

A FRAMEWORK FOR THE PERFORMANCE MANAGEMENT OF HIGH SECURITY HOSPITALS

Agreed between



ISSUE NO: 1
ISSUED: April 2008
REVIEW: April 2009
LEAD: Elizabeth Stevens (Elizabeth.Stevens@eastmidlands.nhs.uk)

DH INFORMATION READER BOX

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

Document Purpose	For Information
Gateway Reference	10215
Title	A framework for the Performance management of high security hospitals
Author	NHS East Midlands/ NHS London/ NHS North West SHAs
Publication Date	01 Apr 2008
Target Audience	
Circulation List	Those with an interest in high secure services
Description	This framework describes the structure and mechanisms by which the Secretary of State for Health's 'line of sight' in relation to high security hospitals should be discharged by Strategic Health Authorities.
Cross Ref	n/a
Superseded Docs	New arrangements for the performance management of high security psychiatric services (2002)
Action Required	n/a
Timing	n/a
Contact Details	Elizabeth Stevens NHS East Midlands elizabeth.stevens@eastmidlands.nhs.uk
For Recipient's Use	

CONTENTS

SECTION 1 INTRODUCTION

- Introduction
- The Context of High Security Hospitals
- Significant Stakeholders
- Background to Performance Management of High Security Hospitals

SECTION 2 RESPONSIBILITIES OF THE SECRETARY OF STATE

- The Secretary of State's Statutory Responsibilities
- The Secretary of State's Power of Direction
- The Secretary of State's Safety & Security Directions
- The Secretary of State's License Criteria

SECTION 3 RESPONSIBILITIES OF STRATEGIC HEALTH AUTHORITIES

- Responsible SHAs
- Overarching SHA Responsibilities
- The Role of the Performance Manager
- Lines of Accountability
- SHA Presence at the High Security Hospital
- Access to the High Security Hospital
- Confidentiality
- Specific Responsibilities of Performance Managers
- Performance Manager Boundaries
- The Formal Infrastructure for Performance Management
- Performance Information
- Incident and Issue Reporting (National Reporting Policy)

Appendix 1 National Commissioning Strategy for High Secure Services

Appendix 2 License Criteria and Arrangements

Appendix 3 Critical Relationships

Appendix 4 Quarterly Performance Report

Appendix 5 Cluster Groups

Appendix 6 National Reporting Policy for High Security Hospitals

Appendix 7 Performance Management Arrangements & Wales

(Documents subject to different timeframes for review to this framework are contained within the Appendix. Subsequent readers of this framework should contact the Department of Health Secure Services Policy Team for updated editions).

SECTION 1 INTRODUCTION

1.1 Introduction

This framework brings together and builds on work to establish the structure and mechanisms by which the maintenance of the Secretary of State's 'Line of Sight' to high security hospitals should be discharged by Strategic Health Authorities (SHAs).

The framework is endorsed by the Department of Health and the Welsh Assembly Government and is approved by Ministers on behalf of the Secretary of State for Health.

In 2002 'New Arrangements for the Performance Management and Commissioning of High Secure Psychiatric Services' proposed a structure for the oversight and commissioning of high security hospitals and standards for the measurement of those services derived from recommendations made in 'The Report of the Review of Security of the High Secure Hospitals' (2000).

Two factors indicate the need to now review and set out more specific and developed arrangements for the performance management of high security hospitals:

Firstly, SHAs have now had the opportunity to experience the range of risks connected with high security hospitals and to test the performance management arrangements necessary to mitigate and manage those risks. SHAs have also now had the opportunity to develop relationships with their respective high security hospital providers and to implement a range of structures that maintain those relationships. A revised framework provides the opportunity by which the three SHAs can share their learning and agree upon the arrangements that work within a common structure.

Secondly, new arrangements for the commissioning of high secure services have since been set out in 'A Strategy for High Secure Services' (2006) (see Appendix 1 for summary), superseding 'New Arrangements for the Performance Management and Commissioning of High Secure Psychiatric Services' (2002) in respect of commissioning. The commissioning framework takes account of the devolution of commissioning to PCTs and aims to achieve congruence with National Specialised Services commissioning arrangements in line with the Carter Report.

1.2 The Context of High Security Hospitals

High security hospital services for England and Wales are provided across a small network of three hospitals - Ashworth, Broadmoor and Rampton.

Each of the three hospitals is currently integrated within local NHS mental health services that operate under license from the Secretary of State to provide high security hospital services.

High security hospitals have a Category B prison equivalent security perimeter supported by the security procedures necessary for the safe and secure detention of patients posing a grave danger to the public. Those physical and procedural security policies are audited annually by the prison service.

Patients detained for therapeutic treatment in high security hospitals can be genuinely difficult to manage. They are admitted having been assessed as posing a grave and immediate danger to others if at large. The prevalence of self harm is high and patients frequently exhibit subversive, violent and assaultive behaviour.

It is not unique to high security services that healthcare staff balance the provision of modern therapeutic interventions with the management of issues of security and safety. Mental health services are faced with this challenge daily. However, managing these dynamics together *equally* and with such levels of risk in a way that satisfies the needs of patients and that of interested parties makes these services amongst the most complex in the NHS. It also makes them amongst the most expensive - in 2006/07 the SLA value was £224.5m.

The serious offending profile of patients, the public protection imperative, the specialist security arrangements necessary and the legal requirement for the Secretary of State to provide these services places them amongst the highest profile in the NHS. This profile also gives rise to a high level of sensationalised public and media interest and makes them subject to considerable legal challenge at a local and national level.

These components together make the performance management of such services different to any other specialist service and explain the need for very specific, possibly unique, performance management function required by the Secretary of State to ensure an appropriate level of external scrutiny in the services.

1.3 Significant Stakeholders

Parties with a significant stake in the services provided by high security hospitals include:

- The Secretary of State for Health
- The Department of Health
- The Welsh Assembly Government
- The National Oversight Group
- National Offender Management Service
- HM Prison Service
- Ministry of Justice
- Mental Health Act Commission
- Social Services
- Professional organisations (Royal College of Psychiatrists etc)
- Police
- Immigration Service

1.4 Background to Performance Management of High Security Hospitals

Specific performance management arrangements for high security hospitals were established in response to recommendation 44 of the Report of the Committee of Enquiry into the Personality Disorder Unit at Ashworth Special Hospital. The report stated "We recommend that Ministers reflect on our comments and consider whether the chains of accountability in the NHS, at all levels, should be reviewed and clarified".

The report raised a catalogue of concerns about operational practice, culture and management arrangements all pointing to the existence of a 'closed institution' into which it was felt there was insufficient scrutiny from an external perspective.

The Review of Security at the High Security Hospitals (2000) reinforced the importance of high security hospitals being subject to rigorous scrutiny and effective monitoring processes, setting out the need for new performance indicators and clarity about the roles of the parties involved in the performance management of the services. The report stated that "those with responsibility for monitoring the performance of the high security hospitals will need to possess a real understanding of the hospitals and the potential risks which they present. We believe that, in order to gain this understanding, there is no substitute for spending time within the hospital sites, visiting wards and other areas and speaking to staff and patients."

Responsibility was delegated to NHS Executive Regional Office Directors (through NHS reform becoming Strategic Health Authorities) for those areas in which high security services were delivered.

SECTION 2 RESPONSIBILITIES & POWERS OF THE SECRETARY OF STATE

2.1 The Secretary of State's Statutory Responsibilities

Section 1 (1) of the National Health Service Act 2006 ("the 2006 Act") provides that the Secretary of State's must continue the promotion in England¹ of a comprehensive health service designed to secure improvement–

- (a) in the physical and mental health of the people of England, and
- (b) in the prevention, diagnosis and treatment of illness.

Subsection (2) provides that the Secretary of State must provide or secure the effective provision of services in accordance with the Act.

Section 4 of the 2006 Act states that the duty imposed on the Secretary of State by section 1 (above) includes a duty to provide hospital accommodation and services for persons who are–

- (a) liable to be detained under the Mental Health Act 1983 and
- (b) in the opinion of the Secretary of State require treatment under conditions of high security on account of their dangerous, violent or criminal propensities.

These services are referred to in the 2006 Act as "high security psychiatric services".

2.2 The Secretary of State's Power of Intervention

The 1977 NHS Act awards the Secretary of State powers of direction which enable her/him to intervene in a high security hospital in matters of management, security, service provision or capacity. These powers are exercised through the Strategic Health Authorities.

2.3 The Secretary of State's Safety & Security Directions

Safety and Security Directions were issued by the Secretary of State in 2000. The Directions are mandatory and set out the requirements for standards of safety and security in high security hospitals.

The Secretary of State further issued guidance in relation to the Directions which, though not mandatory, place a requirement upon the chief executive of the provider organisation responsible for the high security hospital to set out the reasons for not doing so in writing.

¹ The National Health Service (Wales) Act 2006 places a similar duty on the Welsh Ministers.

2.4 The Secretary of State's Criteria for Operating High Security Services

Paragraph 15(2) of Schedule 4 to the 2006 Act provides that an NHS Trust may not, as provider, enter into an NHS contract for the provision of high secure services unless the NHS Trust is approved for the purposes of that paragraph by the Secretary of State. There is also provision in secondary legislation stating that PCTs cannot let NHS contracts for high security services without Secretary of State approval.

Such approval:

- (a) must be for the period specified in the approval
- (b) may be given subject to conditions
- (c) may be amended or revoked at any time.

The Secretary of State's performance management functions under section 4 of the 2006 Act are exercisable by Primary Care Trusts/Strategic Health Authorities: see Part 2 of Schedule 1 to the National Health Service (Functions of Strategic Health Authorities and Primary Care Trusts and Administration Arrangements) (England) Regulations 2002 (S.I. 2002/2375)

The criteria for NHS Trusts to operate high security hospitals were set out in September 2000 by the Secretary of State for Health and remain the standard by which NHS Trusts are assessed by Strategic Health Authorities for the renewal of the license to operate a high security hospital.

Appendix 2 sets out the license criteria and the process by which SHAs assess potential providers of high security hospital services in more detail.

SECTION 3 RESPONSIBILITIES OF STRATEGIC HEALTH AUTHORITIES

3.1 Responsible Strategic Health Authorities

The SHAs (having undergone reform in 2006) responsible for maintaining the Secretary of State's 'Line of Sight' are:

NHS East Midlands	-	(Rampton Hospital)
NHS London	-	(Broadmoor Hospital)
NHS North West	-	(Ashworth Hospital)

The implementation of 'Commissioning a Patient Led NHS' fundamentally altered the role of SHAs. New core business objectives and a higher level overview of performance in NHS organisations has created some distance between the new role of the SHA and its unique and very operational performance management responsibilities for high security hospitals.

Responsible SHAs must ensure that though unique, the responsibilities for performance managing high secure hospitals are maintained and developed in line with national expectations.

3.2 Overarching SHA Responsibilities

The chief executive of the SHA is responsible for maintaining the line of sight between the Secretary of State and the high security hospital.

There must be a clear line of accountability between the SHA chief executive and the hospital.

SHA responsibilities that are unique to high security hospitals are:

- Maintenance of the 'line of sight'
- Performance management of the outcome of prison service audits
- Operational performance management
- Monitoring of compliance with the Safety and Security Directions
- Stewardship of the license for the delivery of high security hospital services and advise to the department of health on its award
- Specific national incident and media briefing arrangements
- Performance management of specialist forensic commissioners

These unique responsibilities are delivered by SHAs through a dedicated performance management role.

3.3 The Role of the Performance Manager

The performance manager (referred to by SHAs as the Performance & Policy Lead – High Security Hospitals) is a dedicated and focused role with delegated responsibility by the SHA chief executive for the performance management of the high security hospital, its commissioning (See Appendix 3) and the maintenance of the line of sight.

The tasks associated with this role should be undertaken on a full time basis with only minimum responsibilities that are not related to the performance management and development of high security hospitals included within its portfolio. The SHA should also make provisions within local workforce arrangements for any planned or unplanned absence of the performance manager.

The performance manager contributes to the development of policy and leads on its local implementation, ensuring that local and national change agendas are developed and dovetailed with overall national strategies. The performance manager is also required to support the development of national policy and processes by working with national bodies and the other two performance managers to provide for consistent working practices and performance management across all three high security hospitals within the high secure estate.

3.4 Lines of Accountability

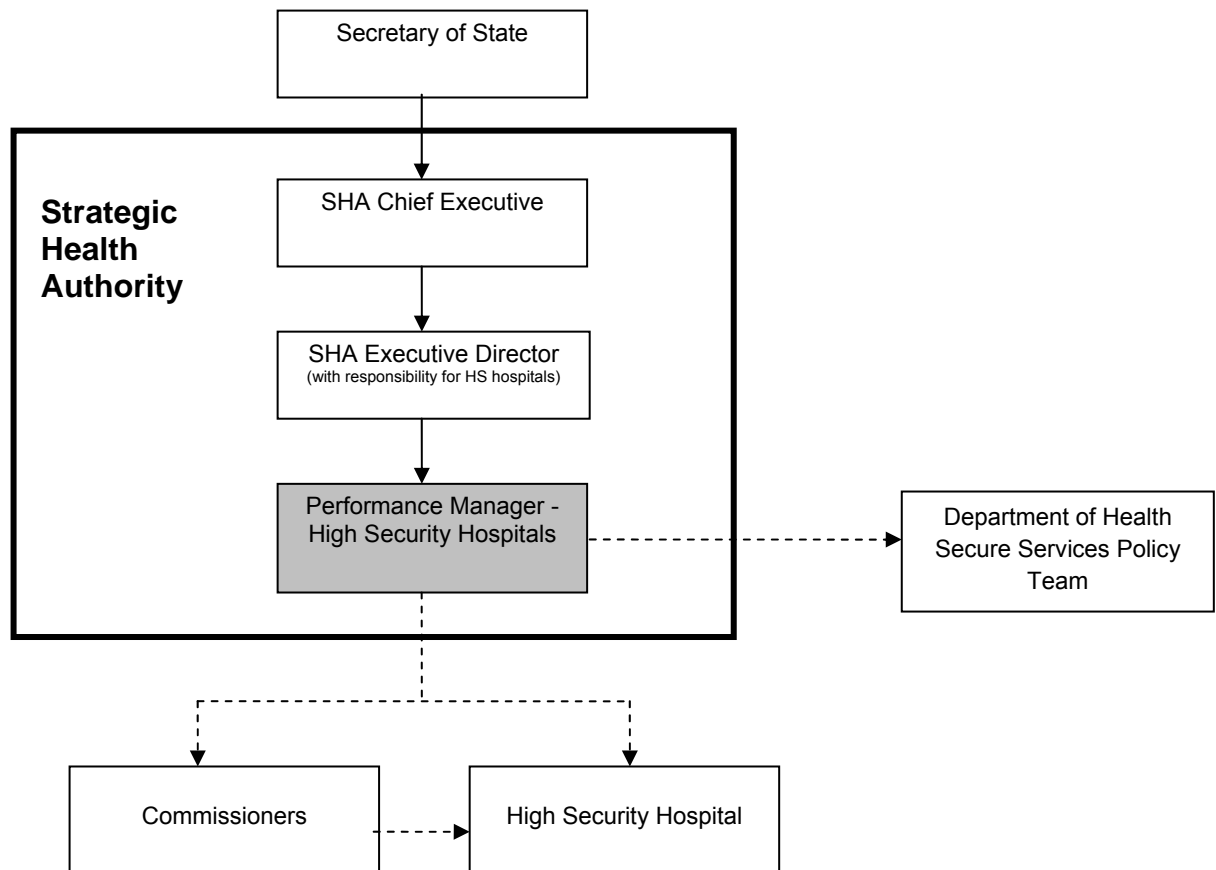
It is a minimum expectation that the performance manager reports to an executive director with delegated responsibility by the SHA chief executive for high security hospitals on a day to day basis. The line of sight must not be weakened beyond this arrangement by the further delegation of executive responsibilities and/or the introduction of other personnel into the line of sight.

Because of the unique responsibilities of the SHA chief executive in respect of high security hospitals, the performance manager should have direct access to the SHA chief executive for such issues that may require their immediate attention.

Fig.1 below describes only the stewardship arrangements for the SHA in respect of the high security hospital. It does not describe the connections to other key stakeholders and organisations.

Appendix 3 describes in greater detail the relationships between the performance manager and other critical parties.

Fig.1 Lines of Accountability



3.5 SHA Presence at the High Security Hospital

Maintaining a balance of input into the high security hospital is for the SHA essential in achieving the equilibrium between operational knowledge and the ability to maintain an impartial perspective.

Although based at the SHA headquarters, the performance manager is expected to spend sufficient time at the high security hospital as to be able to fulfil the operational performance management requirements of the role. The exact degree of on site presence is a decision that requires the judgement of the performance manager. This should be based upon the current intensity of issues and concern and agreed with the accountable SHA executive director.

On site presence is expected to be achieved through the following inputs:

- Visits to areas and departments within the secure perimeter including ward visits
- Regular meetings with members of the hospital management team
- Attendance at meetings or forums relevant to the external performance management of temporary or substantive performance issues

These inputs are expected to contribute to the achievement of:

- Ensuring that the hospital meets the standards of security specified for the service
- A detailed knowledge and understanding of ward based clinical and security issues
- The identification of areas of good practice that can be shared across the system
- The identification of poor or inconsistent practice that requires action by the hospital
- An overall improvement in patient and staff safety
- The overall reduction of risk within the service

3.6 Access to the High Security Hospital

The performance manager should hold standard security keys to the high security hospital for which they are responsible. This should not mean that the performance manager is viewed as an employee of the hospital. Indeed the performance manager should maintain a very clear status of visitor to the hospital.

Not only does the holding of keys demonstrate clear cooperation and openness on the part of the hospital but it allows the performance manager to move freely about the hospital, within the boundaries of safety and appropriateness, to perform their duties unfettered. This should be viewed as critical to providing the Secretary of State with the necessary assurance that the line of sight is not 'managed' in any way.

Duties are also incumbent on the performance manager to demonstrate to the hospital the level of professional responsibility associated with the status of honorary key holder.

The following principles should therefore apply as a minimum:

- The performance manager must meet the criteria set by the hospital for the allocation of keys
- The performance manager must undergo and maintain training relevant to and required by the hospital to achieve approved key holder status
- The performance manager will follow the safety and operational instructions of the hospital and undertake not to place themselves or others in situations of unnecessary risk

3.7 Confidentiality

The provisions of the Data Protection Act and other NHS guidance on issues of confidentiality apply to high security hospitals in the same way as to all NHS services. However, performance managers must be particularly mindful of the importance of confidentiality because of the very high level of public and media interest in these services.

Performance managers must have in place robust arrangements to ensure that all information related to high security services are treated and stored safely in line with SHA policies and procedures.

3.8 The Specific Responsibilities of Performance Managers

The following responsibilities have been agreed as common to all three SHA Performance Managers:

- To lead on the performance management of high secure hospital services and its commissioning
- To ensure high secure health and social care systems are developed to enable fair access to services for patients, equitable with that of the general public population
- To work as part of a national policy & performance system in respect of the three High Secure Hospitals (Rampton, Broadmoor & Ashworth) ensuring system wide performance improvement and consistency where it is appropriate
- To support the development of national processes and policies from time to time as may be required by the Department of Health in agreement with the responsible SHA
- To be available to conduct work on behalf of the national oversight group as may be required from time to time
- To provide advice and support on serious untoward incidents particularly on those incidents of homicide, suicide or adverse incidents with the potential to attract media attention or those that indicate a requirement to change practices
- To liaise with and provide briefings/information for the Department of Health, Ministry of Justice, Ministerial Private Office(s) and other government and NHS agencies in relation to high security hospital issues and events
- To ensure that there is a coherent, effective and on budget service strategy in place by commissioners. Where this necessitates national or local service capital development, ensure works are progressed in line with agreed timescales and within the correct frameworks for capital development
- Work with the Ministry of Justice, Department of Health, police, prison service representatives and the high security hospitals through the Secure Practice Forum to set and implement standards and processes that maximise the effectiveness of security in a therapeutic environment

- Advise on and performance manage the implementation of recommendations arising from key security audits, prison service audits, revisions to the Secretary of State Safety and Security Directions and Child Visiting Directions and any other audits or reviews that may take place locally and nationally from time to time
- Review specifically defined areas of performance at other high security hospitals as may be required
- Contribute to the development of a national emergency planning strategy and performance manage the development of local emergency planning

3.9 The Boundaries of Performance Management

Performance managers are not responsible for developing, implementing or instructing ward staff on hospital policy or activity. This includes clinical decision making in relation to patients.

3.10 The Formal Infrastructure for Performance Management

SHAs will ensure that high security hospitals complete the nationally agreed quarterly performance report (Appendix 4) by the deadlines agreed.

One of the three SHAs will take responsibility for co-ordinating this data and producing a final quarterly performance report that captures the data of all three high security hospitals. This host SHA will also produce annual summaries of data split by patient group in order that meaningful comparisons can be made between the three hospitals.

Quarterly Performance Review Meetings

Each SHA will lead and document a Quarterly Performance Review Meeting with the management team of the high security hospital.

The purpose of this meeting will be to:

- Review the quarterly performance report and consider the actions necessary to improve and sustain performance
- Discuss the progress of any current action plans
- Discuss any other issues that relate to or influence the performance of the hospitals

The meeting should be chaired by the SHA chief executive (or the executive director with responsibility for high security hospitals) and attended by the performance manager. The lead commissioner for the high security hospital should also be a member of this group.

The SHA should ensure that the high security hospital and provider Trust membership of the Quarterly Performance Review is of the appropriate seniority and disciplinary mix to ensure there can be comprehensive discussion in relation to performance and that there is authority for and ownership of the actions agreed.

Cluster Meetings

As part of the performance management function each SHA will lead a Cluster Group (or equivalent group). This group will meet at least quarterly.

Cluster group leadership is an SHA responsibility and as such cluster meetings must be chaired by the SHA chief executive (or the executive director with responsibility for high security hospitals). The purpose and core membership of the Cluster Group is set out in Appendix 5.

3.11 Performance Information

The Review of Security at the High Security Hospitals (2002) set out the importance of ensuring that the high security hospitals were subject to “robust and effective monitoring processes” and that a relevant and consistent suite of performance reports were agreed across all three hospitals.

SHAs will performance manage high security hospitals through a range of standard information sources such as:

- Quarterly performance report (see Appendix)
- Social care reports
- Workforce reports
- Equality reports
- Advocacy reports

SHAs must work collaboratively to ensure that the standards for reporting and those templates used are consistent across the three hospitals/SHAs in order that a meaningful comparison of performance can be achieved across the system. These reports should be reviewed periodically to ensure that the measures remain relevant and targets reflect the need for continuous improvement of services.

Performance managers will also use a number of other sources to ensure that services are improved and sustained. These include:

- Healthcare Commission audits and subsequent action plans
- Prison service audits and subsequent action plans
- Recommendations arising from external reviews and enquiries
- Recommendations arising from internal reviews and investigations
- Recommendations arising from major incidents
- Recommendations arising from table top exercises
- A log of Serious Untoward Incidents (SUI)
- A log of other issues (non SUI)

3.12 Incident and Issue Reporting

All NHS organisations are subject to local SHA policy in relation to the reporting, recording and management of Serious Untoward Incidents.

The Review of Security in High Security Hospitals (2000) pointed to the need for well defined processes for the reporting of information about events arising in high security hospitals. In 2007 in addition to SHA policy NOG agreed a national policy for high security hospitals 'Policy Framework for the Reporting and Briefing of Incidents and Issues in High Security Hospitals' (see Appendix 6).

SHAs are responsible for ensuring that the high security hospitals remain fully aware of local and national responsibilities for reporting and that amendment and revisions to policy are communicated and implemented.

The performance managers of all three SHAs will periodically review the consistency of high security hospitals with each other and with the national reporting policy.

The national reporting policy also sets out SHA responsibilities for the onward reporting and briefing of issues and incidents arising in high security hospitals. The SHA is responsible for ensuring that mechanisms are in place to ensure that those responsibilities are discharged effectively.

The performance managers of all three SHAs, in consultation with key national stakeholders, will periodically review the consistency of SHAs with each other and with the provisions of the national reporting policy.

Appendix 1

REVISED STRATEGY FOR HIGH SECURE COMMISSIONING ARRANGEMENTS

Key Features of the Revised Structure

- The three high secure commissioning roles will be brought together in one team
- The new 'National Commissioning Team' (HSCT) will be hosted by one Specialised Commissioning Group (SCG), the North West SCG, on behalf of the other nine SCGs and Wales
- There will be clear and robust mechanisms in place for commissioning the whole high secure system and explicit links between high secure commissioning and the rest of the secure specialised forensic system
- The HSCT will be accountable to the NSCG for high secure commissioning, so will be compatible with current NHS commissioning structures, and will also report directly to NOG, thus retaining Secretary of State's clear line of sight and powers of direction.
- In the event of any disagreements between NSCG and NOG, the Chairs of both bodies will be required to reach a resolution
- The performance management arrangements carried out on the Secretary of State's behalf will continue to be hosted within the relevant Strategic Health Authority for each high secure hospital. Strategic Health Authorities will continue to performance manage both the provider and the local commissioner to ensure that the Secretary of State's statutory obligations are met
- The performance of the HSCT overall, and the Director thereof will be performance managed by NHS North West in line with existing arrangements for the local performance management of the SCG
- The Director of the HSCT will be performance managed by the Chief Officer of the North West SCG who will be held to account through the North West SHA and the National Specialised Commissioning Group.

Appendix 2

THE SECRETARY OF STATE'S LICENSE FOR PROVIDING HIGH SECURITY HOSPITAL SERVICES

1.0 Background

The criteria for NHS Trusts to operate high security hospitals were set out in September 2000 by the Secretary of State for Health and remain the standard by which NHS Trusts are assessed by Strategic Health Authorities for the renewal of the license to operate a high security hospital.

2.0 The Criteria

- The provider must be an NHS Trust. Independent providers, including those who already provide medium security care, will not be allowed to provide high security services
- The NHS Trust must have a track record in the effective provision of secure services using physical, relational and operational security for patients detained under the Mental Health Act
- The NHS Trust must have a reputation for the provision of high quality medium security services
- The NHS Trust should be able to demonstrate that the provision of medium security services locally is fully integrated with general mental health services, including community mental health services (but not necessarily provided by the same NHS Trust)
- The NHS Trust must have a strong track record of sound strategic, financial and clinical leadership
- The NHS Trust must demonstrate a commitment throughout the organisation to clinical governance. This would be measured against the main components of clinical governance which were set out in 'A First Class Service', continuing professional development, full participation by all hospital doctors in audit programmes, ongoing programmes to disseminate evidence-based practice, implementing the clinical standards of NSFs and NICE, workforce planning and development fully integrated within the Trust's service planning, processes for ensuring the quality of clinical care integrated with the quality programme for the Trust as a whole
- The NHS Trust should have strong academic links. It should be approved for post-graduate training in all disciplines involved in the provision of comprehensive mental health services and it should have a track record in research and development activity

- The NHS Trust should have the physical capacity to develop a designated, separate high security facility
- The NHS Trust should have capacity in terms of staffing and resources to develop a high security service facility.

3.0 SHA Assessment against the License Criteria

The licence for operating high security hospitals is awarded to providers by the Department of Health.

The SHA is responsible for assessing the providers (or potential providers) of high security hospitals against the license criteria set by the Secretary of State (see Section 2) and making a recommendation to the Department of Health on the suitability of the organisation to provide (or continue to provide) such services. In doing so, the SHA may also outline any additional measures, risks or provisions necessary to provide the system with the necessary reassurance about the suitability of the provider to deliver the services.

4.0 Process

The SHA will write to the provider (or potential provider) requesting a formal submission that demonstrates the organisation's capability against each element of the criteria. The hospital should be encouraged, where it is appropriate, to provide real examples of how it can, has or continues to meet the criteria.

The SHA will convene a panel to review the submission against the criteria. The following groups/disciplines should be represented on the panel to ensure all elements of the criteria are fully addressed:

- Performance
- Commissioning
- Finance
- Clinical governance
- Security

The SHA will write to the Department of Health confirming the outcome and recommendation of the review panel.

Appendix 3

CRITICAL RELATIONSHIPS

1.0 SHA Performance Managers

The post of the performance manager has the potential to be isolated as a consequence of its distinctiveness, its remote working arrangements and its variation from core SHA objectives. This makes the connection between respective SHA performance managers and the support that they provide to each other vital.

By working together within both formal and informal infrastructures performance managers should be able to:

- Provide support to each other on issues in the respective hospitals
- Provide assistance to other SHAs in exceptional circumstances
- Facilitate joined up working and the development of consistent practice across the high security system
- Share learning and examples of good practice across the system
- Provide a system by which one performance manager can provide another with an informed but impartial perspective to a formal investigation, enquiry or audit
- Jointly develop national work programmes

2.0 SHA Performance Managers and the High Security Hospital

The relationship that the performance manager has with the high security hospital is critical to the successful performance management and development of services.

This relationship should be built on an understanding and acceptance of the role each plays in the maintenance of safe services and the preservation of the boundaries of responsibility.

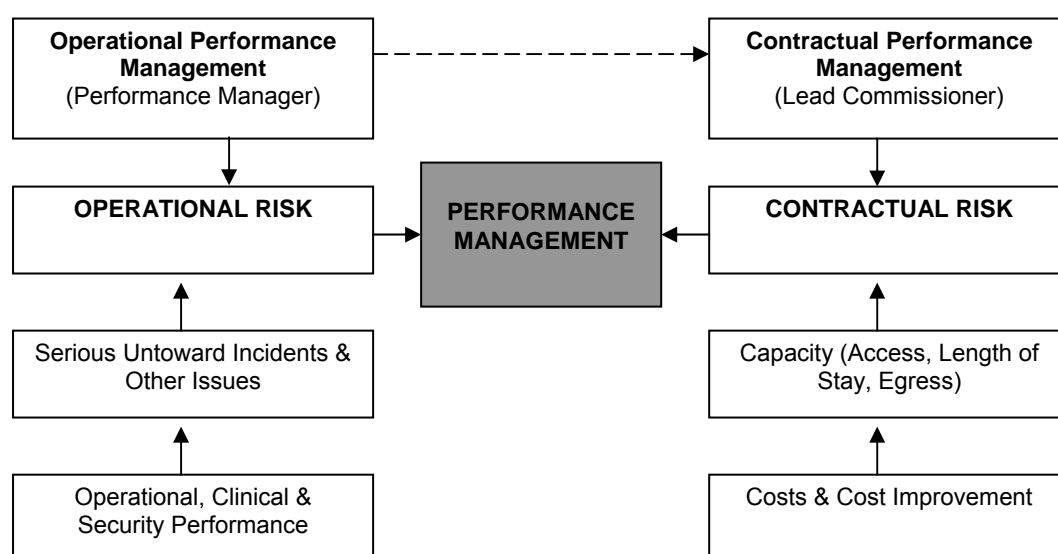
Where this relationship succeeds, there is an opportunity for each party to provide the other with a wider appreciation of the service. For the performance manager this might mean the opportunity to understand in far greater detail the dynamics of the hospital and the local issues that influence it. For the hospital it might provide a wider perspective on the development and direction of policy and the current political priorities in relation to the services.

The independent judgement of the performance manager can provide the hospital with a 'critical friend' perspective. However, it is essential that this is achieved whilst preserving clear boundaries and the ability, if necessary, for the performance manager to take the required courses of action to maintain the line of sight and the safety of services.

3.0 SHA Performance Managers and Commissioners

The importance of the relationship between the performance manager and the lead commissioner for the high security hospital can not be overstated.

SHA performance managers are responsible for the performance management of the local Lead Commissioner for high security services. The responsibilities of each are clear but it is the interface between those responsibilities that is critical to ensuring that the operational and contractual perspective is integrated to provide an overall picture of performance and risk.



The relationship can be illustrated by the example of capacity management. It is a commissioner responsibility to ensure that national capacity targets set for the service are met. However, it is the performance manager's responsibility to identify and reduce operational risk. A performance manager through knowledge of operational issues may consider that an operational area might be exposed to risk by the pressure of capacity. Only by the performance manager and commissioner working together and sharing information can a resolution be agreed that achieves both objectives.

4.0 SHA Performance Managers and the Department of Health

The performance manager has a clear line of accountability to the SHA. However, because of the specific arrangements in place for the policy and oversight of secure services within the Department of Health, performance managers may also receive guidance and instruction from the director of secure services at the Department of Health.

This relationship should not conflict with SHA responsibilities but strengthen them. The relationship between the performance manager and the Director of Secure Services should reflect central support of the SHA and provide for the Director of Secure Services to brief ministers on the stewardship of performance management and issues relating to the services for which they are responsible.

Performance managers will meet monthly with the Department of Health director of secure services in order to:

- Report on elements of the national work programme lead by individual performance managers
- Discuss key issues related to the high security system and agree consistent management strategies and responses
- Discuss key areas of risk relating to individual hospitals and the progress made in addressing such risks
- Provide performance managers with updates on national issues and the political climate surrounding secure services
- Provide the mechanism by which the Department of Health can seek and gain assurance about the SHA performance management of the services

5.0 Other Relationships

The SHA through the performance manager should also develop and maintain links with the broader range of groups relevant to high secure services. These include:

- National Oversight Group
- National Offender Management Service
- Welsh Assembly Government
- Ministry of Justice Mental Health Unit
- Secure Practice Forum
- DSPD Programme Board
- Prison Service
- Mental Health Act Commission
- Police
- Immigration Service

Appendix 4

QUARTERLY PERFORMANCE MANAGEMENT REPORT

The quarterly performance management report is available as a separate document.

Appendix 5

CLUSTER GROUPS

3.0 Purpose

The purpose of the Cluster Group meeting will be to:

- Bring together the key stakeholders responsible for patient access to, management within and egress from high secure services
- Take a whole system view of the services related to the high security hospital (including medium and low secure services)
- Improve and sustain performance in relation to forensic patient pathways and service delivery
- Discuss service developments and agree priorities for the allocation of any capital funding made available to the group
- Provide a mechanism to communicate national issues and developments to local stakeholders
- Provide a platform for local stakeholders to present relevant issues and developments in greater detail

4.0 Core Membership

The core membership of the Cluster Group should include:

- Host SHA chief executive or delegated executive director (chair)
- SHA performance manager
- Lead commissioner (representing the host specialised commissioning group for the respective high security hospital)
- Representative of the National High Secure Commissioning Team
- Lead commissioners for the specialised commissioning groups within the high security hospital catchment area
- High security hospital commissioning leads for the other two hospitals
- Executive director of the high security hospital

3.0 Frequency

The Cluster Group should meet at least quarterly

4.0 Documentation

The Cluster Group should be formally documented and the meeting minutes stored centrally by the SHA and copied to the National Oversight Group.



POLICY FRAMEWORK FOR THE REPORTING AND BRIEFING OF INCIDENTS AND ISSUES IN HIGH SECURITY HOSPITALS

ISSUE NO: 3
ISSUED: June 2007
REVIEW: June 2008 (or on implementation of other policy which affects this)
LEAD: Elizabeth Stevens (Elizabeth.Stevens@eastmidlands.nhs.uk)

This policy has been produced in consultation with the below organisations:

The Department of Health



National Offender Management Service



Welsh Assembly Government



East Midlands Strategic Health Authority



London Strategic Health Authority



North West Strategic Health Authority



Nottinghamshire
Healthcare NHS Trust



Mersey Care NHS Trust



CONTENTS

SECTION 1 INTRODUCTION

SECTION 2 SERIOUS UNTOWARD INCIDENT REPORTING

SECTION 3 REPORTING OF OTHER EVENTS & ISSUES

SECTION 4 COMMUNICATIONS & MEDIA

SECTION 5 INTERNAL ACTIONS TO BE TAKEN BY THE HIGH SECURITY
HOSPITAL

SECTION 6 INTERNAL ACTIONS TO BE TAKEN BY THE STRATEGIC HEALTH
AUTHORITY

SECTION 7 BRIEFING ISSUES BEYOND THE STRATEGIC HEALTH
AUTHORITY

SECTION 8 INDEPENDENT ENQUIRIES

SECTION 9 INTEGRATION WITH RELATED PROTOCOLS

APPENDIX ESSENTIAL CONTACT DETAILS

SECTION 1 - INTRODUCTION

Aim of the Framework

This framework aims to provide the infrastructure for ensuring the clear, consistent and co-ordinated communication essential for the effective management of Serious Untoward Incidents and other significant issues and events.

The framework covers Serious Untoward Incidents, other briefing issues, media handling issues and the infrastructures that both the high security hospitals and Strategic Health Authorities must have in place for the effective reporting, management and monitoring of reportable incidents and events.

Background to High Security Services

The Secretary of State for Health is required to provide high security hospital services under the National Health Service Act 1977.

High security hospital services in England are provided across a small network of three hospitals Ashworth, Broadmoor and Rampton. Each of the three hospitals is integrated within local NHS mental health services that operate under license from the Secretary of State to provide high security hospital services.

Patients detained within high security hospitals are those defined as having a high risk of posing a grave and immediate danger to others (if at large). Many also present a high risk of self harm and often demonstrate violent and/or difficult behaviour.

The hospitals have a prison category B equivalent security perimeter. The physical and procedural security policies are audited annually by the Home Office Compliance and Assurance Group.

Because of the unique nature of this patient group and the specialist security arrangements that are required it is necessary to have arrangements for the reporting and escalation of incidents and issues within high security hospitals in addition to existing Strategic Health Authority reporting policies.

Interested Parties

The legal requirement for the Secretary of State to provide these services ensures a high level of political interest. This close political interest is reflected in the establishment of a National Oversight Group (NOG) and specific line of sight arrangements for the performance management of high security hospitals through Strategic Health Authorities.

There is also a high level of public and media interest in the services provided by high security hospitals and in the patients they treat. Many patients have committed serious offences and some of the type that captures public curiosity.

Other parties that have a high stake in the services provided by high security hospitals include:

- The Department of Health
- The National Oversight Group
- National Offender Management Partnerships
- HM Prison Service
- Home Office
- Mental Health Act Commission
- Social Services

SECTION 2 – SERIOUS UNTOWARD INCIDENT REPORTING

Incident Categories

Incidents occurring in high security hospitals are categorised into:

Category A	Major Incident
Category B	Serious Incident
Category C	Untoward Incident
Category D	All other recordable incidents (i.e. Minor assault, verbal abuse etc)

Definition of a Serious Untoward Incident

A Serious Untoward Incident is defined as:

- An incident or accident when a patient, member of staff, or members of the public suffers serious injury, major permanent harm or unexpected death, (or the risk of death or injury), on hospital, other health service premises or other premises where health care is provided
- Where actions of health service staff are likely to cause significant public concern
- Any event that might seriously impact upon the delivery of service plans and/or may attract media attention and/or result in litigation and/or may reflect a serious breach of standards or quality of service.

All Category A incidents and Category B incidents qualify as a Serious Untoward Incident

Category A – Major Incident			
	Incident	Definition	Guidance
A1	Escape	Patient is absent without leave from within the hospital secure area	Escape having been confirmed following search of site
A2	Absconsion	Patient is no longer in escorted custody during escorted leave of absence	A patient driven separation from escorting staff where staff lose sight of and/or effective supervision of the patient for a period greater than 5 minutes
A3	Hostage taking	An individual / group is held by captor/s	Within a static location or mobile
A4	Serious sexual assault	This may include an allegation of rape, where genital, oral or anal penetration by part of accused body or by an object using force and without the victim's consent	Where it is immediately reasonable to determine that a sexual assault has/may have taken place necessitating immediate police forensic and investigative involvement
A5	Major concerted indiscipline	A disturbance involving two or more patients resulting in violence, damage or destruction	E.g. sit in protest involving violent behaviour, group assault, barricade where multiple patients may be involved etc.
A6	Roof top disturbance	Where more than one patient is on the roof for any length of time <u>or</u> where one patient is on the roof for over 30 minutes	
A7	Major fire	Major fire leading to widespread loss of property or considerable spread of fire from source of ignition	Requiring action from the Fire Service to control. Fire spread may be from one building to another or causing significant disruption to service/s - e.g. fire in Control Room
A8	Major loss of service	Unplanned loss of buildings or services or loss of service causing major disruption	Loss of ability to maintain security and/or deliver patient care e.g. loss of control room / reception / IT / Ward/s / no alternative accommodation / significant staffing shortage and there is reference to contingency/business continuity plan
A9	Major key compromise	The permanent or long term compromise of any personally allocated or centrally controlled security key	E.g. the loss or theft of staff personal security keys that results in the need for total or partial re-locking of hospital
A10	Death	Unexpected or expected	Where potential suicide, homicide or

			as a result of a known or unknown physical condition
--	--	--	------------------------------------------------------

Category B – Serious Incident

	Incident	Definition	Guidance
B1	Attempted escape	Failed or prevented attempt to breach the secure perimeter	An assault on the secure perimeter which demonstrates an intent to escape
B2	Attempted absconsion	Patient attempts to leave the custody of the staff during an escorted leave of absence	Any patient driven attempted separation from escorting staff where effective supervision and control may not be lost but <i>if</i> lost for a period of less than 5 minutes
B3	Attempt to take a hostage	An attempt to hold an individual / group by captor/s	Where a clear attempt at hostage-taking has been thwarted by intervention
B4	Attempted serious sexual assault	A failed/thwarted attempt to seriously sexually assault another individual OR a retrospective claim of a sexual assault where there is no immediate evidence	Where the event is reportable to the Police
B5	Concerted indiscipline	A non violent protest by multiple patients	E.g. a sit in protest but where there is no violence or damage/destruction caused.
B6	Roof top protest	A roof top incident involving only one patient	Where there is no significant damage and where the incident lasts less than thirty minutes
B7	Serious Fire	Fire at any part of the hospital that causes damage	That requires action from the Fire Service. May cause some disruption to service provision but not requiring the removal of patients
B8	Serious disruption to service	The partial loss or significant restriction of buildings or services	Where temporary additional operational controls or contingency / business continuity plans are required
B9	Key compromise	The short term loss of any personally allocated or centrally controlled security key but where it is subsequently found	Where the re-locking of the full hospital is not required but may be required for a small area
B10	Key making	Evidence of attempts to make any type of key	

B11	Attempted suicide	An attempt which has been assessed by clinical staff as genuine by a patient to take their own life	Where as a consequence the patient may require a significant level of local intervention and/or may require medical treatment outside the high security hospital perimeter
B12	Serious self harm	Where it has been assessed that there was not a deliberate attempt to commit suicide but where deliberate self injury has been caused to the body requiring significant intervention or medical treatment	Where the immediately requires a significant level of local intervention and/or requires medical treatment outside the high security hospital perimeter
B13	Serious assault	Assault with weapon or sustained attack where there is the clear potential to seriously injure or endanger life	Where as a consequence the victim may require a significant level of local intervention and/or may require medical treatment outside the high security hospital perimeter
B14	Serious accident or injury	Any event that results in injury or ill health or harm	Where as a consequence the injured person may require a significant level of local intervention and/or may require medical treatment outside the high security hospital perimeter
B15	Unexplained serious injury	Serious injury to a patient which cannot be readily explained	Where as a consequence the patient requires a significant level of local intervention and/or requires medical treatment outside the high security hospital perimeter
B16	Room barricade	An attempt by a single individual to prevent others entering a room or area by constructing/ placing a significant barrier	Furniture or items placed in such a way it requires dismantling to gain access/egress and control
B17	Weapon making	The discovery of weapons or evidence of weapon manufacture	Weapons may be 'home-made' or otherwise
B18	Security breach	A serious failure of perimeter security or a failure of internal security where patient/s have taken advantage of that failure	E.g. where a perimeter gate left unlocked although there is no breach or where an internal security door is door left open and a patient moves uncontrolled
B19	Illicit substances	Supply or use of illicit / restricted substances such as classified drugs, alcohol, etc.	Where classified drugs are found or where there is evidence of use/dealing within the hospital. (This does not include positive drug testing at admission)
B20	Serious allegations against staff	Any serious allegation against staff related to their behaviour	May include allegations of abuse or neglect, fraud or inappropriate

		or care of patients	behaviour requiring further investigation
B21	Serious medication error	Wrongful administration of medication which has a significant impact on the patient and has the potential either to do irreparable harm or to be life threatening	Patient requires medical treatment or intervention or is hospitalised
B22	Serious breach of confidentiality	Breach of patient or organisational confidentiality	Where this is done either intentionally or unintentionally
B23	Loss of data	Permanent loss of clinical and/or organisational information	Where no back up exists

Category C – Untoward Incident			
	Incident	Definition	Guidance
C1	Assault	Without a weapon	Where the injury is such that no treatment is required or minor treatment (i.e. first aid) can be given on site as required. Any RIDDOR reportable assault which does not fall into Category B
C2	Medication error	The incorrect prescribing / dispensing / administration of medication to a patient	Where the administration was unlikely to cause irreversible side effects and/or where no treatment is required
C3	Sexual assault	Inappropriate touching / grabbing of sexual areas	This may include an alleged sexual assault with no evidence and is not pursued by the police. (May be up-graded later)
C4	Accidental / intentional damage to property	Where it is assessed that there was no intention to cause serious damage and or where any damage was low value	Flood or other unforeseen catastrophe not requiring the removal of patients or staff to another area but there may be some disruption to service and significant cost
C5	Sudden deterioration of physical health	Assessed as a natural medical emergency	Which requires emergency admission to another hospital for treatment outside the perimeter of the high security hospital
C6	Fire	Quickly contained or extinguished within immediate area or room.	Insignificant damage with no loss of service. Not necessitating any action from the Fire Service (even if emergency call placed)
C7	Minor disruption to services	A partial loss or restriction of buildings or services which does not have a significant impact	Where normal controls and operating procedures can be used and contingency plans are unnecessary
C8	Other substance misuse	A patient in possession of or under the influence of non illicit but other unsafe substances (such as glue) or medication prescribed for another patient	Where prescription drugs are found or where there is evidence of use within the hospital. (This does not include positive drug testing at admission)
C9	Moderate / minor harm to self	Where it has been assessed that there was not a deliberate attempt to commit suicide but where deliberate self injury has been caused to the body	Where the injury is such that no treatment is required or minor treatment (i.e. first aid) can be given on site as required.

C10	Accident or injury	Any unplanned event that results in injury or ill health or harm	Where any injury is such that no treatment is required or minor treatment (i.e. first aid) can be given on site as required
C11	Unexplained injury	Injury that cannot be readily explained	Where the injury is such that no treatment is required or minor treatment (e.g. first aid) can be given on site as required.
C12	Key compromise	Loss of any other locally controlled key (i.e. not personally allocated or centrally controlled security key) even if it subsequently found	e.g. medicine keys / toll cupboard keys / pharmacy keys
C13	Security breach	Any security breach not covered in Categories 'A' and 'B'	e.g. Internal door left unlocked but where no patient takes advantage of the situation
C14	Threats	Any threats to take hostage / kill / escape / abscond	Any evidence of verbal or written threats
C15	Attempt to flee from staff or locked area	A patient makes an attempt to flee from a locked area or escort within the secure perimeter	E.g. a locked ward or day care or run away from an escort. Any attempt breach the perimeter will be classified as B1
C16	Security Compromise	A compromise of security or operational policy not of the seriousness as reportable as a Category B incident but with the potential to have resulted in a category A/B incident	E.g. Internal door left unlocked but no patient takes advantage, minor breach of hospital policy.

Responsibilities for Reporting a Serious Untoward Incident (SUI)

The high security hospital is responsible for informing the Strategic Health Authority (SHA) of all reportable incidents.

Foundation Trusts are required to continue to report all SUIs to the SHA until national agreement has been reached with the Office of the Regulator for Foundation Trusts.

Reporting Timeframes and Methods

Category A Major Incident

Category A incidents are reportable to the SHA **immediately** firstly to the SHA Director on call arrangements (see essential contact details).

The hospital should also contact the High Security Policy & Performance Lead

Category B Serious Incident

Category B incidents are reportable to the SHA **within 1 working day** firstly to the High Security Hospital Policy & Performance Lead (see essential contact details)

Category C Untoward Incident

Category C incidents do not need to be reported to the SHA **unless** they fall within the guidelines for reporting of other incidents and events (Section 3) in which case they should be reported **within 1 working day**

The high security hospital must also inform its Lead Commissioner of a reportable incident within the same timeframes above in order to:

- Inform future commissioning discussions
- Ensure that questions from the public and or media can be managed appropriately
- Ensure any relevant remedial action is made as soon as possible
- Ensure appropriate engagement in a joint investigation

Lead Commissioners are responsible for briefing their local commissioners.

Police Investigations

If the police are involved in any SUI and place restrictions on hospital investigations this should be clearly documented in the SUI report and in reports to the SHA.

Confidentiality

This reporting system follows the NPSA model and encourages openness, trust and continual learning based on the Caldicott Guardian principles, which are already in place to safeguard patient confidentiality throughout the NHS. To this end reporting from the hospital will be anonymous, with the provision that there is an audit trail on a 'need to know' basis. This means that should SHA consider the SUI to be of a nature where patient (and practitioner) identifiable information is necessary in order to protect patient safety the service will be asked to release this information. The data protection act will be adhered to at all times.

STEIS

The high security hospital is responsible for ensuring that all SUIs are reported through the STEIS reporting system.

SECTION 3 – REPORTING OF OTHER EVENTS & ISSUES

Interested parties require regular information from and reassurance about the arrangements within high security hospitals. Such requests for information often relate to security and safety arrangements in the hospital and the operational procedures that support those arrangements being effective.

Incidents or issues are likely to arise within high security hospitals that may not constitute that reportable as a SUI but that should be 'briefed up' anyhow. Such briefings should be made to the SHA High Security Policy and Performance Lead. The SHA High Security Policy & Performance Lead will decide upon any onward briefing that may need to occur.

Such briefing of other events or incidents may most often be achieved verbally but must always be summarised by the hospital following the briefing by email or writing to provide an auditable trace of events.

Briefing up, and the choice about what to brief up, relies upon the hospital being attuned the anxieties of the public or current interests and priorities of others such as the national press, the SHA, the Department of Health and Ministers. These issues will vary over time with public mood and political agenda requiring the high security hospital to be cognisant of the current external climate and to respond to it accordingly.

Examples of other events and issues include:

- Legal challenge to the hospital or that which may also challenge national policy
- Press enquiries of a significant or particularly sensitive nature
- A series of lower level incidents that together form a 'cluster' worthy of further investigation
- Requests for information under the Freedom of Information Act relating to highly sensitive material or activities
- Positive experiences and successes of the hospital
- The trial or movement of a high profile patient
- Indications of actions or issues that may result in a SUI
- Issues relating to the management plans of particularly difficult, challenging or high profile patients
- Significant changes to working practices, arrangements or the organisation of the hospital

Briefing up is about building understanding, sharing risk and creating confidence in the high security system through open communication and transparency.

SECTION 4 – MANAGING COMMUNICATIONS & MEDIA

Communication is a vital element to supporting and delivering effective management. Communications for internal, stakeholder, patient, staff and media relations should be an integral part of the whole process of managing a SUI or other significant issue/event at every level.

Emergency Communications Room

Some serious events may generate sufficient interest from external stakeholders as to warrant the implementation of dedicated information lines to manage call volumes.

The high security hospital must have policies in place which ensure the swift implementation of such a facility and the effective operation of the unit. This should include a provision the appropriate levels of IT and telephony equipment.

All such communications from the emergency communications room must be documented in detail.

Media Relations

A SUI, significant event or alleged event at a high security hospital can lead to an intensive degree of media attention both at a local and national level. Media coverage can continue beyond the event and for long periods, sometime years, and are re-ignited as investigation reports are generated from the incident, or as other related incidents occur elsewhere.

Unplanned or media coverage that an organisation is unprepared for can in itself constitute an untoward incident. In such cases the high security hospital Communications Lead must liaise with the SHA Head of Communications and the SHA High Security Policy & Performance Lead in order to agree handling and reporting strategies.

The high security hospital must have a media relations policy in place which addresses the appropriate action to be taken in relation to:

- Serious Untoward Incidents, including protocols with other local organisations and agencies on media handling and strategies for ongoing and longer term management of media coverage
- Requests for significant and/or sensitive information from the press or media

The high security hospital Communications Lead will work closely with the SHA High Security Policy and Performance Lead and the SHA Head of Communications in agreeing appropriate media handling strategies.

The SHA High Security Policy and Performance Lead is responsible for briefing SHA Executives, the Department of Health, the Home Office and other affected parties as appropriate.

The SHA Head of Communications is responsible for briefing the Department of Health Communications Team and the Ministerial Briefing Unit as appropriate.

Interaction with Other Press Offices

Press issues that relate to national services, pilots or particular areas of political interest may require a co-ordinated response from a national press office such as the Department of Health or Home Office. Where this is the case the SHA High Security Policy and Performance lead will advise the high security hospital Communications Lead.

In such cases, the high security hospital will not issue statements to the press, media, public or any other body without that proposed statement having been approved by the co-ordinating press office.

Requests for Information via Freedom of Information Act

The high security hospital should advise the SHA High Security Policy and Performance Lead of any significant requests for information under the Freedom of Information Act where:

- the disclosure of the information might attract press or general public interest or,
- it might be reasonably assumed that the information request will also be submitted to other high security hospitals.

Forward Planning

The high security hospital must have in place processes to identify, record and report future known or predicted events that may attract public and/or press interest. These events might include:

- Trial dates of high profile patients
- Publication of external reviews or enquiries
- Anniversaries of significant events or index offences of high profile patients

SECTION 5 – INTERNAL ACTIONS TO BE TAKEN BY THE HIGH SECURITY HOSPITAL

The high security hospital will have in place the following:

- A policy and procedure clearly stating how Serious Untoward Incidents will be managed within the organisation
- Processes for reporting the event to other local agencies, e.g. police, local authority
- A system that records all incidents
- A forward planning system to highlight future events which require briefing or media preparation
- A process for copying the incident form to key stakeholders using discretion with regard to the nature and location of the incident
- Mechanisms to ensure appropriate action is taken and referrals are made as necessary using the cause for concern process, the General Medical Council and the Nursing, NCAA, HSE etc
- Arrangements for ensuring that investigations and root cause analysis take place as appropriate
- Arrangements for ensuring that staff receive appropriate support following Serious Untoward Incidents
- A system to ensure that follow-up reports are obtained and distributed
- A process for establishing and approving terms of reference for investigations
- A process for the review and sign off investigation reports
- A process for the monitoring of action plans
- A Serious Untoward Incident monitoring group

Serious Untoward Incident Monitoring Group

The group should meet on a no less than quarterly basis to discuss incidents that have occurred in the intervening period. The group should analyse all incidents and identify trends.

The Serious Untoward Incident Monitoring Group should suggest remedies and ensure corrective action is implemented and that such action leads to reduced risks.

Investigations

All Category A incidents and some Category B incidents will require a formal internal investigation to be completed by the high security hospital.

The Terms of Reference for such investigations should be agreed with the SHA prior to commencement.

The investigation should be systematically conducted to examine underlying causes and learn how to prevent incidents from happening again.

The 'product' of an investigation is the Investigation Report (see below) and Action Plan (see below). Both these documents should accurately describe the investigation process including tools and techniques used, the findings, recommendations and consequent actions.

Investigation Reports

The investigation report may need to be shared with other stakeholders. Therefore the content and format of the report should withstand external scrutiny.

Stakeholders might include:

- Patients and families
- Coroners Office
- Strategic Health Authority
- Commissioners
- NHS Litigation Authority
- Solicitors
- Department of Health
- Internal staff

The names of patients or staff involved in the incident should not be contained within the body of the report. Reports should be written in a way that describes who the person is and what their role is, without using names, e.g. the patient, the wife, Dr A, Nurse B etc.

The report must:

- State who the authors/ investigation team are
- Be dated
- Have page numbers
- Have a contents page

Body of report must contain:

- Summary (Background including relevant medical, psychiatric or social history, details of incident and findings)
- Process of investigation and methodology (Documentation reviewed, interviewers, interviewees, tools and techniques used to identify root causes)
- Chronology of events (tabular timeline to include appropriate details)
- Analysis and findings (Include: what went well & areas of good practice care and service delivery problems identified, contributing factors)
- Recommendations (Solutions to prevent recurrences, based on analysis and findings)
- Appendices (List of documents reviewed, Root Cause Analysis tools; timeline, fishbone diagrams etc)

Action Plans

Where as part of the learning from a SUI or other event, there are actions to be taken. These should be reflected in an action plan.

The high security hospital must share the action plan with the SHA High Security Policy and Performance Lead and provide regular updates on progress.

At the outset of the commencement of the action plan, the following must be defined:

- Who has commissioned the action plan
- Who will monitor the implementation of the action plan
- How often the action plan will be reviewed
- Who will sign off the action plan when all actions have been completed

The action plan must contain:

- Recommendations/issues
- Action agreed
- Person responsible for the action (identifying the individual, department and organisation)
- By when
- Record of activity/progress towards completion
- Indication of actions complete and those outstanding

Record Keeping

Following a SUI or other significant event the high security hospital must make a contemporaneous record of the incident as soon as possible. This will be particularly relevant where a police or internal investigation may be required.

SECTION 6 – INTERNAL ACTIONS TO BE TAKEN BY THE SHA

The Strategic Health Authority will have in place:

- A log of all Serious Untoward Incidents to monitor trends and progress towards resolution of issues
- A log of all non SUI briefed issues to monitor trends and progress towards the resolution of issues
- A log of all action plans being managed and monitored by the high security hospital
- A log of all ongoing police investigations related to serious issues/incidents to ensure serious offences of patients or staff are appropriately and swiftly investigated and if appropriate, prosecuted
- Mechanisms to ensure that onward and upward briefing can be effected immediately
- Clear lines of responsibility for briefing up to include leave cover
- A structure of internal and high security hospital meetings to discuss progress towards the resolution of issues and review incident related management information produced by the high security hospital.

Structure of Internal and External Review Meetings

The following meetings will take place to review issues and trends:

Meeting	Frequency	Membership
Internal review of SUI and non SUI issues	Monthly	SHA Responsible Executive SHA HS Policy & Performance Lead
Formal review of SUI and non SUI issues	Bi - Monthly	SHA HS Policy & Performance Lead Lead Commissioner Executive Forensic Director
Review of High Security Hospital Incident Statistics	Quarterly KPI Meeting	SHA Responsible Director SHA HS Policy & Performance Lead Lead Commissioner Executive Forensic Director Other appropriate parties

SECTION 7 – BRIEFING BEYOND THE SHA

As a consequence of the high level of public and political interest in the services provided by high security hospitals there is a requirement for senior officials and Ministers to be notified of significant issues or incidents occurring at a high security hospital or of any other issue which might affect or generate adverse attention in high security hospitals.

Responsibilities

The SHA High Security Policy & Performance Lead will discuss issues arising with the SHA Responsible Director and a decision will be taken on any further briefing that may need to occur outside the Strategic Health Authority. In the absence of the Executive Director, the High Security Policy and Performance Lead will make the decision.

The SHA High Security Policy & Performance Lead has direct access at any time to the SHA Chief Executive on matters relating to high secure services

The SHA High Security Policy and Performance Lead is responsible for the briefing of all stakeholders.

The SHA Communications Lead will liaise with the SHA High Security Policy & Performance Lead and the high security hospital Communications Lead and send any MB Alerts to the Ministerial Briefing Unit and the Department of Health Media Desk.

The Principle of Briefing Up

For some issues/events the requirement to brief up will be clear. However, similarly to the briefing of 'other' issues from the high security hospital to the SHA, the choice about what to brief up will sometimes rely upon the Strategic Health Authority being attuned the anxieties of the public or to current interests and priorities of others such as the national press, the Department of Health and Ministers. These issues will vary over time with public mood and political agenda requiring the Strategic Health Authority to at all times to be cognisant of the current external climate and to respond to it accordingly.

In cases where there is doubt about whether an incident requires a Ministerial Briefing, the SHA High Security Policy and Performance Lead will seek advice from the Department of Health National Policy Lead.

In cases where there is doubt about whether an incident should be escalated to the Department of Health National Policy Lead the decision should always to be brief.

Minimum Briefing Up Standards

(See Section 2 – Serious Untoward Incident Reporting and Section 3 – The Reporting of Other Events & Issues for wider definitions of issues/events)

		Category A	Category B	Issue/ incident likely to create media interest	Legal Challenge (hospital or national policy)	Media interest in high profile patient or services	Significant FOI requests
SHA	CEO	√	√	√	√	√	√
	Accountable Director	√	√	√	√	√	√
	Lead Commissioner	√	√	√	√	√	√
	Communications	√		√	√	√	√
	Other SHA Performance Leads	√	√	√	√	√	√
DH	National Policy Lead	√		√	√	√	√
	Central Team	√		√	√	√	√
NOMS	Director General	√					

Other Parties to Include in the Circulation of Briefings

The following parties must be copied in the circulation of briefings:

- Secure Psychiatric Services Team - Department of Health
- Responsible SHA Executive
- Relevant Commissioning Lead
- SHA Communications Team
- High Security Hospital Communications Team
- Executive Forensic Director at the High Security Hospital

In the case where an issue/incident concerning a Wales catchment patient is briefed up to the Department of Health, the Department of Health will forward that briefing to the equivalent responsible department in the Welsh Assembly Government for information.

In the case of an issue/incident occurring in or affecting the DSPD (Dangerous & Severe Personality Disorder) pilot or service:

- DSPD Program Director
- DSPD Department of Health Central Team Lead

Depending upon the nature of the event or issue, consideration should also give to circulating the briefing to further parties that might be affected:

- Director General – Health & Offender Partnerships
- SHA High Security Policy & Performance Leads
- Commissioning Leads for other high security hospitals
- Communications Teams for other high security hospitals
- On call executive directors (SHA & high security hospital)

Method of Briefing

The SHA High Security Policy and Performance Lead should brief up as soon as a decision has been taken to do so but at least within 1 working day. A standard brief should be comprehensively but succinctly completed and emailed to the parties above.

If it is not practicable for the immediate generation of a written brief, the SHA high Security Policy & Performance Lead will contact all parties by telephone or email immediately and follow up with the written brief within a further working day.

Records

The SHA will maintain a secure, electronic and comprehensive record of all briefings generated by the SHA.

SECTION 8 – INDEPENDENT ENQUIRIES

Criteria for Commissioning an Independent Enquiry

In the context of high security hospitals and NHS guidance, the Strategic Health Authority is responsible for commissioning an independent inquiry in the event of:

- A homicide
- A violent incident, (not resulting in homicide) but where it is judged by the SHA and the high security hospital that an independent inquiry process would be in the interest of public accountability and/or establish further understanding of and learning from the incident
- When the SHA determines that an incident or event warrants an independent investigation

And in each case when:

- legal proceedings have been concluded, including any appeal processes
- an internal inquiry and investigation has been completed by the high security hospital

Recommendations for the commissioning of an independent inquiry will be made to the SHA Executive Management Team following consultation with the Chief Executive, the Director of Public Health and the high secure hospital.

The Purpose of an Independent Enquiry

The purpose of an independent inquiry is to secure the future safety of patients and the public through the translation of learning into improved practice. It is neither a legal or disciplinary process and is not a process that seeks simply to apportion blame.

Public interest must be served by the inquiry process therefore openness and transparency is essential. However, the NHS has a duty to maintain and protect the rights of patients and their families to confidentiality. An independent inquiry must fully explore all of the relevant facts, documents and records without compromising those rights.

High secure hospital Independent inquiry proceedings will usually be held in private. However, in the event of significant public interest, or where there is deemed to be no possible breach of confidentiality e.g. in circumstances where the inquiry panel will be considering only information and documentation which is already in the public domain, the SHA will commission an inquiry to be conducted in the public arena

Panel Membership

The SHA will appoint a Chair with extensive experience of conducting inquiries and who also meets the criteria for panel members.

Panel members should have:

- Previous experience of participating in inquiries or with auditing agencies e.g. Mental Health Commission
- Experience of the issues that are likely to be raised
- Independence from the circumstances of the incident under inquiry and from the high secure hospital
- personal credibility and authority

In addition, other specialist members should be selected based on:

- their specialist knowledge of relevant security, treatment, care, research or service provision
- their experience in providing “expert” testimony to previous inquiries or legal proceedings
- their professional experience particularly with relevance to security, clinical governance, standard setting and developing good practice

Terms of Reference

The SHA will ensure that all members of the inquiry panel understand their remit and of the depth of the inquiry.

The Terms of Reference will include:

- A statement on openness and whether the inquiry is to be held in public or private
- A statement on the independence of the inquiry and the role of the SHA in commissioning it
- The parameters of the inquiry

The Terms of Reference will be agreed with:

- The SHA Executive Management Team
- The inquiry panel Chair

Management and Accountability

The SHA will oversee the inquiry and appoint an individual to ensure that the following actions are taken:

- Recruitment and selection of the inquiry panel
- Development of a project plan in liaison with the chair
- Providing advice and support to the inquiry panel including, updating the panel on health service policy and procedures
- Ensuring the panel investigation and analysis uses Root Cause Analysis techniques
- Arrangement of the inquiry schedule, including visits to other establishments e.g. prisons

- Ensuring all appropriate documentation is available including, preparation of background papers, which should include a chronology of events - Trust Liaison manager
- Obtaining consent to access medical and health records, including criminal records where relevant
- Ensure that all interviews undertaken by the panel are recorded at the time and transcripts shared with the interviewee for factual accuracy/clarification
- Ensure all panel meetings are recorded and notes available for panel use and external scrutiny if required
- Ensure that drafts of the report are shared with the high secure hospital to check for factual accuracy, points of clarification
- Ensure that the panel chair meets with the trust CEO to discuss the initial findings of the review at draft stage and provide opportunity for identify any issues relating to factual accuracy
- Liaison with Directors of the SHA/ Department of Health and other stakeholders providing regular progress reports
- Acting as a point of contact for all aspects of the inquiry

The Draft Report

Although the inquiry panel acts independently of the commissioning organisation, as the commissioner of the inquiry, the SHA should expect to preview the report at final draft stage and before final completion of the report.

The SHA will decide at this point if any other agencies should be made aware of the report's contents prior to publication, and will discuss this with the inquiry panel Chair. The SHA share the draft report with the Department of Health.

In cases where a draft report levels criticism at an individual witness, the inquiry panel should circulate the relevant sections of the report in draft form to allow an opportunity for discussion with the panel.

The panel chair should meet with the Chief Executive of the high secure hospital to share initial findings and provide the Trust with opportunity to comment on factual accuracy.

The Final Report

The final report should:

- Give an account of the incident, draw conclusions and make recommendations
- Conform to the NHS corporate identity standards in terms of presentation and content
- Objective, written in a non emotive style and based on evidence

The final report of the inquiry is provided by the panel to the SHA. The SHA will then ensure that the report is effectively distributed to the agreed recipients.

As soon after completion of the final report as possible, the enquiry findings and recommendations will be reported to the SHA Board, the Department of Health, Lead Commissioner and the high secure hospital. Through these processes each Board

will consider its response to the findings and recommendations of the report and agree the actions to be taken as a result.

The SHA will brief key stakeholders on the report and the process for publication before ensuring the report is disseminated effectively to agreed organisations and access points with an interest in its findings and recommendations.

SECTION 9 – INTEGRATION WITH RELATED PROTOCOLS & AGENCIES

Informing Other Agencies

This framework does not replace the duty of the high security hospital to inform other authorities and organisations where appropriate. Specific national guidance governs certain types of incidents e.g. homicides and other serious incidents involving mentally ill people (HSG 94, 27) and arrangements for dealing with major incidents (HSC 98,197).

Related Protocols

A number of other protocols also relate to the management of Serious Untoward Incidents and significant events, which should be followed as appropriate in individual cases.

These may include:

- The SHA general Serious Untoward Incident Reporting Policy
- The SHA on call reporting and escalation procedure
- Child protection procedures in respect of children who have been or are suspected of being abused
- Vulnerable adults policies
- The notification and management of infectious disease outbreaks
- The management of bed crises
- NHS Complaints Procedure
- Major Accident/Event policies
- Other SHA expectations for reporting professional conduct issues

APPENDIX

ESSENTIAL CONTACT DETAILS

Rampton Hospital (Nottinghamshire Healthcare NHS Trust)		East Midlands Strategic Health Authority	
Executive Forensic Director	01777 247 301	High Security Policy & Performance Lead	0115 968 4405 / (07887 626 399)
Duty Manager (on main hospital reception 24 hrs)	01777 248 321	Responsible Director	0115 968 4405
Communications Department	0115 993 4529	NHS East Midlands Director on call (Out of Hours for Category A incidents)	08700 555 500 Call group code NHSEM1
		Lead Commissioner	0115 912 3344 ext' 49391/ 07876 740 344

NB: All major Incidents should be reported to the SHA Director on call immediately

ESSENTIAL CONTACT DETAILS

Broadmoor Hospital (West London Mental Health NHS Trust)		London Strategic Health Authority	
Executive Forensic Director and Associate Director	01344 754 050 01344 754 250	High Security Policy & Performance Lead	020 7391 6223 / 07768 553 838
Site Manager (via main hospital Control 24 hrs)	01344 754 500	NHS London Director on call	08700 555500 Call group code NHS01
Duty Manager (off site)	01344 754 500		
Communications Department	In Hours 020 8354 8847 or 01344 754 292 Out of hours Via hospital control	Lead Commissioner	020 7756 2638 / 07736 666 727

NB: All major Incidents should be reported to the SHA Director on call immediately

ESSENTIAL CONTACT DETAILS

Ashworth Hospital (Mersey Care NHS Trust)		North West Strategic Health Authority	
Executive Forensic Director	0151 471 2237	High Security Policy & Performance Lead	0161 237 2598 & 07786 390 089
Duty Manager (on main hospital reception 24 hrs)	0151 471 2235	Responsible Director: Director Out of Hours on Call	0161 237 2900 & 07917 776840 0161 223 4732
Communications Department	0151 471 2336	Comms Director on call Director on call (Out of Hours for Category A incidents)	07966 937133 07966 937133
		Lead Commissioner	01244 389269 / 07776 183627

NB: All major Incidents should be reported to the SHA Director on call immediately

Appendix 7

PERFORMANCE MANAGEMENT ISSUES SPECIFIC TO WALES

5.0 Background

The National Health Service (Wales) Act 2006 places a duty on Welsh Ministers similar to that of the Secretary of State for Health in England for the provision of accommodation and services for patients detained under the Mental Health Act 1983.

Currently there are no high security hospital services in Wales and Welsh health commissioners procure services from England (Ashworth, Broadmoor & Rampton hospitals). For the purposes of catchment design, Welsh patients fall within the catchment of Ashworth Hospital but Wales also utilises Rampton Hospital in respect of national services (Women, LD, Deaf & DSPD).

Wales is also represented as a key stakeholder at the National Oversight Group.

6.0 Issues that Require a Specific Approach for Wales

2.1 Reportable Serious Untoward Incidents Involving Welsh Patients

As per the National Reporting Policy (Appendix 6) those Serious Untoward Incidents that require briefing to the Department of Health by Strategic Health Authorities (see page 22 – Minimum Briefing up Standards) should also be briefed in respect of Welsh Patients to the equivalent Welsh department. The Department of Health Policy Team will brief the Welsh Assembly Government Mental Health Policy Team immediately following incidents being reported to them.