South East Coast Ambulance Service NHS
NHS Foundation Trust

Security Management Procedure

Contents

1 Scope

1.1. This procedural document, the Violence Prevention and Reduction Strategy, procedure and the Security Management Policy they relate to, exists to clarify clear and precise protocols for the management of security within South East Coast Ambulance Service NHS Foundation Trust (the Trust).

1.2. It is recognised that this can be broken down into two key elements, namely:

1.3. The protection of all staff employed by the Trust, including temporary and agency staff and Trust contractors, from violence, abuse, and aggression whilst in the course of their duties.

1.4. The protection of Trust vehicles, equipment and premises from theft and criminal damage, as well as assisting staff in preventing the loss/theft of their own personal items.

1.5. In addition to this, this document will highlight key steps that must be taken in the event of any incident of a security related theme that relates to the above areas, and in particular guidance to the reporting and management of such incidents and the steps that must be taken, with appropriate responsibilities listed.

2 Prevention of instances of violence and abuse

2.1. Education and training

2.1.1. All frontline operational staff as part of their training receive conflict resolution training. This will assist them in identifying behaviour which may lead to violence and, should it occur, practical means to minimise the likelihood or severity of an incident taking place.

2.2. Dynamic Risk Assessment

2.2.1. Frontline Operational staff complete a dynamic risk assessment in all instances when on duty, taking into account all relevant information to hand e.g. from history marks or call details and the circumstances around them e.g. how secluded or well lit the location is, the behaviour of persons encountered, the ability to leave etc.

2.2.2. Dynamic Risk Assessment is an on-going process that must be used continuously and in all circumstances. It must influence the decisions and behaviour exhibited by staff whilst on duty and should encapsulate all pertinent information that might affect safety on scene i.e. ensuring there is a point of escape if needs be and keeping ones distance from people exhibiting signs of aggression.

2.2.3. Through use of this process, staff should make informed and reasoned decisions to enter or remain in any given circumstance, with due consideration for their own safety and the safety of crew mates and other responders.

2.2.3.1. Management of instances of non-physical assault against a member of staff

2.2.3.2. Staff actions

2.2.3.3. It is recognised that any situation requiring the attendance of an ambulance may cause stress to either the patient or those accompanying them, which may, in turn, lead to them using coarse language and overt agitated behaviour.

2.2.3.4. It has been shown that on these occasions an explanation from staff stating they are offended by such behaviour and that it is inappropriate may lead to the person behaving more acceptably and this is advocated as a way to address these circumstances, however, the Trust recognises this is a judgement call by the employee on if and how to address matters, based on a dynamic risk assessment of the circumstances and the risk of exacerbating them.

2.2.3.5. It is unacceptable that any employee should be subjected to verbal abuse and all such incidents should be reported as soon as possible after the incident by the affected staff member.

2.2.3.6. Employees must :

2.2.3.7. Complete and submit an incident report (IWR-1) before the end of their shift. This report will be processed in accordance with the Incident Reporting Policy (DATIX) & Procedure.

2.2.3.8. The victim of any such incident should be encouraged to seek police involvement and the possibility of prosecution and contact the police to report the incident immediately after the incident.

2.2.3.9. Ensure that Emergency Operations Centre (EOC) is aware of the incident and, where appropriate for the incident and the location of the incident (i.e. not a public place or building), that a temporary history marker has been placed via use of a History Marking Form.

2.3. Managers actions

2.3.1. The Operations or Emergency Operations Centres (EOC)Manager responsible for the employee must ensure an IWR1 investigation is completed in accordance with the Trust’s Violence and Aggression Procedure and Incident Reporting Policy (DATIX) & Procedure.

2.3.2. In the event of the Manager being absent, due to annual leave or sickness, the investigation must be commenced by a deputy covering the role.

2.4. Security Team

2.4.1. Where support, Police/CPS liaison and/or guidance through Court processes is needed, the Security Team can either be contacted or where available will contact the employee to ascertain additional details concerning the incident and will advise the employee of further options.

2.4.2. If the victim wishes to seek sanctions, the Security Team will guide and support them in making a police report and will follow the same practices throughout the police investigation and any subsequent legal action as in the circumstances of a physical assault.

3 Management of instances of physical assault against a staff member

3.1. Actions for staff and managers following a physical assault are the same as would be followed for a non-physical assault, with the following important additions.

3.2. Staff actions

3.2.1.1. Immediately following a physical assault, employees should do the following as a matter of priority:

3.2.1.2. Withdraw from the area of violence.

3.2.1.3. Call for police attendance via Emergency Operations Centre (EOC) using the man down button or other appropriate means.

3.2.1.4. If possible, and only if safe to do so, employees should keep the offender under observation until the arrival of the police, at which point they should explain what has happened to the attending police officers.

3.2.2. **Staff should state that they want action taken against the offender at the time of police attendance**, but if the incident does not require or allow for police attendance, they should report the assault to the police as soon as possible and, where requested, provide a statement.

3.2.3. Any incident of violence against staff must be reported via the Trusts incident reporting mechanism as soon as possible after the incident by the affected crew member, or where this is not possible by their crewmate or manager.

3.2.4. Where an injury has or may have occurred, be examined at A&E or by their local GP, where possible, within 48hrs of the incident.

3.2.5. The following details, where available, should be recorded in the incident report alongside the details of the date, time, location and name of crew members involved;

3.2.6. Details of the police officer who is dealing, including name, number, and station.

3.2.7. The crime report number (or where this is not yet applied, a police CAD/incident number)

3.2.8. Details of the circumstances leading up the assault, and the nature of the assault itself (including any injuries)

3.2.9. Details of the assailant, including name, date of birth and appearance.

3.2.10. Details of any pertinent incident factors, such as racist or homophobic elements, or the involvement of drugs or alcohol

3.2.11. If appropriate for the location of the incident (i.e. not a public place or building) a History Marking Form must also be filled in and before going off duty as per the History Marking Procedure.

4 Protection of Assets, Equipment and Premises

4.1. Education and Training

4.1.1. All staff have access to information concerning:

4.1.1.1. Security in the workplace.

4.1.1.2. Security of personal belongings.

4.1.1.3. Personal security.

4.1.1.4. Awareness of how breaches of security or incidents of violence are to be reported.

4.1.1.5. Operational staff will receive additional information concerning awareness of incidents of violence and abuse and the support they will receive should it occur.

4.2. Premises Security

4.2.1. The majority of Trust premises have swipe access, however any remaining premises doors that require code changes will have scheduled code changes which are to be performed as part of a structured rolling process, with the Estates department facilitating a door lock change at a different Trust site every six weeks.

4.3. Internal thefts/damage/security issues

4.3.1. The Trust recognises that, with over 4500 employees, there is a likelihood of criminal activities taking place within the Trust workforce that may be perpetrated by Employees, in particular:

- Theft

- Criminal damage
- Fraud

4.3.2. Where detected, these incidents must be reported immediately to the Silver Officer, who will consider the need to make an immediate report to the police in the same way as any other incident of theft, based on the severity of the incident.

4.3.3. The theft itself (without details of the offending member of staff) must be reported as an IWR1 incident and Security.Management@Secamb.nhs.uk informed as soon as is practicable.

4.3.4. In all cases, these incidents should be addressed with the involvement of Human Resources at the earliest opportunity.

4.4. Searches of lockers/bags

4.4.1. Trust managers do not have the power to initiate searches of Employees personal kit without the owner's permission.

4.4.2. However, where there is a reasonable suspicion that a specific stolen item has been taken by a specific Employee and is being stored in a specific place, a Trust Manager (either Operational or Non-operational), with written or verbal approval of a Silver Officer or above, should consider the following.

4.4.3. Contacting the police, who do have the power to initiate a search.

4.4.4. Request the permission of the Employee to search the kit.

4.4.5. It should be made clear that a request to search has been approved, but that it does not have to be granted by the member of staff (in which case the search cannot continue). Where a search is refused the Trust has the right to record this refusal for use in subsequent disciplinary proceedings and consideration should then be made, with the Silver Officer, of contacting the police for the same purpose.

4.4.6. Where a search is carried out, regardless of whether items are found, an IWR1 should be filled out recording the date and time this took place, the reason for doing so and the route that permission to search was sought from Silver Officers.

4.5. Security Audits

4.5.1. Security Audits must be carried out by the Security Team, who must visit the site in person to make their assessment.

4.5.2. Security Audits carried out must contain the following information;

4.5.3. Date and time of the assessment.

4.5.4. Details of the surrounding area and layout of the site.

4.5.5. The crime figures for the area compared with the national average.

4.5.6. A history of any specific incidents at the site itself.

4.5.7. A written report on the site, including lighting, access control, security of controlled drugs and other pertinent issues.

4.5.8. A list of recommendations for site security, as risk assessed against need and effectiveness.

4.5.9. An action plan for implementation based on the recommendations.

4.5.10. The survey and its recommendations will be shared with the appropriate OM and OUM and the compiled list of recommendations with Estates to be prioritised and implemented.

4.5.11. The action plan should be updated as each is performed to demonstrate progress against the recommendations.

5 Lockdown

5.1. The Trust has a requirement to undertake a lockdown risk profile for each of its organisational sites and other specific buildings/areas (such as Emergency Operations Centres) and includes these assessments in the Security Audit for each site.

5.2. The profile will consider many aspects that are specific to each area (i.e. surrounding area/buildings, security of external doors, key control etc.), however the following will also be considered specifically for lockdown purposes for each site:

5.3. The contents and purpose of the building and in particular whether this is critical to the Trust’s service provision or the national infrastructure.

5.4. The presence of any “hazardous materials”.

5.5. The ability to secure the perimeter of the site and the building itself and prevent and control access.

5.6. The ability to call for assistance (via EOC, the Police etc.)

5.7. For larger sites only (HQ’s, Regional Offices and Make Ready Centres) the ability to lockdown segments and areas of the site.

5.8. These individual assessments, once completed for the entire Trust, shall be compiled into an organisational overview, highlighting specific and general areas of concern, with recommendations and subsequent instructions for the lockdown process.

6 Deterrence and Promotion

6.1. The Trust will publicise the unacceptability of violence and abuse against employees of the Trust via media services with newspapers, radio, and television. It will also participate in ambulance appropriate campaigns coordinated by NHS England designed to raise awareness and deter would be offenders.

6.2. Internal Trust publications, such as the Bulletin weekly newsletter should be used to publicise the following;

6.3. Security issues and concerns that have been raised via external parties (i.e. through NHS England or the National Ambulance Violence Security Group (NAVSeG network)

6.4. Recent sanctions achieved against people who have assaulted or abused staff.

6.5. Recent sanctions achieved against people who have committed theft or criminal damage against the Trust.

6.6. Clarification of Trust policies and procedures i.e. for History Marking.

6.7. General reminders relating to matters of security.

6.8. The Trust will publicise via signage on its vehicles that violence and aggression will not be tolerated against its staff and sanctions will be sought against offenders.

7 Responsibilities

7.1. Chief Executive Officer

7.1.1. Ultimately responsible for all policies and procedures within the Trust, including those pertaining to the prevention and management of violence, abuse and aggression and the protection of all Trust assets.

7.1.2. Overall responsibility for ensuring compliance with Security statutory and regulatory requirements.

7.1.3. Overall responsibility for ensuring compliance with Healthcare statutory requirements.

7.2. The Trust Board

7.2.1. The Trust Board is responsible for ensuring that the strategy is implemented and tracking progress of its delivery.

7.3. Executive Director of Nursing and Quality

7.3.1. Responsible for ensuring processes, procedures and systems are in place to manage the protection of assets and prevention and reduction of violence and aggression incidents against staff.

7.4. Security Team

7.4.1. Responsible for assisting the Trust to realise the requirements and directions issued by the Secretary of State, Department of Health and NHS England relating to security.

7.4.2. Responsible for escalating to the SMD awareness of security issues which may affect the Trust, its staff, patients or the levels of service.

7.4.3. Develop and lead on Trust wide improvement plans for Security Management and have oversight of assurance work to ensure a strong security culture is embedded.

7.4.4. Will be the named role in charge of Security for the Trusts Controlled Drugs Licence.

7.4.5. To advise on crime reduction measurements of Trust properties and activities which may place employees, patients and the public at risk.

7.4.6. To provide specialist expert advice information, guidance and training to assist directors, managers and staff in the performance of tasks and duties in relation to Security Management.

7.4.7. Oversee the investigation of security incidents in accordance with established practice and legislation and liaise with the Police, NHS England and other relevant parties to secure suitable sanction where necessary.

7.4.8. Liaise with the Police, Crown Prosecution Service (CPS) NHS England and other interested stakeholders and act on their behalf as required in the best interests of the Trust, and where required in an effort to secure prosecutions, give evidence or otherwise to safeguard the Trust, and it's activities.

7.4.9. Acting where required as the official Trust Witness in support cases through the Criminal Justice System for Security related incidents affecting the Trust.

7.4.10. Will be the Trust's representative/member at the National Ambulance Security Group meetings and supporting the determination of best practice for local Trust implementation.

7.4.11. The Trust Lead for Security will liaise with the Trust's Local Counter Fraud Specialist (LCFS) where security issues are raised that are of joint or mutual interest, or where specialist advice or assistance is needed. An MOU is in place for this.

7.4.12. Responsible for administration of Security Incidents on the Trusts' Incident Reporting System and ensuring managers conduct proportionate security related investigations.

7.4.13. Responsible for the administration of the Trust's ID card system.

7.4.14. Circulating advice set out by specialists/management/senior management within Security, to support violence, aggression, theft, criminal damage cases etc. as well as processes around ID card management, CCTV, BWC and lone working.

7.5. **Managers**

7.5.1. Responsible for engaging, and ensuring the staff they are responsible for engage, in the processes outlined in this procedure in response to issues and incidents within the guidelines stated.

7.5.2. Where incidents occur, responsible for ensuring that:

7.5.3. The incident is recorded and reported correctly.

7.5.4. An internal manager's investigation is conducted on the appropriate form (IWR1).

7.5.5. Welfare support is given to those who have been subjected to an incident of verbal abuse or physical assault.

7.6. **All Employees**

7.6.1. Responsible for reporting incidents where they have been subjected to verbal abuse or physical assault, as well as near misses.

7.6.2. Reporting incidents of theft that they are victim of or made aware of.

7.6.3. Following security guidelines and reminders, to ensure measures are taken to prevent incidents of theft and criminal damage, as well as ensuring they are cognisant of security in general and their responsibilities for maintain it in their duties, even without specific direction.

7.6.4. Responsible for, where they have been the victim of an incident of violence and abuse or theft (either of their own personal items or Trust equipment), making the initial report to police and providing a statement.

7.6.5. Must make dynamic risk assessments for all incidents to which they respond, to assess the potential for danger or injury to themselves and balance their obligations to providing emergency care with the safety of themselves, patients, or other members of the public.

7.6.6. Responsible for requesting an identity card and ensuring it is stored securely, kept up to date and not loaned or shared to any other party.

7.6.7. Responsible for making themselves aware of all policies, procedures and guidelines regarding security matters and the protocols they must follow.

8 Audit and Review

8.1. The Trust Lead for Security will ensure that he/she is cognisant of the contents of this procedure; continuously reviewing the content through its use, to ensure it meets the security needs of the Trust, whilst remaining relevant and appropriate prior to its scheduled review.

8.2. All policies have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new policy is approved and disseminated.

8.3. Effectiveness will be reviewed using the tools set out in the Trust's Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).

8.4. This document will be reviewed in its entirety every three years or sooner if new legislation, codes of practice or national standards are introduced, or if feedback from employees indicates that the policy is not working effectively.

8.5. All changes made to this procedure will go through the governance route for development and approval as set out in the Policy on Policies.

9 Equality Analysis

9.1. The Trust believes in fairness and equality, and values diversity in its role as both a provider of services and as an employer. The Trust aims to provide accessible services that respect the needs of each individual and exclude no-one. It is committed to comply with the Human Rights Act and to meeting the Equality Act 2010, which identifies the following nine protected characteristics: Age, Disability, Race, Religion and Belief, Gender Reassignment, Sexual Orientation, Sex, Marriage and Civil Partnership and Pregnancy and Maternity.

9.2. Compliance with the Public Sector Equality Duty: If a contractor carries out functions of a public nature then for the duration of the contract, the contractor or supplier would itself be considered a public authority and have the duty to comply with the equalities duties when carrying out those functions.

10 References

10.1. Healthcare Act 1977

10.2. Assaults on Emergency Workers (Offences) Act 2018

10.3. Investigatory Powers Act 2016

10.4. Offences Against a Person Act 1861

10.5. Theft Act 1968

10.6. Criminal Damage Act 1971

10.7. Criminal Justice Act 1988

10.8. Protection from Harassment Act 1997

10.9. Malicious Communications Act 1988

10.10. Communications Act 2003

10.11. National NHS Security Management Standards

10.12. NHS Violence Prevention and Reduction Standard

10.13. The Department of Health and Counter Fraud Security Management Service – A professional approach to managing security in the NHS

10.14. Health and Safety at Work Act (1974)