The Shrewsbury and Telford Hospital NHS Trust

Board of Directors' Meeting: 12 October 2023

Agenda item		Report in Supplementary Information Pack		
Report Title		Annual Security Report 2022-23		
Executive Lead		Sara Biffen, Acting Chief Operating Officer		
Report Author		Jon Simpson, Trust Security Manager		
CQC Domain:		**Link to Strategic Goal:**		**Link to BAF / risk:**
Safe	√	Our patients and community	√	BAF1, BAF2, BAF3, BAF8
Effective	√	Our people	√	
Caring	√	Our service delivery	√	**Trust Risk Register id:**
Responsive	√	Our governance	√	312, 326, 325
Well Led	√	Our partners	√	
Consultation Communication		2023.06.08: Health, Safety, Security & Fire Committee 2023.10.04: Audit and Risk Assurance Committee		
Executive summary:		In accordance with the provisions of the NHS Violence Prevention & Reduction Standard[1], NG10[2], Mental Health Units Act[3] and national emergency preparedness standards[4] Providers are required to have in place and maintain security management arrangements in their organisations. The attached annual security report provides information on reported security incidents, security team activity and other security management work across the Trust in 2022-23.		
Report Recommendations:		The Board is asked to note the contents of the Annual Security Report.		
Appendices:		Appendix 1: Annual Security Report 2022-23		

[1] NHS (Social Partnership Forum) Violence Prevention & Reduction Standard (December 2020).
[2] NG10: Violence and aggression - short-term management in mental health, health, and community settings (**28 May 2015).**
[3] Mental Health Units (Use of Force) Act 2018.
[4] Emergency Preparedness & Resilience Response (EPRR) Standard No 21 (Lock Down).

The Shrewsbury and Telford Hospital NHS Trust

Annual Security Report

2022-23

Foreword

The Shrewsbury and Telford Hospital NHS Trust is committed to ensuring a safe environment for staff and patients so that the highest possible standard of care can be delivered; to this end security remains a key priority within the development and delivery of health services. All of those working within the Trust have a responsibility to assist in preventing security related incidents or losses. This approach underpins and directly links to the Trust's values and objectives.

Sara Biffen Acting Chief Operations Officer (COO) was the designated Board level Director responsible for security management matters during the reporting period that this report covers, including prevention and reduction of violence and aggression towards NHS staff, and ensuring that there is adequate security management at the Trust.

Sheila Fryer, Deputy Chief Operating Officer (DCOO) had day to day line management responsibility for the Trust Security Manager.

Jon Simpson is the Trust Security Manager who ensures that the Trust complies with all NHS security guidance and requirements and oversees the implementation of security management across the Trust.

This annual security report looks at security governance arrangements and incidents for the past year. It also reviews continuing efforts to keep staff and patients safe as well as securing Trust property and assets.

Sara Biffen June 2023

Acting Chief Operating Officer

Section	Contents	Page
	Title Page	1
	Foreword	2
	Contents	3
1	Governance, Risk & Assurance	4
2	Security Incident Reporting	7
3	Safe Environment for Staff & Patients	8
4	Communications, Awareness & Training	16
5	Conclusion	17

1 Governance, Risk & Assurance

A sound Governance framework is essential in ensuring a consistent approach to security.

1.1 *Security Arrangement Provision*

In accordance with the provisions of the NHS Violence Prevention & Reduction Standard (2020), NG10 (short-term management in mental health, health and community settings 2015), The Mental Health Units (Use of Force) Act (2018) and Emergency Preparedness & Resilience Response Standard No 21 (Lock Down) Providers are required to have in place and maintain security management arrangements in their organisations.

1.2 *Policy*

The Trust has the following security policies in place with scheduled review dates.

- SY01 Security Management Policy
- SY02 Violence & Aggression Policy
- SY03 CCTV Policy
- SY04 Lock Down Policy
- SY05 Counter Terrorism Procedures
- SY07 Patient Search

In accordance with those schedules SY01 was reviewed using national guidance and local protocols and republished. SY02 was also reviewed against the same and is due to be re-published shortly along with an updated NHS Violence Prevention & Reduction Standard self-assessment.

1.3 *Security Risks*

Security risks are managed in accordance with the Risk Policy and entered on to the Datix risk management system where they can be regularly reviewed. There is one security risk scoring more than 15 concerning the inconsistent use of door access control systems (particularly swipe card access) across all areas of the Trust, especially on general wards[1].

1.4 *Security Risk Assessment*

Through year security needs/risk assessment advice/support was given to Estates Capital and other Project Management Offices (PMO) on the following:

- Hospital Transformation Program (HTP) new build at RSH (access control, CCTV, intruder/staff duress and new-born security alarms, counter terrorism and general crime prevention measures)[2].

[1] 4-digit keypad pin code locks are on some entrances, but these systems are always subject to very easy compromise/misuse and counter compromise action is time consuming and very disruptive. Use is awkward and clumsy when linked with or part of a patient or other manual handling task especially if doors do not open or close with electrical assistance, so doors get left open. In the event of a known or immediate external threat all ward doors have the option to be secured manually and good physical security is provided to ward areas until an incident is over/stood down. This functionality is checked and tested every 3 months by site security teams with records held by security manager.

[2] A Building Research Establishment Environmental Assessment Method (BREEAM) assessment uses recognised measures of performance, set against established benchmarks, to evaluate a building's specification, design, construction. This includes a Security Needs Analysis (SNA) which will be completed by the Security Manager. The build is also being registered for 'Secured by Design' (SBD) accreditation. SBD is the official UK police security initiative that works to improve the security of buildings and their immediate surroundings to provide safe places to work and visit. Both initiatives will assist the Trust with meeting a new statutory obligation known as the Prevent duty which becomes law in 2024. Also known as Martyn's Law it places a legal duty on those responsible for certain publicly accessible locations to consider the threat from terrorism and implement appropriate and proportionate mitigation measures. If the new build application proved successful further effort could be considered to register other Trust facilities and premises that have already had incorporated similar security design proposals and features e.g. Hollinswood House.

- Hollinswood House (Telford) Community Diagnostic Centre (CDC) and Renal Unit (access control, CCTV, intruder alarms, staff duress/panic alarm systems, counter terrorism and general crime prevention measures).
- PRH Elective Theatre Hub (access control, CCTV).
- PRH Ambulance Receiving Area (ARA) (access control, CCTV).
- Shropshire Women & Children's (W&C) Centre Delivery & Paediatric Wards (access control).
- PRH Administration HUB new build (including security arrangements during site demolition and enabling works phase).
- Mortuaries (both sites) (access control and CCTV).

On completion of risk assessment security infrastructure improvements modifications and changes were made to the following departments/areas during the course of the reporting period:

- PRH A&E reception (access control).
- PRH Waste Yard (access control).

In addition, security risk assessment advice to support departmental development plans and business cases has been given for the following departments/areas.

- PRH A&E mental health room (location and general security environment).
- PRH A&E entry points x2 (access control).
- PRH Children & Young Persons Unit (CYPU) (access control and CCTV).

Areas of Special Interest. Regular and scheduled security risk assessment is undertaken on the following key areas of security:

- Lock Down; every three months our security team supervisors undertake audit and functionality tests of the emergency Lock Down plan for each of our ED. This ensures that paper copies of Lock Down plans are in the place staff expect them to be should they need them, are the correct version and the instructions, systems and facilities referred to in each plan are correctly functioning. Whilst this is being done opportunity is provided for the Nurse in Charge (NIC) and any new or less frequent working A&E staff to walk the department and understand the plan firsthand. After the ED check security supervisors then complete a site wide check of the emergency Lock Down arrangements for each Ward and/or publicly accessible department/entrance at both main sites. Any service or maintenance issues identified are addressed and the check also gives security staff the opportunity to liaise with clinical staff and highlight the procedure and mechanism for securing departments which are not regularly locked and secured because of operational constraints. Records on all these audits are retained by the Trust Security Manager.

- Lone Working (s3.9 refers); Every three months the security team supervisors test and assess lone worker pagers issued to/held by departments to ensure they are available for staff and to ensure equipment functionality by testing them with Switchboards. Records on all these audits are retained by the Trust Security Manager.

- Infant/Newborn Security (s3.10 refers); every 3 months to prevent the undue removal of a baby from the hospital the Baby Tagging security systems are tested to ensure system operability and staff knowledge/reactions. Results of each test are fed back to senior Women & Children's leadership/management, Chief Operating Officer (COO), Deputy Chief Operating Officer (D/COO). Records on all these audits are retained by the

Trust Security Manager. The benefit of this assessment process has been noted in previous CQC Inspection[3].

Mental Health & Learning Disability Operational Group. All activity concerning the safe holding/restraint of patients are reviewed by this group. Chaired by the Deputy Chief Nurse with involvement of Lead Nurses, Patient Safety, MHP and the Security Manager, this group meets monthly. Data on security team interventions (s3.5 and s4.1 refer) is provided on a twice weekly basis to members and discussion on security team involvement and actions with restraint is standing agenda item.

Health Safety Security & Fire Safety (HSSF) Committee. A quarterly security report is presented to the Trust Health & Safety Committee which is attended by staff side Chairs/representatives, Union representatives and has Divisional and Centre management representation. The report provides insight on progress with managing violence and aggression by service users (clinical as well as intentional/inexcusable aggression) including reports on sanction and redress and support to staff affected. In the fourth quarter, the annual security report is presented which gives feedback and a full account of all security management work in the reporting year.

Risk Management Committee. The Trust Security Manager attends monthly Risk Group meetings. Chaired by Director of Governance & Communications, this ensures security management oversight and advice is readily available for all matters discussed or raised.

1.5 *Release of Information/Freedom of Information (FOI), Complaints & Challenges*

Release of Information

11 releases of CCTV and/or recorded Body Camera footage were made to police (10) and/or to support internal investigation (1). In addition:

- 1 release of CCTV was made in response to a FOI request by a member of the public.
- 1 release was made to support development of a patient story.
- 1 release was made to assist in process/review of Legal Services case.

Releases to the police concerned criminal activity that occurred on Trust premises. In addition to the release of CCTV footage there were 6 other occasions where non-video related security guidance or data was given to assist with Trust responses to FOI requests from the public[4].

Complaints

1 formal complaint was made by a patient regarding alleged inappropriate use of force by a security guard when the patient was attendant at the PRH A&E. On review of CCTV video the security guard was found to have used disproportionate force whilst preventing the patient (who at that point had not been discharged) from leaving. The security guard was subsequently dismissed by his parent company and a full and unreserved apology made to the patient.

[3]"Staff followed the baby abduction policy and undertook baby abduction drills. All babies were electronically tagged, and labels and tags were checked daily. Tags were removed as part of the discharge process. All staff were trained and aware of the baby tagging process". Source: CQC Inspection Report (Evidence Appendix) published 8 April 2020 page 392.

[4] Responses and data were provided to Corporate Services staff that coordinate Trust responses.

2 Security Incident Reporting

Security incident reporting remains key to the maintenance of a pro-security culture.

2.1 Comparative figures for 2022-23 are shown in Table 1[5].

Table 1 - Security Incident Reporting

ALL SECURITY INCIDENTS	2020/21	2021/22	2022/23
First quarter: Apr, May, Jun	157	199	294
Second quarter: Jul, Aug, Sep	199	204	296
Third quarter: Oct, Nov, Dec	232	203	235
Fourth quarter: Jan, Feb, Mar	137	199	272
Running Total	**725**	**805**	**1097**

2.2 Of the reported 1097 incidents 696 occurred at the RSH, 394 occurred at PRH and 7 were off-site. The 7 off site incidents included:

Incidents effecting staff: Verbal abuse of Patient Engagement staff at event in Oswestry town center and verbal abuse of midwife during home visit (Oswestry).

Incident effecting contractor: 2 instances of contracted Renal Technician being inappropriately touched by patient (with known learning difficulties and diagnosed behavior issues) during home visit.

Security other: Missing keys for Trust offices at Shrewsbury Business Park (security other). Potential compromise of Trust credit card pin code (security other).

2.3 There were 220 non-aggression security incidents reported, a breakdown is herewith:

- Other Security (141)[6]
- Damage to Property (26)[7]
- Theft/alleged theft of Trust Property (7)[8] and non-Trust Property (46)[9]

[5]Source: Datix. Excludes Cyber Security and security related Information Governance incidents which are managed by IT and Information Governance teams. Figures are as available/recorded with effect 16 May 2023; this applies to all figures contained within this report hereafter. Figures may be subject to increase thereafter due to late reporting and/or incidents being re-coded from other categories during end of year accounting/verification.

[6]Examples include building/office insecurities, building alarm activations, suspicious behaviour, general concern re service user behaviour, undue interest in staff (harassment), nuisance phone calls, suspect packages or unattended luggage/bags and service users suspected to be or seen to be in possession of knives, blades or other illegal substances/items. 8 searches for such were carried out during the period. 6 were due to concern re possession of a knife or blade by as service user, on 5 occasions the presence of a knife or blade was confirmed and removed. Security staff have metal detector search wands available for use when searching patients, this equipment allows for more accurate searching of patients with less likelihood of harm to staff or opportunity for later use of the knife or blade). The other 2 searches revealed possession of alcohol or other illegal substance. Trespass included unwelcome/unnecessary presence of relatives, rough sleepers and/or intoxicated members of public in hospital grounds, unauthorised presence of public in staff only areas, refusal of patients to leave after discharge.

[7]Majority concerned minor damage to hospital structures and fittings by confused patients or patients in crisis or damage to private motor vehicle through collision with another vehicle or object.

[8]Concerning actual/attempted/suspected/alleged theft. Matters involved small quantities of uniform, NHS iPad from ED reception self-check in.

[9]Majority concerned allegations of theft of cash from staff and patients. In all instances monies had either been left unattended or based on the available information nothing further could be done to investigate. Incidents also included alleged theft of personal items (jewelry) and catalytic convertors from private motor vehicles.

3 Safe Environment for Staff & Patients

A key principle is that staff working at the Trust and patients and visitors using the Trust, have the right to do so in an environment where all feel safe and secure.

3.1 *Intentional/Inexcusable Violence & Aggression*

Figures for reported intentional/inexcusable violence and aggression incidents in 2022-23 are shown in Table 2. Intentional/inexcusable incidents ranged from acts of physical contact (however minor or inconsequential including spitting) to verbally threatening or intimidating behaviour and racial abuse. Intentional/inexcusable incidents are those incidents where the perpetrator *was not* deemed to have any reasonable excuse for their behaviour e.g. an underlying medical condition or illness such as dementia or toxic infection. Legally excess alcohol and/or drug misuse are not seen as mitigating circumstances for adverse behaviour, but as aggravating factors.

Table 2 – *Intentional/Inexcusable Violence & Aggression*[10]

INTENTIONAL/INEXCUSABLE VIOLENCE & AGGRESSION	**Year**		
	2020/21	**2021/22**	**2022/23**
First quarter: Apr, May, Jun	16	30	42
Second quarter: Jul, Aug, Sep	31	38	38
Third quarter: Oct, Nov, Dec	34	47	17
Fourth quarter: Jan, Feb, Mar	22	27	18
Total	**103**	**142**	**115**

Of the reported 115 intentional/inexcusable violence and aggression incidents 81 occurred at the RSH, 32 occurred at PRH and two off-site. 29 involved physical contact (however minor or inconsequential) of these 15 were on hospital staff.

3.2 *Non-intentional / Clinical Aggression*

These are incidents where an individual is deemed to lack capacity and are not therefore held responsible for their actions due to their medical condition, treatment or other underlying medical issue e.g. dementia.

Table 3 - Non-intentional Clinical Violence & Aggression[11].

CLINICAL VIOLENCE & AGGRESSION		**Year**	
	2020/21	**2021/22**	**2022/23**
First quarter: Apr, May, Jun	75	95	79
Second quarter: Jul, Aug, Sep	89	109	110
Third quarter: Oct, Nov, Dec	98	103	81
Fourth quarter: Jan, Feb, Mar	47	116	93
Total	**309**	**423**	**363**

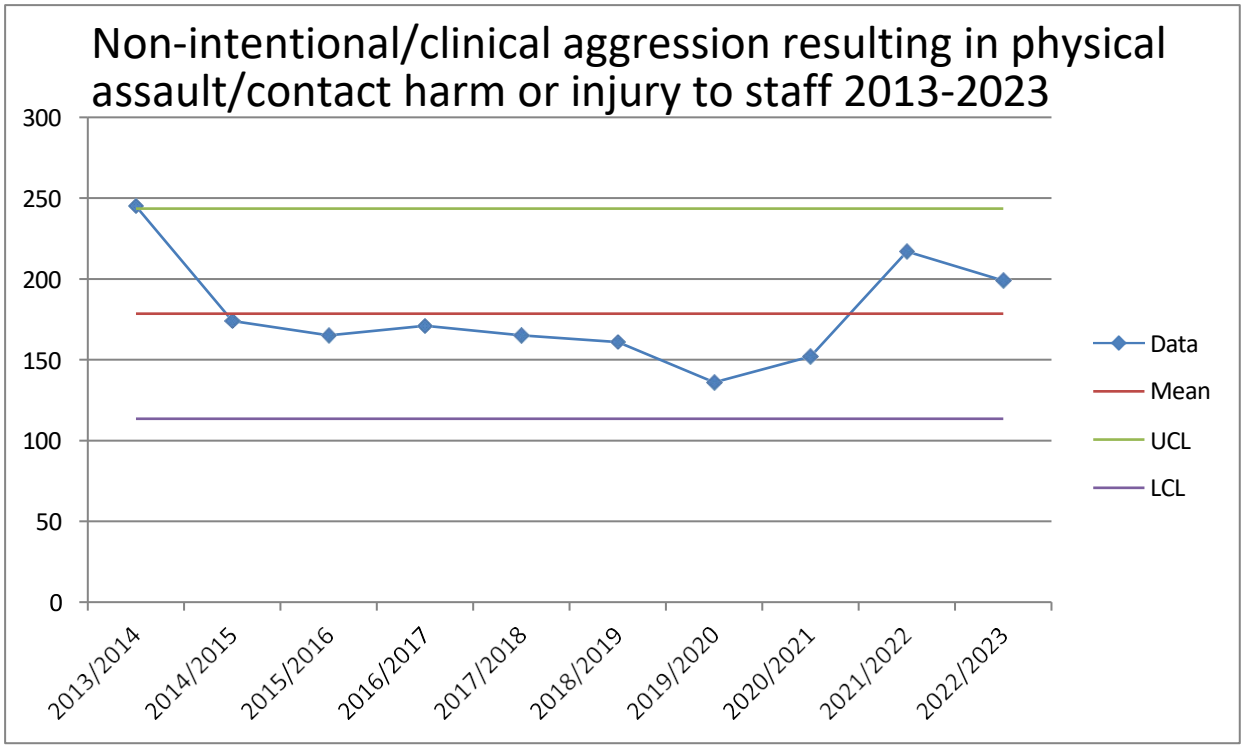
[10]Concerning all staff, patients, visitors and contractors. Source: Datix.
[11]Concerning all staff patients, visitors and contractors. Source: Datix.

Of the reported 363 non-intentional clinical aggression incidents 197 occurred at the RSH, 165 occurred at PRH and 1 off-site. 216 involved physical contact (however minor or inconsequential) of these 201 were on hospital staff.

Aside from the incidents reported in Tables 2 and 3, there were a further 399 occasions where staffs reported concern regarding potential for aggression from a patient[12]. Through appropriate de-escalation and/or intervention including where necessary security team contribution and/or rapid tranquilisation, patient behaviours were controlled, and each occasion passed without further escalation, harm or injury.

Safe handling and restraint training for security staff (4.1 refers) and use of security staff as the principal resource within the Trust for the safe handling of aggressive service users (3.5 refers) started in 2013-14. The number of incidents of non-intentional clinical aggression resulting in physical contact, harm or injury to staff reported each year since remains less and below the given upper control limit, with a welcome decrease from the previous reporting period, Figure 1 refers.

Figure 1: Number of reported non-intentional/clinical aggression resulting in physical assault/contact, harm or injury to staff between 1 January 2013 and 31 December 2022.



It is recognised that the risk of clinically related aggressive behaviour will always be present in an acute hospital, not least due to consistent pressures from an ageing population in Shropshire which is above the national average and increasing levels of dementia and mental health related issues. However Figure 1 shows that outcomes to this type of behaviour can be diverted or de- escalated from physical contact and therein physical harm and injury to staff.

[12]This may be through assessment of patients known to be in-crisis or at risk of self-harm whose behaviour is unpredictable, because of a patient needing a clinical or other intervention, but the patient is known for or will resist the intervention or will become agitated during the intervention and safe holding or restraint may be required for the safety of all concerned.

3.3 *Immediate Response to Violence & Aggression*

In line with our published policy on dealing with violence and aggression an escalated approach is used to deal with all violent and aggressive incidents, namely:

Step 1 - Use by all staff of conflict resolution techniques to diffuse situations (4.3 refers).

Step 2 - Calling for emergency assistance from hospital Security Officers. Security Officers provide emergency response and support to all staff facing threats of violence and aggression from service users, intentional or not (3.5 refers). As well as being backed up by an extensive CCTV network (3.7 refers) all Security Officers carry body worn camera[13].

Step 3 - Enlisting emergency assistance from the police.

3.4 *Post Incident Action, Sanction & Redress*

All reported security incidents from either hospital staff or the security teams are individually reviewed by the Trust Security Manager. This includes liaison with staff affected by more serious incident and/or their line management. The COO acknowledges reported incidents of violence and aggression by writing to all members of staff who may have been physically injured, harmed or significantly affected by an incident, offering support through line management or occupational health/counselling services and advising of the Trust's response to incidents. During the reporting period 146 such letters were sent to staff[14].

Where an assailant's actions were deemed to have been intentional/inexcusable, an entry is made on our electronic violence and aggression register. Linked to a patient's electronic SEMA record this allows staff in future to be warned of the potential for adverse behaviour from a patient[15]. A warning letter, signed by the COO is sent to the perpetrator of the adverse behaviour and copied to the victim and police, advising that non-emergency treatment could be withdrawn if there are any further episodes and support for police action or civil action by the Trust[16]. In the reporting period 32 SEMA alerts and 51 warning letters/final warning letters and/or letters of concern were issued. Only 3 of those receiving a warning letter in this period have come to further attention despite further hospital attendances, thereby giving some assurance as to the effectiveness of warning letters and the importance of challenging unacceptable behaviour.

The Trust supports all police and Court actions when taken and every effort is made to enable partnership working and achieve rightful sanction and redress for unacceptable behaviour. This includes provision of supporting CCTV, body camera recordings or other documentary evidence (1.5 refers). Examples of outcomes to prosecutions are herewith:

[13]A statement on how the equipment is used and controlled is included within our published CCTV policy. Body Camera are not used when dealing with patients who lack capacity.

[14]In line with the strategy outlined for dealing with violence and aggression a resulting outcome is that much adverse behaviour is diverted away from medical and nursing staff by the intervention of security staff before the behaviour escalates and so medical and nursing staff can avoid injury or unnecessary involvement; by virtue of their involvement security staff, based on their early involvement become responsible for reporting on the incident with medical/nursing staff being identified as witnesses as opposed to victims. This explains in some way the disparity between numbers of support letters issued to Trust/NHS staff and all reported incidents (Tables 2 and 3 refer).

[15]A recommendation for an alert on a patient's SEMA record and the issue of a warning letter is made by the Trust Security Manager. However, prior to this action being undertaken the recommendation must be approved and supported by an ED Consultant; this ensures that patients who may have lacked capacity at the time of the incident and whose circumstances may not have been accurately reflected in the incident reporting process are not unnecessarily sanctioned.

[16]It should be noted that it is not always possible or appropriate to issue a warning regarding unacceptable behaviour because the individual may not have been identified or the circumstances of the individual deem it inappropriate.

A female patient who assaulted a Nursing Sister in PRH ED on 9 March 2021 (web166941) pleaded guilty at Kidderminster Magistrates Court on 11 July 2022 to assault by beating of an emergency service worker. The woman was sentenced to 14 weeks imprisonment and ordered to pay the victim compensation. The Trust responded to the incident at the time in accordance with the provision of the Violence & Aggression Policy, this included support to affected staff.

At Telford Magistrates Court on 26 April 2023 a man pleaded guilty to causing, without reasonable excuse, a nuisance, and a disturbance at the RSH ED on 24 December 2022 (web208178). The man was fined and ordered to pay costs. The Trust responded to the incident at the time in accordance with the provision of the Violence & Aggression Policy, this included support to affected staff.

The annual NHS Staff Survey suggested that the number of staff at the Trust experiencing physical (Q13a) or non-physical (Q14a) abuse from patients, service users, relatives or other members of the public was below the national average and very much below those Trusts with the worst experiences[17].

3.5 *Principle Role of Security Officers*

The Trust's manned security guarding contract is key to being able to implement the provisions of several security policies and numerous other staff and patient safety policies. The security guarding contract which had been running for a number of years ended on 28 February 2023. Shropshire Healthcare Procurement Services (SHPS) completed a contract re-tender process utilising the North of England Commercial Procurement Collaborative (NOECPC) Framework. 10 suppliers expressed interest in the contract, 5 of these made formal submissions. Quality and financial submissions by the 5 were evaluated and scored by the Trust Security Manager and Procurement colleagues. The Quality Assessment Offer Schedule considered the following areas:

- Delivery of the Services 13%
- Management Capability & Capacity 13%
- Staff Retention/Motivation 6%
- Training 3%
- Service Delivery Failure 9%
- Environment/Sustainability 6%
- Social Value 10%
- Price Weighting 40%

MITIE Security Limited (the incumbent) achieved the highest score across the combined Quality and Price evaluation achieving a score of 89.11% and were awarded a 4-year contract to continue providing uniformed emergency security services at the Trusts 2 main operating sites. The MITIE submission evidenced their front-line NHS experience with several large acute hospital Trusts (including SaTH) as well as strategic/national level involvement and engagement in the

[17] NHS Staff Survey Benchmark report 2022 (nhsstaffsurveys.com) p73 and p74.

development of healthcare security and forthcoming statutory and regulatory legislation affecting healthcare security[18].

The 22 existing core team locally employed security staff working at both hospital sites were retained and transferred to the new contract under TUPE thereby retaining the invaluable experience. MITIE are a Real Living Wage (RLW) employer, and the contract provides for hourly pay rates to staff that are above the RLW as well as the National Living Wage (NLW) rate, which further encourages retention of staff and knowledge[19].

With any aggression incident security staff are called to help provide reassurance and assistance in seeing the safe closure of the incident or prevent further escalation, as well as providing pre- arranged preventative support to staff to stop a foreseeable incident escalation[20]. Often staff may note a SEMA warning alert for aggression on a patient's electronic record, this triggers a request for security staff presence when they attend. All Security Officers carry body camera recording equipment[21]. Security Officers are licensed in accordance with the Private Security Industry Act (PSIA) by the Security Industry Association (SIA) for Door Supervisor duties & Public Surveillance CCTV Monitoring. They are also trained to make physical interventions by way of safe holding / restraining those service users whose behaviour has escalated to the point that the safety of staff, the service user or others is being endangered. To provide security staff with the skills and confidence to do this, specialist training is delivered over a one-week training course to security teams by accredited NHS training staff from the Midlands Partnership Foundation Trust (MPFT) (4.1 refers).

364 safe hold/restraint interventions were undertaken across both sites by security staff during the reporting year. All safe hold and restraints are the subject of Rapid Review and reported to Deputy Chief Nurses, Lead Nurses and Matrons and the Trust Mental Health & Learning Disabilities Group (1.4 refers). Not all 'safe holds/restraints' were undertaken as a result of actual aggression towards staff. Some were undertaken due to concern about potential aggression due to:

- Concern by medical/nursing staff about safety during a planned invasive procedure where the patients mental or physical state, whilst not aggressive, suggested that harm or injury to the patient or staff would have occurred had an intervention not been undertaken.

- A need to prevent patients in personal crisis from attempting/carrying out acts of self-harm.

- High risk confused and/or agitated patients who had or were attempting to leave the hospital buildings and/or their ward/bed spaces and refusing to return.

[18] MITIE have representation on the Security Industry Authority (SIA) Strategic Violence Reduction Working Group as well as the Restraint Reduction Network (RRN) and the British Institute for Learning & Development (BILD).

[19] All employees on the same job role will benefit from the same pay rate, regardless of demographic group. This Tender is not a CIP and is not delivering a saving albeit it must be recognised that hourly rates for security staff are a flat 24/7 rate. There is no incremental pay or unsocial hours expenditure related to this contract.

[20]"Staff we spoke with were positive about the responsiveness of security staff within the hospital" and "nursing staff told us that the security team were often called if a patient's behaviour was challenging, and they were skilled in dealing with these challenges in a sensitive manner". Source: CQC Inspection Report (Evidence Appendix) published 8 April 2020 pages 270 & 91.

[21]A statement on how the equipment is used and controlled is included within our published CCTV policy.

3.6 *Other Duties*

Security staff also contribute to a wide range of tasks which are not specifically recorded as security incidents, but occur daily, these include:

- Help with preventing or locating absconded/missing patients or patients in crisis deemed to be vulnerable and/or at high risk of self-harm or may/are intending to take flight (patient safety).

- Fire alarm activations and other fire incident related activity (fire safety incidents).

- Attendance at Air Ambulance arrival/departure (operational task).

- Emergency resuscitation team calls to victims in public areas of the hospitals to ensure resuscitation teams can work without disruption or oversight of victims and ensure safe passage for patient evacuation etc. (medical emergency task).

- Escort of General Office staff carrying out cash transfer and filling/emptying of change machines and collection of valuables from night safes (cash security).

3.7 *Closed Circuit Television (CCTV)*

Each main hospital site has a dedicated CCTV camera control room which forms an operating base for Security Officers. Output from security cameras on our main hospital sites is fed back to these camera control rooms. As well as addressing a wide range of security issues and requirements these facilities prove very helpful with the rapid investigation of missing patients, some of whom have either inadvertently or intentionally left the hospital buildings[22].

Images recorded on all systems are stored and controlled in accordance with our CCTV operating policy. CCTV equipment at all our sites is covered by 24/7 maintenance support contracts from an approved contractor.

In the reporting period new CCTV facilities and/or improvement/upgrade to existing CCTV equipment was delivered in the following areas:

- PRH Ambulance Receiving Area (ARA) (new installation).
- PRH rear staff entrances/approach routes from staff car parks (upgraded cameras).
- PRH Mortuary and Estates entrance (new installation).
- RSH Copthorne House basement and Shrop-Doc out of hours entrance (new installations).
- RSH grounds (upgraded equipment in vicinity of SECC and Learning Centre.
- RSH grounds (new equipment in vicinity of Endoscopy/Renal/Hummingbird/Learning Centre/Treatment Centre).

In the reporting period plans were agreed for inclusion of CCTV facilities in the following Capital Estate Projects:

- HTP new build at RSH.

[22] 146 cameras at the Princess Royal Hospital and 158 at the Royal Shrewsbury Hospital. The Trust has 24 cameras used at other outlier sites at Shrewsbury Business Park (offices at Douglas Court 1 & 2), Queensway Business Park Telford (Sterile Services & Medical Records facilities), Ludlow Community Hospital (Midwife Led Unit (MLU)) and the William Farr NHS site, Shrewsbury (Therapy Services Building).

- Hollinswood House (Telford) Community Diagnostic Centre (CDC) and Renal Unit.
- PRH Elective Theatre Hub.
- PRH Admin HUB (security arrangements during site demolition and enabling works phase).

3.8 *Networked Swipe Card Door Access Control*

A networked swipe card system which can be accessed at both main sites i.e. you can swipe in at RSH and PRH with same card is already used in high-risk patient areas[23] and some departments requiring high levels of assurance for accreditation and licensing purposes[24]. Due to the engineering challenges presented because of the systems age and increasing maintenance costs a replacement system is being procured[25]. The new system will be required to replace the existing swipe card provision at the Trust but has also been included in design proposals for the following Capital Estate Projects:

- HTP new build at RSH.
- Hollinswood House (Telford) Community Diagnostic Centre (CDC) and Renal Unit.
- PRH Elective Theatre Hub.
- PRH Admin HUB (security arrangements during site demolition and enabling works phase).

In addition a separate business case to address concern around other poor provision of access control arrangements at the Trust[26] has been given £1.2m Capital funding to deliver the same swipe card access control to both A&E departments and all in-patient ward areas at both main sites[27].

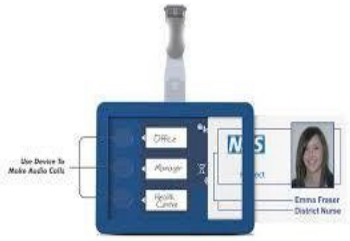
3.9 Lone *Working*

The Trust has a two-track strategy, one for off-site lone workers or those out in the community and one for those working alone on-site.

(i) Off-Site Strategy

The lone worker device used is in the form of an identity badge holder worn around the neck or clipped to a belt or tunic. It includes a panic alarm that can be discreetly activated, and which automatically opens a line of communication (via roaming mobile phone signal) to a national Alarm Receiving Centre (ARC), thereby allowing situation assessment and immediate response/escalation, as well as recording of evidence. In very extreme instances ARC staff are able to directly provide information from the staff member's device including pre-recorded information on where the staff member is located, to the nearest police control room. The advantage here is that police response is quicker because the information being received by them is from an accredited source as opposed to an anonymous cold call to police from public.

[23] In-patient Maternity & Paediatrics.
[24] RSH Pharmacy, Pathology, Mortuary. Data Centers at both sites.
[25] Competitive tender multi-quote issued 2 March 23, concluded May 23.
[26] 4-digit keypad pin code locks are on some entrances, but these systems are always subject to very easy compromise/misuse and counter compromise action is time consuming and very disruptive. Use is awkward and clumsy when linked with or part of a patient or other manual handling task especially if doors do not open or close with electrical assistance, so doors get left open (Datix Risk Register 312). In the event of a known or immediate external threat all ward doors have the option to be secured manually and good physical security is provided to ward areas until an incident is over/stood down. This functionality is checked and tested every 3 months by site security teams with records held by security manager.
[27] Capital Planning Group (CPG) meeting minutes 16 Sep 22 (minute 2022.75). Funding to delivered over 3 FY. Project board established May 23.



The device is not seen as a risk eliminator, rather as a risk reducer designed to work with and complement other safe systems of work. The use of this system was noted during the last CQC Inspection[28]. 201 staff currently have access to a live device.

(ii) On-Site Strategy

In this system upgraded hospital pagers allow a lone worker to send a discreet emergency alert to security staff pagers and hospital switchboards. As well as being used on a daily basis in departments whose task requires continual support e.g. overnight Pathology Laboratory staff, devices have also been used to provide immediate short-term reassurance to staff who through no fault of their own have become the victim of undue interest from patients/public.

As well as regular checks by our security team supervisors (s1.4 refers) a maintenance and support contract with the supplying company is in place to ensure specialist technical support and equipment repair is available.

3.10 *Baby Tagging*

This facility is in operation at the Shropshire Women and Children's Centre at the PRH on the Post-Natal Ward and the Wrekin Midwife Led Unit (MLU) at the PRH. Each new-born has a tag fitted after delivery. Should the infant then be taken towards a doorway, including a fire exit, the tag will alarm and send doors into Lock Down mode whilst discreetly alerting staff at the nurse base via a PC type console so they can investigate. If doors are physically forced, breached or someone manages to tail-gate out, the system will immediately alarm in a very loud and audible manner. In the Women & Children's Centre should the alarms at the doors fail, a second layer of sensors will activate in the main foyer and each external entrance to the building.

[28]"Lone worker security devices had been provided for each community midwife". Source: CQC Inspection Report (Evidence Appendix) published 8 April 2020 page 429.

If a tag is forcibly removed or cut off the system automatically goes into alarm. The same occurs if the system detects an inability to communicate with a tag e.g. if the infant were wrapped in coverings or placed in a bag to enable unauthorised removal.

As part of our security management assurance program, checks and testing of the system and staff reactions are carried out every 3 months by Ward Managers and the Trust Security Manager with feedback provided to senior management on the outcome from each test. A maintenance and support contract with the supplying company is in place to ensure system continuity and reliability. A 24/7 emergency telephone help line is included within the support element of the contract, so staff have constant access to specialist technical support. Inclusion of similar is being included within the Security Needs Analysis (SNA) for the HTP new build.

4 Communication, Awareness & Training

4.1 *De-Escalation & Management Intervention (DMI)*

Security staff are the primary trained resource at the Trust for the safe handling and restraint of physically violent or aggressive patients. To provide security staff with the skills and confidence to do this, specialist DMI training is delivered by accredited NHS training staff from the MPFT. The training, which consists of a 5-day foundation course and annual refresher days thereafter, has been accredited by the British Institute for Learning & Development (BILD) and the Institute of Conflict Management. A syllabus ordinarily delivered to NHS Mental Health Professionals (MHP) working at MPFT is followed, but with additional bespoke content aimed at recognising the role of our security staff and the varied and different circumstances and settings experienced in a busy acute hospital environment. In the reporting period 9 security staff undertook whole day annual refresher training whilst 11 completed the initial 5-day foundation course with 4 more recent new starters scheduled for next available training.

As part of a recognised wider training need for key clinical staff to be trained in safe handling and restraint a number of nursing staff received training from MPFT during the reporting period. Having key clinical staff trained in this way allows for due oversight of any safe holding or restrictive intervention activity to the betterment of patients and security staff undertaking such activity. It will also help provide on-hand skills for completion of low level clinical safe holding for patient safety and reduce the need for security team presence at such.

4.2 *Conflict Resolution Training (CRT)*

In the reporting period 2216 employees completed on-line CRT. Of the 3852 patient facing staff for whom the training is mandatory 3662 staff were identified as in date on 01 April 2023, which equates to 95.07% compliance[29].

[29]Workforce Directorate 18 May 2023.

4.3 *Lone Workers*

During the reporting period 69 members of staff who work alone in the community (regularly and/or occasionally) were trained on lone worker device usage and personal security. All staff using lone worker devices for use under the off-site strategy are given training by the service provider prior to a device being enabled. The training not only informs on how to use the device in terms of practicalities like switching on and off and battery charging, but also informs on the risks to lone workers identifying vulnerabilities and risk assessment.

5 Conclusion

In addition to maintaining and progressing the activity already covered in this report we will also seek to:

- Continue to provide specialist security risk assessment advice and guidance on security infrastructure and security resources for the HTP (including assessment of manned guarding needs and any subsequent business case for each of the main sites upon completion of HTP new build) and other Capital investment in its sites.

- Continue to provide corporate security risk assessment advice, support, guidance to the Trust and all Centres and departments.

- Ensure that continued and credible professional uniformed 24/7 emergency security support remains available and at the disposal of all Centres and departments at the Trust including ensuring continued investment in the training of security teams to deal with conflict resolution and support clinical staff with aggressive and/or agitated/confused patients.

- Continue to ensure clear messages are sent to perpetrators of unwelcome and anti-social behaviour to reinforce the Board's robust approach to abuse of staff and patients.

6 Looking Forward to 2024-25

- In 2024 the Trust will be required to meet a new statutory obligation known as the Prevent Duty. Also known as Martyn's Law, the Prevent Duty is forthcoming legislation that will place a statutory requirement on those responsible for certain publicly accessible locations to consider the threat from terrorism and implement appropriate and proportionate mitigation measures. In preparation for its arrival and in addition to maintaining existing security arrangements and measures already outlined in this report, the following *proposals* will be made to further strengthen the organisations security profile and mitigate relevant threats:

    1) 3 yearly security awareness training for all staff in the form of Action Counters Terrorism (ACT) awareness eLearning. This is a free 60 minute online counter terrorism awareness training course for all UK based companies, organisations and individuals. ACT Awareness eLearning provides nationally recognised corporate counter terrorism guidance to help people better understand, and mitigate against, current terrorist methodology.

    2) Introduction of video format Corporate welcome security briefing for new starters.

    3) Increasing current regime of 3 monthly emergency Lock Down checks at each of the main operating sites to monthly.