services should meet.

The typing of each standard is indicated by the number in square brackets following the standard number, e.g. [Type 1].

What training should I receive in physical security?

The level of training required for each person within a secure service will vary dependant on the role and the day-to-day duties or functions. All staff working within a secure service must receive basic security training covering type 1 and type 2 standards during their induction and prior to taking full responsibility for any service security elements applicable to their role.

Each organisation will have a standard baseline for statutory and mandatory training. For secure services, additional training will need to be identified to support procedural, relational and physical security which is a key stone for this service type.

Within each section, key learning is indicated to guide training within your service. These sections should be collated and feature in a training plan/development portfolio and staff competency should be assessed.

Information governance

Your organisation's data protection officer is responsible for ensuring personal data is managed according to the General Data Protection Regulation (GDPR).

Your Quality Network review

The PSD should be held at a local level and not sent or stored outside of your organisation. As part of your self-review, you will be asked to share the audit and review (Section 7.0) only as evidence of compliance with the various sections. This section is on a **separate Word Document** provided by the Quality Network team. The full document should be readily available on Quality Network visits for review by the peer-review team. Please do not submit this PDF document.

What is a physical security document?

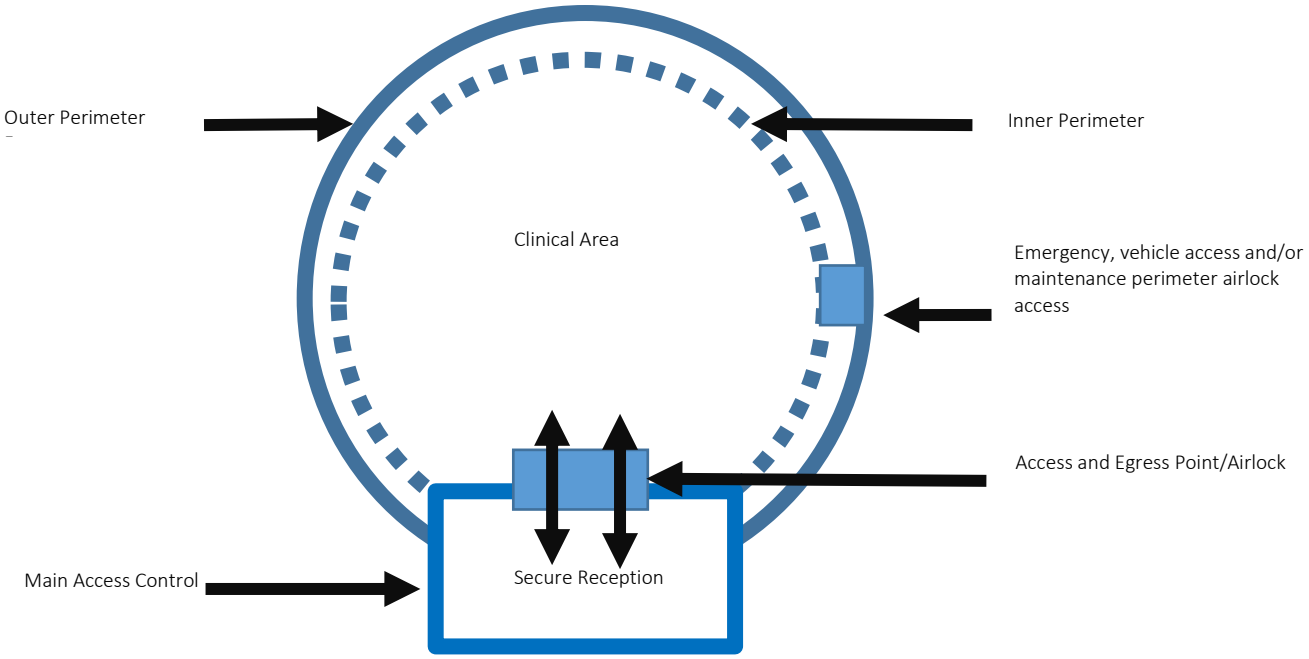
Key learning:

- **General awareness of physical security principles in secure care and its relationship with procedural and relational security mechanisms**
- **Understanding of the physical security document in relation to individual roles**
- **Patients and carers are offered a basic introduction to physical security and the reasons underpinning practices (good and open understanding of the rules that people live within supports positive behaviour)**

A physical security document (PSD) describes the physical security in place at the service, including:

- How the building and security elements work;
- The inner and outer security of the building and how they relate;
- The security process in controlling the environment;
- The security systems in place to a level that it can be used as a training aid;
- How physical security processes are monitored, audited and reviewed;
- How staff are trained, evaluated and developed.

The following diagram illustrates a basic model of a secure service:



Guidance

The PSD is a central place to bring the range of policies, procedures and practices together to aid the service in describing how and what security is, how it is monitored and developed. Its importance is as a central record of these various elements and is a live document that should be reviewed regularly. These reviews should reflect any changes to policy, procedure or practice and occur after all policy reviews, after any significant security incident or where any new procedure or training requirement is developed. It should act as the descriptor of the service and aid in training, monitoring and ensuring and reflecting ongoing development of the service.

Security of this document

This document is a resource for the service and should be used to assure, inform and validate practice. In the interests of security, it should not be accessible to unauthorised people. The organisation should store this document in a safe location where staff can access it routinely.

This is a live document and influences training, induction and practice. Security leads should always be mindful of the information contained and seek the best way to share the information, in a way suitable for the audience. For example, a simplified patient/carer guide to inform them of their role within physical security.

What does my service look like?

Within the following table, detail the level of security, gender and number of beds for each ward:

Ward name	Level of security	Gender	No. of beds	Ward type (e.g. mental health, learning disabilities, autism, personality disorder, deaf, neurological etc)

Guidance

Please ensure that the information provided accurately summaries the type and function of wards/units within the secure perimeter of the service. It assists in understanding the role of security within the perimeter. On mixed sites, it aids the identification of different levels of security. It may be necessary to add additional information that can clarify a unit's function. Such as a blended security ward, pre-discharge ward or independent living unit. This information should then be reflected throughout the PSD to ensure that all services within the perimeter are described.

1.0 Who is responsible for physical security?

Key learning:

- **The responsibility of individual staff in maintaining service integrity and the safety of patients, staff and the public**
- **The responsibility of the designated security lead**
- **How to report concerns or issues relating to physical security**

The designated security lead undertakes tailored training to their role which encompasses:

- **The role of the designated security lead**
- **Responsibilities and expectations**
- **Governance and audit processes**
- **Restrictive practices**
- **Liaising with external agencies**

Everyone is responsible for physical security within your service. Physical security systems promote safety and public protection.

All staff are expected to complete some level of physical security training, however there is one designated security lead within your service.

The following standards indicate the expectations of the designated security lead. The designated security lead has the responsibility of managing the physical security of the service, as determined by this document.

Standard 1.1 [Type 2]: A designated security lead has responsibility for security within the service. The designated individual has relevant experience and training.

Guidance

Oversight on security is a key task, one that requires a significant amount of training, support and supervision. Although there are various roles within a service, from shift to shift functions, through to a service wide coordinator role and right up to board. It is important to remember that security is the function of all staff within secure care and its inherent in their role, and their function. It is clearly stated in job descriptions and all staff are trained and developed in that role. However, the board of the service has the overall responsibility and authority to ensure safe practice. The security lead role is a key individual that undertakes a leadership role in the service to maintain standards and practice relating to security and assurance to the board (directly or via a clearly set out accountability framework).

Description of practice(s):
Local policies and procedures:
Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Standard 1.2 [Type 2]: The designated security lead ensures policies and procedures are proportionate to the risks identified. A process for reviewing restrictive practices is in place, with specified timescales.

Guidance

All policies are reviewed within the set timescales and after significant breaches of security. Continuous learning is required to ensure safe practice and the security lead is part of any clinical development structure to ensure safe and effective practice. Breaches to policy and practice standards are alerted via the services management structure and managed in line with the services polices and practice.

Description of practice(s):

Local policies and procedures:
Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Standard 1.3 [Type 2]: The designated security lead has systems in place to ensure effective liaison with local police on incidents of criminal activity/harassment/violence and other criminal justice agencies, where relevant. A memorandum of understanding is in place with local police on reporting crime.

Guidance

Liaison with local police occurs at senior level to formalise any joint policies. Day-to-day or regular monitoring and sharing of experience can assist in ensuring positive working relationships, avoiding misunderstandings and confusion. Shared training opportunities, to understand the scope of practice, the functions of the services, and wider mental health issues, can also aid collaboration. It should be remembered that other blue light services may also benefit from this approach. This will also enhance any desktop exercises or shared protocols.

Description of practice(s):
Local policies and procedures:

Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Section 1.0 Who is responsible for physical security?
Valid from:
Valid to:

2.0 Perimeter and access

Key learning:

- **What is a secure perimeter?**
- **Internal and external perimeter: Key features**
- **Maintaining service integrity**
- **Controlled systems and expectations**
- **Inspecting the perimeter**
- **Escalating concerns and remedial action**
- **Record keeping and audit**
- **Maintaining a therapeutic environment and patient experience in secure services**

The designated security lead undertakes additional training or has experience in more depth:

- **Maintaining service integrity**
- **Escalating concerns and remedial action**
- **Record keeping and audit**

As specified in the Environmental Design Guide for Adult Medium Secure Services (2007), the secure perimeter comprises:

- Areas where patients are continually observed or engaged in treatment and therapy for example in clinical and therapy rooms, workshops and communal day areas including the secure garden
- Areas where patients are intermittently observed such as bedrooms and en-suite, communal bathrooms and toilets, visitors' facilities
- Staff areas that are directly related to operational service delivery
- The reception and control room

In order to facilitate freedom of movement for patients within the unit, the service should agree an internal perimeter normally defined by the secure doors leading to outside areas (see illustration in 'What is a physical security document?' section above).

The following section sets out the standards and requirements to maintain service integrity.

Standard 2.1 [Type 1]: The secure perimeter is in line with the planning specification for the level of security offered, is protected against climbing, and is easily observable.

Guidance

The secure external perimeter is a physical barrier aimed at reducing risk and maintaining service integrity. It can be defined as a number of systems and processes that protect against unauthorised egress and access to a facility.

Perimeter security involves the use of multiple layers of interdependent systems, including CCTV surveillance, security roles, protective barriers, locks, access control protocols, and many other techniques.

A holistic approach is taken to perimeter security; the perimeter is the solid foundation upon which the other aspects of security are built.

It is essential that it conforms to the minimum design standards and there are systems and processes in place that can be demonstrated to evidence its compliance, maintenance and control.

A secure external perimeter:

- Is formed by buildings;
- Is formed by buildings connected with fencing (5.2 m high for MSU and 3m high for LSU from ground floor level);
- Joins the secure reception and surrounds the remainder of the unit;
- Surrounds the whole unit.

Fencing is weld mesh in design (3mm diameter and 13mm centres vertically and 75mm centres horizontally).

Features within the secure external perimeter are anti-climb.

Any weaknesses within the external perimeter are documented (images of weaknesses are provided).

Describe the external perimeter of your service

Local policies and procedures:
Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Standard 2.2 [Type 2]: There is a daily recorded inspection of the perimeter and programme of maintenance specifically for the perimeter, with evidence of immediate action taken when problems are identified.

Guidance

A physical inspection of the perimeter occurs, as a minimum, twice daily. The inspection captures the features that define the external perimeter, including any fixtures and fittings.

Inspection times are varied. Any checks are captured in a recordable format, open to inspection and retained in line with local policy. The physical condition of the fencing and walls are checked and reported on. Any physical, relational or procedural breaches are recorded and available for audit.

The record is a standardised template; it is completed to a high quality and records are audited monthly.

Description of practice(s):

Local policies and procedures:
Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Standard 2.3 [Type 1]: Windows that form part of the external secure perimeter are set within the building masonry, do not open more than 125mm and are designed to prevent the passage of contraband.

Guidance

Bedroom windows ensure privacy, allow ventilation for fresh air, and provide adequate natural light. Their construction and design prevent against escape, the passage of illegal/contraband items and are ligature free. They comply with the minimum standards.

Where compliance cannot be fully achieved, a risk-based approach is adopted.

Description of practice(s):
Local policies and procedures:

Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Standard 2.4 [Type 1]: Access to the secure service for visitors, staff and patients is via an airlock.

Guidance

An airlock is a physical access security system comprising a space with two or more doors/gates, one of which must be closed before another can be opened. All access through the secure perimeter is managed by such an airlock system, either procedural or electronic, whereby the integrity of the secure perimeter is maintained by at least one of the two doors/gates being locked at all times. This applies to pedestrian and vehicular access to the service.

Description of practice(s):
Local policies and procedures:
Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Standard 2.5 [Type 2]: The reception/control room is:

- **Within or forms part of the secure external perimeter;**
- **Staffed 24 hours per day 7 days a week or can be made fully operational in the case of an emergency.**

Guidance

A control room is a purpose-built facility. It acts as the co-ordination and control centre for all aspects of the unit's security.

The operation of the secure reception is documented within the operational procedure.

A local operating procedure identifies how the control room manages its day to day tasks, which includes the following:

- Allocation of keys/fobs
- Staff access
- Staff egress
- Allocation of staff radios and alarms
- Alarms
- Service user access and egress procedures
- Service user access unescorted
- Service user access escorted
- Access and egress for deliveries
- New admissions
- Visitors
- Emergency access to the control room
- Access by emergency services
- Staff permitted to authorise visitors

Description of practice(s):
Local policies and procedures:

Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Standard 2.6 [Type 1]: There are controlled systems in place to manage access and egress through all doors and gates that form part of the secure perimeter.

Guidance

The control room is responsible for access and egress through all doors and fates that form part of the outer secure perimeter.

Description of practice(s):
Local policies and procedures:
Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Standard 2.7 [Type 2]: In outside areas within the secure perimeter, permanent furniture, fixtures and equipment are fixed and are prevented from use as a climb aid.

Guidance

All garden furniture is fixed and away from eaves to prevent climbing.

Trees are well maintained to prevent overhanging external perimeters. This includes any climbing plants/weeds that could grow on the fencing.

An estates maintenance programme is in place for landscaping.

Description of practice(s):
Local policies and procedures:
Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

3.0 Inner perimeter and controls

Key learning:

- **The inner and outer perimeter**
- **Authorised movement between the inner and outer perimeter**
- **Management of key handling and technological systems that maintain the integrity of the inner perimeter**

Standard 3.1 [Type 2]: There is a key management system in place which accounts for all secure keys/passes, including spare/replacement keys which are held under the control of a senior manager.

Guidance

Key handling and management are the most critical parts of maintaining service integrity. Constant accounting for the correct allocation and receipt of keys and associated technology ensures any breaches in security are immediately identified. Immediate response to any key handling breaches will ensure the service is able to maintain effective perimeter security.

Management of key systems, including the design of the key suiting systems, supports effective key control. In routine practice, keys allocated are zoned to support good perimeter control. Services do not allocate a master key or sub-master key in routine use, as this will compromise perimeter security. The transition between inner and outer perimeter results in a key exchange that is designed to prevent pass-back or the use of inner security keys outside of the building.

Description of practice(s):
Local policies and procedures:
Associated policies and procedures:

Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Standard 3.2 [Type 2]: Secure pass keys are:

- **On a sealed ring;**
- **Secured to staff at all times within the secure perimeter;**
- **Prevented from being removed from the secure perimeter.**

Guidance

Key sets are designed with a minimum amount of keys. Technological solutions are available for key allocation and these also limit the amount of keys allocated to one individual. Multiple sets and multiple access zones being available to one individual at the same time is poor practice.

Key sets or other technological solutions are securely attached to staff to prevent key loss.

To prevent loss of keys from within the perimeter, a system of key exchange occurs at the point of inner and outer perimeter transfer.

A key set is an identified sealed unit that is accounted for within the key handling system.

Description of practice(s):
Local policies and procedures:
Associated policies and procedures:

Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Standard 3.3 [Type 1]: There is a process to ensure that:

- **Keys are not issued until a security induction has been completed;**
- **Keys are only issued upon the presentation of valid ID;**
- **A list of approved key holders is updated monthly identifying new starters who have completed their induction training and any leavers from the service.**

Guidance

The key handling system is robustly monitored. Keys/technological solutions are issued to an identified and approved individual and access is only provided to authorised zones.

A form of photographic or biometric identification is presented to confirm the authorisation of keys to an individual.

An active approved key allocation list is maintained by the service; this includes what key access that individual is usually entitled to and what additional authorisation is required for them to have an alternative set.

Description of practice(s):
Local policies and procedures:
Associated policies and procedures:

Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Standard 3.4 [Type 1]: Patient bedroom and bathroom doors are designed to prevent holding, barring or blocking. Bedrooms have patient operated privacy locks that staff can override from the outside.

Guidance

The integrity of the inner perimeter requires governance over significant risk areas.

Access to patient bedrooms is maintained at all times for the purposes of patient and staff safety.

There is a staff override system in place on bedroom doors, regardless of whether patients have allocated bedroom keys or simple privacy locks are in place. This can include simple override keys or more complex systems to render the locking system redundant (such as, removable box staples or bi-swing doors).

Description of practice(s):
Local policies and procedures:
Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Standard 3.5 [Type 1]: Doors in rooms used by patients have observation panels with integrated blinds/obscuring mechanisms. These can be operated by patients with an external override feature for staff.

Guidance

Accessing any space during emergencies or to maintain general or specific observation requires staff to be able to visually monitor patients when they are within their own room or other risk areas.

As with all observation, the maintenance of privacy and dignity requires a process to enable observation that supports patient privacy but allows staff override.

Description of practice(s):
Local policies and procedures:
Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

4.0 Technology and surveillance

Surveillance technology includes CCTV, cameras and microphones. Where a service is using surveillance technology, it operates in line with the CQC's Using surveillance in your care service guidance[2].

Key learning:

- **Using technology and supportive surveillance equipment**
- **Confidentiality, privacy and legal issues in relation to data protection**
- **Benefits and limitations of technological solutions to surveillance (including passive or active surveillance)**
- **Using surveillance recording in the management of incidents and subsequent investigations**

Standard 4.1 [Type 2]: Where CCTV is in use, there should be passive recording of the perimeter, reception frontage and access from the secure area to reception.

Guidance

CCTV (closed-circuit television) is a television system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes.

Services that have CCTV in use around their perimeter or in communal areas have policies/procedures in place that address the following:

- The identification of individual who is responsible for overseeing CCTV, often referred to as a data controller.
- A defined and identified purpose relating to the use of CCTV in the service, including what information can be stored.
- The identification of staff that can operate the system and manage the data.
- A process for viewing, storing, retrieving and deleting data once it is no longer required.
- A process for surrendering stored data onto a disc and associated documentation that protects the subjects within the data.
- Services using CCTV should ensure that all processes associated with its use are compliant with General Data Protection Regulation (ICO, 2018).

[2] https://www.cqc.org.uk/guidance-providers/all-services/using-surveillance-your-care-service

Standard 4.2 [Type 1]: There are clear lines of sight to enable staff members to view patients. Measures are taken to address blind spots and ensure sightlines are not impeded.

Guidance

Observation of the environment is a key part of relational and procedural security. The physical design of the building should support and enhance good observation.

Consideration is given to reducing observational difficulties where physical obstructions to observations exist that cannot be ameliorated by design.

Measures may include:

- Staff placement and observational duties
- Use of mirrors
- Removal of obstructions to observation panels or internal glazing (i.e. have a clear window policy onsite)
- CCTV

If CCTV is used to monitor lines of site, services adhere to the guidance relating to CCTV documented in the section above.

Description of practice(s):
Local policies and procedures:
Associated policies and procedures:

Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Section 4.0: Technology and surveillance
Valid from:
Valid to:

5.0 Contingency and emergency planning

Key learning:

- **Planning for unplanned disruptions**
- **Risk management approaches**
- **Building a contingency framework**
- **Communicating in an emergency**
- **Working with partner agencies and local services**
- **Maintaining patient and staff safety during an emergency**
- **Ensuring continuity of care during emergency situations**
- **Live and desktop exercises**

The effects of unplanned disruptions to the delivery of healthcare activities can range from short-term impacts, such as interruptions to utilities or IT services, or major or more long-term disruption effects, such as the loss of physical facilities which would require the relocation of patients to alternative care facilities.

Whilst the focus should always be on preventing disruption as part of a proactive risk managed approach, it is important that up to date contingency plans and arrangements are available and practiced to mitigate disruption effects and to reinstate patient care delivery with the minimum of delay.

Standard 5.1 [Type 1]: A contingency plan addresses:

- **The chain of operational control;**
- **Communications;**
- **Patient and staff safety and security;**
- **Maintaining continuity in treatment;**
- **Accommodation;**
- **Testing by live and desktop exercises, including a collective response to rehearsing alarm calls at least six-monthly.**

Guidance

The following paragraphs detail each element of a contingency plan:

The chain of operational control: There is a clearly understood organisational structure to manage the response to disruptive events. This includes the identification of specific roles to facilitate the management response at different stages of an event, for instance, the emergency response phase, the 'taking

control' phase (i.e. incident command procedures) and activating the business continuity phase of the recovery.

Responsibilities of staff members within the chain of operational command are documented and training is provided to these individuals.

The organisational arrangements identify how information will be escalated for decision-making or support within the organisation.

Communications: Effective communications are essential to the successful management and response to a disruptive event or situation.

Current and up-to-date contact lists of key personnel and functions are maintained and accessible and available to use when required.

Communications plans identify how information will be 'cascaded' to relevant persons and functions internally and externally to the organisation, and also the means for escalating information to senior management for support and decision-making.

Patient and staff safety and security: Patient safety and security will be dependent upon the continued availability of a range of facilities, services or resources, which if lost or disrupted could have significant safety and security impacts.

A risk assessment on facilities, services and resource dependencies for patient safety and security is in place to identify the potential impacts of the loss of one or more of these factors on patient safety and security. This will then prioritise contingency planning arrangements.

Contingency plans consider requirements for temporary and alternative accommodation for patients, accommodation security levels, the provision of access to medications and prescriptions, access to patient medical records, availability of specialist clinical equipment, and the availability of sufficient numbers of trained staff to maintain care and safety standards, safety and security.

If relocating patients, their location is tracked and monitored, at all times. If moving patients to alternative environments, the implications for detention orders are assessed and communicated to the relevant authorities, and instructions awaited.

Maintaining continuity in treatment: Where there is disruption to the usual arrangements for patient care delivery, the recovery objective for contingency arrangements must be to reinstate care delivery to the required standards as soon as possible. Contingency plans address alternative accommodation requirements for patients, accommodation security levels, the provision of access to medications and prescriptions, access to patient medical records, availability of

specialist clinical equipment, and the availability of sufficient numbers of trained staff to maintain care and safety standards and security.

Accommodation: The most significant contingency exposure to low and medium secure facilities is the loss of use of ward environments.

There is a risk that the supply of alternative low and medium secure patient accommodation may not be available when required. To mitigate this, each ward has a contingency arrangement for the relocation of patients to temporary accommodation pending a move to secure accommodation elsewhere.

Contingency considerations for temporary accommodation include:

- The security of temporary accommodation is paramount.
- Temporary accommodation is checked for hazards, e.g. sharps, ligature points and other safety risks, which are removed before the patients occupy.
- Consider patient access to toilets, washing facilities and bedding, as well as arrangements for providing food and drink, and access to medications.
- Plan for how different patient groups will be accommodated, considering patient risk, dignity and safety.
- Sufficient staff are available to manage the situation.
- Record keeping is in place to identify where patients have been relocated to.
- Stakeholders are kept informed on any changes to detention order requirements regarding patient locations, and any instructions received concerning the patient.

Where patients are to be relocated to alternative low or medium secure accommodation, the following arrangements are considered in the contingency arrangements:

- Patient moves comply with any revised detention order terms.
- Staff are provided to accompany the patient to the alternative accommodation and may be required to continue to support the patient for a period pending handover to the alternative provider.
- Arrangements are in place to anticipate additional staff costs potentially including overtime and accommodation costs.
- Patient records accompany the patient and may ultimately need to be transferred to the alternative provider.
- Patient medications accompany the patient during the transfer.

The period of denied access to the original ward environment will have a bearing on the activation of accommodation contingencies.

Testing by live and desktop exercises, including a collective response to rehearsing alarm calls at least six-monthly: Management and staff receive information and training on the contingency planning and recovery arrangements in place and how they are activated. This training may take place in a number of ways:

- Presentations and training sessions
- Desk-top exercises
- Rehearsals to activate and practice contingency arrangements, e.g. rehearsing emergency evacuation and incident command procedures
- Scenario exercises involving other organisations/functions/departments, including emergency services and local services

Training exercises are undertaken at regular intervals to ensure management and staff are practised and confident in the use of the plan and that the contingency arrangements and plans are effective.

Mutual aid: A system of mutual aid is identified to establish capacity that will be available to suit the re-accommodation of patients during an emergency. Joint working agreements are in place between geographical areas/provider collaboratives/organisations. This type of mutual aid is developed through desktop exercises, as stated above. Provider collaboratives are particularly suitable for establishing this kind of mutual aid system.

Description of practice(s):
Local policies and procedures:
Associated policies and procedures:

Standard type:
Valid from:
Valid to:
Compliance RAG rating:

Section 5.0: Contingency and emergency planning
Valid from:
Valid to:

Standard 5.2 [Type 1]: Call button/personal alarms are available to all staff, patients and visitors within the secure perimeter.

Guidance

Staff: All staff entering areas of direct patient contact are allocated an alarm which is pre-programmed for alarm response appropriate to the area(s), which they are entering. Alarms are issued by secure reception staff who are responsible for ensuring the units are charged. Once an alarm has been issued this is worn on the individual staff's person without delay. A daily record is kept of individuals that have been issued an alarm.

Patients: Patients have access to either a nurse call button or a panic attack alarm, depending on the systems available on the ward.

Visitors: Visitors entering the secure perimeter are accompanied by a staff member in possession of an alarm at all times, or they are offered their own alarm. Practices are outlined in local policies. Alarms are issued by secure reception staff who are responsible for ensuring the units are charged. Once an alarm has been issued this is worn on the individual's person without delay. A daily record is kept of individuals that have been issued an alarm.

The designated security lead reviews the use of alarms each month to identify key themes and issues.

Description of practice(s):
Local policies and procedures:
Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

6.0 Developmental practices

Developmental security practices, such as body worn cameras, do not form part of the formal agreed QNFMHS standards. Services can choose to participate in developing practice in relation to these areas further. However, any developments should adhere to relevant guidance provided by commissioners, regulators and organisations providing national guidance and advice on health and social care.

Use this section to describe practice(s) in development.

Description of practice(s):
Local policies and procedures:
Associated policies and procedures:
Standard type:
Valid from:
Valid to:
Compliance RAG rating:

7.0 Audit and review

**** Please refer to the Audit and Review document and return section 7.0 to the Quality Network. This is a Word Document for section 7.0-9.0. ****

Reference list

Care Quality Commission (2019) Using surveillance in your care service. Available at: https://www.cqc.org.uk/guidance-providers/all-services/using-surveillance-your-care-service

Department of Health (2007) Best Practice Guidance Specification for adult medium-secure services. Health Offender Partnerships 2007. Available at: http://data.parliament.uk/DepositedPapers/Files/DEP2007-0001/DEP2007-0001.pdf

Department of Health (2011) Environmental Design Guide: Adult Medium Secure Services. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/215623/dh_126177.pdf

Information Commissioner's Office (2018) Guide to the General Data Protection Regulation (GDPR). Available at: https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

NHS England (2018) Service specification: low secure mental health services (adult). Available at: https://www.england.nhs.uk/publication/service-specification-low-secure-mental-health-services-adult/

NHS England (2018) Service specification: medium secure mental health services (adult). Available at: https://www.england.nhs.uk/publication/service-specification-medium-secure-mental-health-services-adult/

RCPsych (2019) Standards for Forensic Mental Health Services: Low and Medium Secure Care – Third Edition. Available at: https://www.rcpsych.ac.uk/improving-care/ccqi/quality-networks-accreditation/forensic-mental-health-services/publications-and-resources

Acknowledgements

The Quality Network for Forensic Mental Health Services would like to thank the following people for their time and expertise in the development of this document:

Patrick Neville, Strategic Development Director, Elysium Healthcare (Chair)

Colin Dowle, Reception Security Team Leader, Hellingly, Sussex Partnership NHS Foundation Trust

Sheena Foster, Family and Friends Representative, CCQI

Gill Hughes, Security Manager, Ashworth Hospital, Merseycare Foundation Trust NHS Trust

Denise Inggall, Modern Matron, Marlborough House, Oxford Health NHS Foundation Trust

Dave King, Clinical Nurse Specialist and Security Lead, Humber Centre for Forensic Psychiatry, Humber Teaching NHS Foundation Trust

Mike Kingham, Consultant Forensic Psychiatrist, Trevor Gibbens Unit, Kent and Medway NHS and Social Care Partnership Trust

Su Pashley, Patient Representative, CCQI

Ash Roychowdhury, Consultant Forensic Psychiatrist and Clinical Director of Forensic Services, St Andrews Healthcare Northampton

Roger Sharp, Patient Representative, CCQI

Neil Woodward, Security Manager, Ridgeway, Tees, Esk and Wear Valleys NHS Foundation Trust

James Wright, Head of Operations, Fromeside Hospital, Avon and Wiltshire Mental Health Partnership Trust

The Quality Network would also like to thank:

NHS England's Clinical Reference Group for Adult Secure Services

Delegates that attended the 'Physical Security in Secure Services' consultation event, 3 March 2020

Royal College of Psychiatrists Centre for Quality Improvement
21 Prescot Street • London • E1 8BB

www.rcpsych.ac.uk

COLLEGE CENTRE FOR QUALITY IMPROVEMENT