The Shrewsbury and Telford Hospital NHS

NHS Trust

Annual Security Report

2021/22

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.

Nigel Lee (Chief Operational Officer) was the designated Board level Director responsible for security management matters during the reporting period that this report covers, including tackling violence against NHS staff, and ensuring that there is adequate security management at the Trust.

Sara Biffen, Deputy Chief Operating Officer 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 also 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 12 April 2022

Acting Chief Operating Officer

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[1], NG10[2] and the Mental Health Units Act[3] 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. In accordance with those schedules SY04 and SY05 were reviewed against national guidelines and local protocols and republished.

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

1.3 *Security Risks*

Security risks are managed in accordance with the Risk Policy and entered on to the 4Risk system where they can be regularly reviewed due to system generated electronic alert[4]. There is one security risk scoring more than 15 which concerns the inconsistent use of door access control systems (particularly swipe card access) across all areas of the Trust, especially on general wards[5]. This risk was discussed as an agenda item at the recently re-convened Risk Group where a risk score of 16 was ratified by the Group who supported the requirement for a swipe access control system. A business case will now be made for Capital Funding.

1.4 *Security Risk Assessment*

Through year security risk assessment advice/support was given to Estates Capital Projects on the following:

- RSH Ward 37 new build (access control, CCTV and other patient safety alarm systems).
- RSH A&E refurbishment (access control, CCTV and other patient safety alarm systems).

[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 Act (Use of Force) 2018.

[4] Risk Register will transfer from 4Risk to Datix during 2022-23.

[5] 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.

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 Education & Learning centre (access control /remote door release system).
- PRH Loading Bay (access control)
- RSH Day Surgery (installation of intruder alarm system to storeroom).
- Douglas Court 1&2 Shrewsbury Business Park (installation of CCTV system).

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

- Mortuary (both sites) (access control, CCTV and intruder alarms).
- RSH Radiography (access control).
- RSH kitchens (access control).
- PRH Theatre (access control).
- W&C Obstetric Wards (Newborn security tagging systems and access control).

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 unauthorised 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 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[6].

[6] "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.

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.

Staffordshire & Shropshire NHS Security Management Forum. This voluntary forum has representation from all NHS sectors in Shropshire & Staffordshire including Acute, Mental Health and Community services. The forum provides opportunity for briefing and discussion on security issues affecting all NHS interests.

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

Release of Information

No releases of CCTV or body worn camera footage were made to the public during the reporting period. 10 releases were made to police and/or to support internal safety investigations.

The releases to the police concerned criminal and/or suspicious activity or other incident requiring further investigation that occurred on Trust premises. Although some of the releases concerned incidents which did not occur on Trust premises, it was often the case that the original incident subsequently led to other adverse attendance or activity on Trust premises.

Freedom of Information (FOI)

13 FOI requests were made regarding other security matters at the Trust. Responses and data were provided to Corporate Services staff that coordinate Trust responses.

Complaints

In the reporting year 3 complaints were made by the public to the Trust Complaints Team regarding alleged inappropriate use of force to restrain patients who were either intent on self-harm, harming or injuring staff or other patients or compromising their own care and safety by unnecessarily leaving a hospital ward or bed space. On review attendant security staff were found to have acted appropriately with responses sent from Complaints Team. A complaint regarding alleged discussion of a patient's personal situation by security staff was found to an incorrect allegation and no further security involvement in the complaint response was required.

2 Security Incident Reporting

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

2.1 Comparative figures for 2021-22 are shown in Table 1[7].

Table 1 - Security Incident Reporting

ALL SECURITY INCIDENTS	**2019/20**	**2020/21**	**2021/22**
First quarter: Apr, May, Jun	170	157	199
Second quarter: Jul, Aug, Sep	182	199	204
Third quarter: Oct, Nov, Dec	166	232	203
Fourth quarter: Jan, Feb, Mar	190	137	199
Running Total	**708**	**725**	**805**

2.2 Of the reported 805 incidents 492 occurred at the RSH, 308 occurred at PRH and 5 off-site.

2.3 There were 240 non-aggression security incidents reported, a breakdown is herewith:

- Other Security (181)[8]
- Damage to Trust Property (8)[9]
- Damage to non-Trust Property (6)[10]
- Theft/alleged theft of Trust Property (9)[11]
- Theft/alleged theft non-Trust Property (36)[12]

[7] 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 5 April 2022; 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.

[8] 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. 16 searches for such were carried out during the period. **On** 9 **occasions the presence of a knife or blade was confirmed and removed from a service user.** 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). 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.

[9] Majority concerned minor damage to hospital structures and fittings by confused patients or patients in crisis.

[10] Majority concerned damage to private motor vehicle through collision with another vehicle or object.

[11] Concerning actual/attempted/suspected/alleged theft. Matters involved small quantities of PPE/clinical supplies, NHS iPad and a wheelchair (perpetrator identified and reported to police, when challenged the perpetrator admitted he had removed the wheelchair without permission or need to go to a pub after discharge from A&E. The wheelchair was not found, and agreement was reached that the perpetrator would pay for a replacement which he did).

[12] Majority concerned allegations of theft of cash from both 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 (in one instance this was jewellery) 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 2021-22 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*[13]

Intentional/Inexcusable Violence & Aggression			
	2019/20	**2020/21**	**2021/22**
First quarter: Apr, May, Jun	33	16	30
Second quarter: Jul, Aug, Sep	36	31	38
Third quarter: Oct, Nov, Dec	30	34	47
Fourth quarter: Jan, Feb, Mar	29	22	27
Total	**128**	**103**	**142**

Of the reported 142 intentional/inexcusable violence and aggression incidents 89 occurred at the RSH, 52 occurred at PRH and one off-site[14]. 31 involved physical contact (however minor or inconsequential) of these 16 were on 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 3a - Non-intentional Clinical Violence & Aggression[15].

CLINICAL VIOLENCE & AGGRESSION	**Year**		
	2019/20	**2020/21**	**2021/22**
First quarter: Apr, May, Jun	62	75	95
Second quarter: Jul, Aug, Sep	62	89	109
Third quarter: Oct, Nov, Dec	71	98	103
Fourth quarter: Jan, Feb, Mar	88	47	116
Total	**283**	**309**	**423**

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

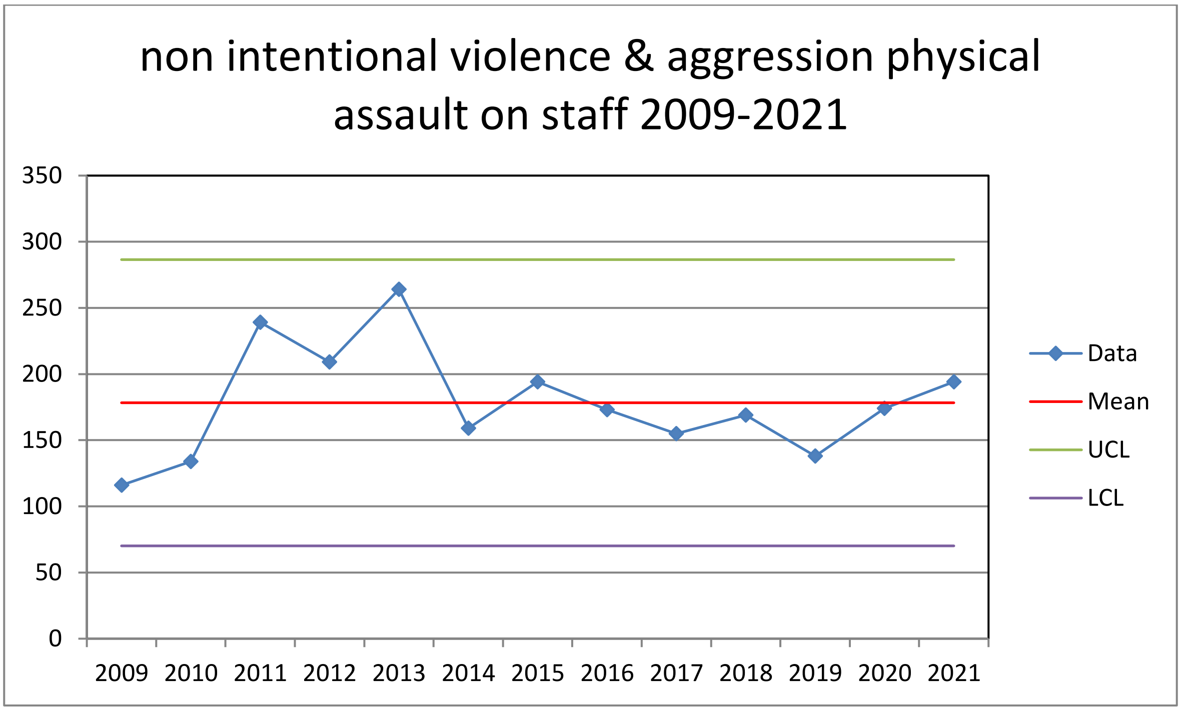
[14] Datix Web; 171783 took place at a patient's home no harm or injury to staff.

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

Of the reported 423 non-intentional clinical aggression incidents 250 occurred at the RSH, 172 occurred at PRH and 1 off-site[16]. 237 involved physical contact (however minor or inconsequential) of these 219 were on staff.

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 then is significantly less and despite slight increase during the reporting period remains below the given upper control limit, 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 2014 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.

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

[16] Datix Web; 180123 took place at Oswestry MLU no harm or injury reported.

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[17].

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 155 such letters were sent to staff[18].

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[19]. 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[20]. **In the reporting period 25 SEMA alerts and 66 warning letters/final warning letters and/or letters of concern were issued. Only 2 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 often includes provision of supporting CCTV, body camera recordings or other documentary evidence (1.5 refers).

3.5 *Principle Role of Security Officers*

Although security staff at both sites are provided by an external company, they are very much seen as part of the hospital team and relied upon for support across all areas of both hospital sites. All of the core team staff only work at the hospital and are not used on other contracts by their parent company[21].

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-

[17] 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.

[18] 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).

[19] 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 has to 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.

[20] 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.

[21] All 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.

arranged preventative support to staff to stop a foreseeable incident escalation[22]. 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[23].

Our regular core team security staffs are 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).

393 safe hold/restraint interventions were undertaken across both sites by security staff during the reporting year and all are reported to a Deputy Chief Nurse, 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.

3.6 *Other Duties*

Security staff also contribute to a wide range of tasks which are not specifically recorded as security incidents, but occur on a daily basis, 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).

[22] "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 page 270 & page 91 respectively.

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

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[24].

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.

CCTV equipment is being delivered as part of the new build Ward 37 at the RSH and has been installed at Trust offices at Shrewsbury Business Park (Douglas Court 1 & 2). The £9.5 million refurbishment of A&E at the RSH has seen the upgrade and replacement of all existing camera in the department as well as a number of new cameras to cover the much-enlarged department as well relocation of the old security camera monitoring room into a new build facility.

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[25] and some departments requiring high levels of assurance for accreditation and licensing purposes[26]. Where funding permits it is included in new builds and major refurbishments, but progress is dependent on project funding priorities and as such is inconsistent. The system is currently being upgraded but this is not deemed as detrimental to further use or expansion[27]. None of the existing general wards at either site have this system[28]. This risk was discussed at the recently re-convened Risk Group where a risk score of 16 was ratified by the Group who supported the requirement for a swipe access control system[29]. A business case will now be made for Capital Funding to expand the networked door access control system.

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

[24] 144 cameras at the Princess Royal Hospital and 155 at the Royal Shrewsbury Hospital. The Trust has 24 cameras used at other outlier sites at Shrewsbury Business Park (offices), 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).

[25] In-patient Maternity & Paediatrics.

[26] RSH Pharmacy, Pathology, Mortuary. Data Centres at both sites.

[27] Associate Director Estates 28 January 2022.

[28] 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.

[29] 4Risk Register No 75.

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.

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[30]. 205 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

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

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.

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. At the time of writing assessment and feasibility work is being completed that would lead to the system being introduced into Delivery and Neo-Natal Units in the Shropshire Women & Children's Centre.

4 Communication, Awareness & Training

Efforts continue to raise staff awareness on security and encourage a proactive security culture.

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 7 of our security staff undertook whole day annual refresher training whilst 16 staff members either completed or have been scheduled to complete the initial 5-day foundation course.

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 *Public Space CCTV Surveillance Training*

All our security staff are licensed and trained in accordance with Security Industry Act requirements for use of CCTV equipment. During the period 12 Security Officers undertook this training.

4.3 *Conflict Resolution Training (CRT)*

In the reporting period 1846[31] staff undertook on-line CRT.

4.4 *Lone Workers*

During the reporting period 110 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/Year Ahead

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

- Prepare and pursue Capital Funding for expansion of networked swipe card access control.

- Continue to invest in the training of the security team 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.

[31] Workforce Directorate 27 April 2022.