**Practice Security and Risk Assessment Policy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Review date:** | **Edited by:** | **Approved by:** | **Comments:** |
| v1 | 20/06/2022 | Sultan Mohamed | Nine Taylor |  |
| v1.4 | 02/10/2024 | Sultan Mohamed | Nine Taylor |  |
|  | October 2026 |  |  | Next review |
|  |  |  |  |  |

**Table of contents**

[1 Introduction 2](#_Toc173752808)

[1.1 Policy statement 2](#_Toc173752809)

[1.2 Status 3](#_Toc173752810)

[2 Premises security 3](#_Toc173752811)

[2.1 General access 3](#_Toc173752812)

[2.2 Staff identification 3](#_Toc173752813)

[2.3 Maintaining awareness 3](#_Toc173752814)

[2.4 Visitor and contractor access 4](#_Toc173752815)

[2.5 Lone working 5](#_Toc173752816)

[2.6 Closed-circuit television 5](#_Toc173752817)

[2.7 Prescription security 5](#_Toc173752818)

[2.8 Medical gases 5](#_Toc173752819)

[2.9 Bomb threat or suspicious package 5](#_Toc173752820)

[2.10 Dynamic lockdown 5](#_Toc173752821)

[2.11 Panic alarms 6](#_Toc173752822)

[3 Organisation security checklist 6](#_Toc173752823)

[3.1 Requirement 6](#_Toc173752824)

[4 Risk assessment 6](#_Toc173752825)

[4.1 Process 6](#_Toc173752826)

[Annex A – Practice security checklist and action plan 7](#_Toc173752827)

[Annex B – Risk assessment template 13](#_Toc173752828)

# Introduction

## Policy statement

The purpose of this policy is to outline the process for conducting a security risk assessment at Sheerwater Health Centre. The organisation faces several risks which must be appropriately assessed and actions taken to mitigate the risks if service users are to continue to receive safe and effective patient care.

Security is the responsibility of all staff at this organisation and it is important staff recognise, understand and act on their responsibility regarding all security matters.

This policy is to be read in conjunction with the organisation’s **Health, Safety and Risk Management Handbook.**

## Status

The organisation aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents). Consideration has been given to the impact this policy might have regarding the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment. Furthermore, this document applies to all employees of the organisation and other individuals performing functions in relation to the organisation such as agency workers, locums and contractors.

# Premises security

## General access

Controlling access at this organisation is particularly difficult given the number of people who visit daily. It is essential only authorised personnel can access staff-only areas within the building.

Staff must ensure that those areas protected with Simplex/key card door locks always remain secure; doors must not be wedged open under any circumstances, nor are codes to be given to patients or visitors. Regular audits will take place to monitor the effectiveness of security controls and the following can be used to support such audits:

* **Internal inspection of premises checklist**
* **External inspection of premises checklist**

Door codes will be changed as follows:

* Every six months
* When a member of staff leaves their role at the organisation
* In the event of a security breach
* At any other time if it is deemed appropriate to do so by the management team

## Staff identification

All staff must wear their NHS identification badge when on the premises as this not only supports security arrangements, but helps patients and visitors to identify staff members.

## Maintaining awareness

To maintain effective security, when entering or leaving staff-only areas, all staff must be aware of ‘tailgaters’ who try to follow them into restricted areas. Staff are permitted to challenge anyone who is trying to access staff-only areas if they do not have the appropriate ID. Should staff have concerns, they are to speak with a member of the management team immediately.

There may be on occasion a requirement for patients to visit staff-only areas, for example for them to meet a member of the management team. In such instances, they are to be issued with a visitor badge and escorted from and back to the reception area.

## Visitor and contractor access

All visitors and contractors are to sign in and out of the organisation in the visitor log. Any visitor or contractor who requires access to staff-only areas will be issued with a visitor badge and escorted by their host when inside staff-only areas.

The organisation’s visitor log contains the following information:

* The date
* Visitor/contractor name
* The company they represent
* Who they are visiting
* Time in and time out
* If applicable, vehicle registration

Upon arrival, reception staff must ensure that visitors and contractors both sign the visitor log and complete the [Third-party confidentiality agreement (incorporating fire safety and risk awareness for visitors)](https://practiceindex.co.uk/gp/forum/resources/third-party-confidentiality-agreement-incorporating-fire-safety-and-risk-awareness-for-visitors.1391/) to ensure that they are fully briefed to act in the event of an emergency.

For fire and risk management reasons, upon leaving the premises, any visitor must sign the visitor log to confirm the individual has left the premises.

The following processes are to be conducted at both the start and end of each day:

1. Opening

The individual responsible for opening the premises (as per the rota) is to enter the building using the nominated door, ensuring that it is secured behind them. They are to then:

* Deactivate the alarm
* Conduct a walk around the building, turning on corridor lighting, etc.
* Open the reception area, turning on computers and other electrical equipment
* Turn on TVs in the waiting area (if applicable)
* Carry out any other actions as briefed by the management team

Staff must not open the premises to patients until there are at least two members of staff present in the building.

1. Closing

All staff have a shared responsibility regarding the security of the organisation. Prior to leaving the premises at the end of the working day, staff must ensure that:

* Where appropriate, all electrical equipment is turned off
* All computers are shut down
* Medical records cabinets are locked (if applicable)
* All windows are shut and locked (if locks are fitted)
* Blinds are closed (if fitted)
* All internal doors are closed and locked (if applicable, i.e., medical records area)

The individual responsible for securing the building (as per the rota) must ensure that they conduct a walk around the building to confirm that all the above actions have been completed. Once they are satisfied, they are to activate the alarm, leave the building and secure the door behind them. Additional security instructions may be given to staff as deemed appropriate by the management team.

Additional information can be found in the organisation’s **Risk assessment – Locking and Unlocking Premises** and the **Key Holder Agreement**.

## Lone working

Detailed guidance on lone working can be found in the organisation’s **Lone Worker Policy.**

## Closed-circuit television

Closed-circuit television (CCTV) is installed at this organisation, with detailed guidance in the **CCTV Monitoring Policy**.

## Prescription security

Guidance relating to the security requirements for prescriptions can be found in the organisation’s **Prescribing Policy**.

## Medical gases

Guidance detailing the security of medical gases can be found in the organisation’s **Medicines and Medical Gases Storage Protocol**.

## Bomb threat or suspicious package

Should the organisation receive any telephone bomb threat warning or a suspicious package is found or received, then the **Suspicious package protocol** is to be adhered to.

## Dynamic lockdown

In the unlikely event that the organisation comes under any form of attack, then the organisation’s [Dynamic Lockdown Procedure](https://practiceindex.co.uk/gp/forum/resources/dynamic-lock-down-procedure.1333/) is to be followed.

## Panic alarms

Should the situation arise where the panic alarm needs to be deployed, then refer to the organisation’s **Dealing with Unreasonable, Violent and Abusive Patients Policy.**

This organisation will undertake regular refresher training to ensure all staff understand how to respond when the panic alarm sounds.

# Organisation security checklist

## Requirement

This organisation will undertake an annual security check of the premises and its contents (using the template at [Annex A](#_Annex_A_–)) to ensure that the organisation has adequate provision to safeguard and protect members of staff, patients, the building and other physical assets including sensitive and personal information.

The identification of risks raised within this document to address any gaps or weaknesses in provision should be evaluated by way of a formal risk assessment. Staff should be aware of the need to report any areas of concern to the Practice Manager so appropriate action can be taken.

# Risk assessment

## Process

Detailed guidance on the completion of risk assessments can be found in the organisation’s Health, Safety and Risk Management Handbook. A risk assessment template for premises security can be found at [Annex B](#_Annex_B_–). .

Sheerwater Health Centre has a Security Risk Assessment template available on private practice website, also included here in Annex B.

Alternative template information and risk assessment templates are given here in Annex A & B for further information and use if required.

# Annex A – Practice security checklist and action plan

This organisation has undertaken a security check of the premises and its contents to ensure the organisation has adequate provision to safeguard and protect members of staff, patients, the building and other physical assets including sensitive and personal information.

A series of questions outlined in the attached document have resulted in the organisation acknowledging what measures it has in place to support any potential risks/hazards that may arise in the event of any incidents. Each question has had its answer risk assessed using the following criteria:

|  |  |
| --- | --- |
| **Risk** | **Actions** |
| Extreme | Could have a serious impact on the delivery of patient care, the security of the building, its contents, staff and confidential/sensitive information (action required) |
| High | Could have an impact on the delivery of patient care, the security of the building, its contents, staff and confidential/sensitive information (action required) |
| Medium | Some impact on the delivery of patient care, the security of the building, its contents, staff and confidential/sensitive information security (action to be considered) |
| Low | Short term disruption to service with low impact on the delivery of patient care, the security of the building, its contents, staff and confidential/sensitive information security (no action deemed necessary) |

The identification of risks has been raised within this document to address any gaps or weaknesses in provision by way of a formal risk assessment. Staff are aware of the need to report any areas of concern to the Organisation Manager so that appropriate action can be taken.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Question** | | **Response** | **Risk level**  **E/H/M/L** | **If action required**  **person responsible, action/target date for completion and/or detail risk assessment number for those where a high level has been attributed** | **Completion date** |
| What security measures are in place to safeguard the outside of the building? (fences, lockable gates, restricted access) | |  |  |  |  |
| Is there any security to monitor the outside of the building? (CCTV, security company surveillance) | |  |  |  |  |
| Does the building have an alarm system that is serviced annually and supported by a maintenance contract? | |  |  |  |  |
| Does the security system cover all areas of the building – in particular, rooms that contain IT equipment or records? | |  |  |  |  |
| Is the security system connected to a police station or a call response centre? | |  |  |  |  |
| How often is the security alarm code changed? | |  |  |  |  |
| Are there warnings on windows, visible alarms, etc. that warn potential intruders that there are physical security measures in place? | |  |  |  |  |
| What types of lighting does the building have to the outside and does this adequately protect staff when they enter/leave? (Security lighting, flood lighting, street lighting) | |  |  |  |  |
| How are external doors protected? (e.g., 5 lever locks or equivalent) | |  |  |  |  |
| How are fire and external doors secured? (e.g., kept closed when not in use) | |  |  |  |  |
| Do all windows have locks that are secured when rooms are not in use? | |  |  |  |  |
| How are rooms secured when not in use? | |  |  |  |  |
| How is access restricted to the reception and administrative areas of the buildings? | |  |  |  |  |
| What types of security devices are in place to safeguard internal doors to rooms that hold IT equipment/patient records? (e.g., keypads/swipe cards/locks) | |  |  |  |  |
| What security measures are in place to protect areas where private and confidential information is stored? | |  |  |  |  |
| What policy is in place for ensuring that windows, blinds and doors are closed, locked and checked at the end of every working day? | |  |  |  |  |
| When the building is not fully occupied, how are unused areas secured? | |  |  |  |  |
| What provision does the organisation have for keeping keys safe? | |  |  |  |  |
| Is there an agreement in place for members of staff or associates who have keys/keypad codes/swipe cards to access the building? | |  |  |  |  |
| How often are keypad codes changed? | |  |  |  |  |
| Does the organisation have a signing in/out policy for attached staff? | |  |  |  |  |
| Are ID badges always worn by staff? | |  |  |  |  |
| How does the organisation identify visitors on their premises? (e.g., visitor badges, work permits) | |  |  |  |  |
| Does the organisation have a procedure for challenging unidentified visitors in controlled areas which has been made available to staff? | |  |  |  |  |
| How are deliveries to the organisation supervised? (e.g., stationery orders) | |  |  |  |  |
| How frequently is the asset register reviewed and updated? | |  |  |  |  |
| Is all IT equipment asset marked? | |  |  |  |  |
| How does the organisation monitor the movement of portable IT equipment used outside of the building? | |  |  |  |  |
| Where are laptops and other items of portable equipment stored overnight? | |  |  |  |  |
| Indicate if the organisation has a protocol for transporting confidential information off-site and where it can be found. | |  |  |  |  |
| Where is the clinical system server located and what safeguards are in place to ensure it security? | |  |  |  |  |
| What provision does the organisation have to ensure that the clinical system server is protected by an uninterrupted power supply? | |  |  |  |  |
| Does the organisation have a business continuity plan that covers loss of premises, computer systems, utilities, essential supplies, security systems, paper records, clinical/non-clinical cover? | |  |  |  |  |
| How will the business continuity plan be tested for effectiveness? | |  |  |  |  |
| **Additional notes/comments** | | | | | |
| **Completed by**  **name and role** |  | | **Date completed** |  | |
| **Signature** |  | | **Review due** |  | |

# Annex B – Risk assessment template

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk assessment title** | **Premises security** | **Date of assessment** | **08/08/2024** |
| **Assessment conducted by** | **L H Jones (Ops Mgr)** | **Date of next review** | **08/08/2025** |
| **Contributors** | **P O Smith (PM)** | **Risk reference** | **17/24** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| What are the potential hazards? | Who is at risk of being harmed and how? | What are you already doing to control the risks? | Risk rating | Additional control measures required | To be implemented: by who, by when? | Residual risk |
| Poor security measures may result in unwarranted access to restricted areas, access to sensitive information and theft of assets. | Staff and patients may experience psychological trauma should confidential information be accessed by unauthorised individuals or personal property is stolen. | All staff receive regular refresher training in security arrangements.  CCTV monitors are in place and there is an extant [policy](https://practiceindex.co.uk/gp/forum/resources/cctv-monitoring-policy.950/).  There are effective locking and unlocking procedures in place, supplemented by a robust [risk assessment](https://practiceindex.co.uk/gp/forum/resources/risk-assessment-locking-and-unlocking-premises.1642/).  Security lighting is in place around the premises.  Key security is supported by a robust [Key Security and Key Holding Policy](https://practiceindex.co.uk/gp/forum/resources/key-security-and-keyholding-policy.1280/).  All staff always wear ID badges.  Visitor management is effective, supported by a [Third party confidentially agreement incorporating fire safety and risk awareness for visitors](https://practiceindex.co.uk/gp/forum/resources/third-party-confidentiality-agreement-incorporating-fire-safety-and-risk-awareness-for-visitors.1391/).  All staff-only areas are protected by effective locking mechanisms. | 9 | Monitor refresher training to ensure staff compliance  Review policy annually  Review the security arrangements for premises on a regular basis  Check lighting effectiveness regularly  Conduct spot checks of key holding record to ensure accuracy  Conduct security audits to monitor compliance. | Ops Mgr – ongoing  PM – every 12 months  Ops Mgr – ongoing  Ops Mgr – ongoing  PM – ongoing  PM – ongoing | 3 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | **Likelihood** | | | | |
| 1  Rare | 2  Unlikely | 3  Possible | 4  Likely | 5  Almost certain |
| **Consequence** | 5  Catastrophic | 5  Moderate | 10  High | 15  Extreme | 20  Extreme | 25  Extreme |
| 4  Major | 4  Moderate | 8  High | 12  High | 16  Extreme | 20  Extreme |
| 3  Moderate | 3  Low | 6  Moderate | 9  High | 12  High | 15  Extreme |
| 2  Minor | 2  Low | 4  Moderate | 6  Moderate | 8  High | 10  High |
| 1  Negligible | 1  Low | 2  Low | 3  Low | 4  Moderate | 6  Moderate |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Security Risk Assessment** | | | | | | | |
|  |  |  |  |  |  |  |  |
| **Address** |  |  |  |  |  |  |  |
| **H&S Responsible Partner** |  |  |  |  |  |  |  |
| **H&S Lead** |  |  |  |  |  |  |  |
| **Date** |  |  |  |  |  |  |  |
| **Assessors** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **SOURCE OF RISK** | **YES /NO/NA** | **LIKELIHOOD OF OCCURANCE (L,M,H)** | **SEVERITY OF OUTCOME (L,M,H)** | **RISK RATING** | **CONTROL MEASURES** | **ACTIONS TO IMPROVE CONTROL MEASURES** | **DATE OF COMPLETION** |
| **Are all windows locked as part of the closing procedure & blinds closed?** |  |  |  |  |  |  |  |
| **Are doors locked as part of the closing procedure?** |  |  |  |  |  |  |  |
| **Is there an Intruder alarm fitted and does it cover the whole of the surgery?** |  |  |  |  |  |  |  |
| **Does the surgery have CCTV installed?** |  |  |  |  |  |  |  |
| **Does the reception door have a keypad lock and is there a shutter or teller style protected front?** |  |  |  |  |  |  |  |
| **Are key pad codes and alarm codes changed regularly?** |  |  |  |  |  |  |  |
| **Are all keys stored on site not obvious and easy to access?** |  |  |  |  |  |  |  |
| **Is petty cash kept to a minimum & locked in a secure area?** |  |  |  |  |  |  |  |
| **Are all doors restricting public access locked when not in use?** |  |  |  |  |  |  |  |
|  |
| **Is there security lighting? Including Emergency Lighting?** |  |  |  |  |  |  |  |
| **Do all fences, boundaries, gates have Prikka strips or anti vandal paint.** |  |  |  |  |  |  |  |
| **Is the fire policy followed and all staff informed?** |  |  |  |  |  |  |  |
|  |
| **Are all vaccine fridges locked and keys secured?** |  |  |  |  |  |  |  |
| **Are all server rooms locked and restricted access?** |  |  |  |  |  |  |  |
| **Do staff wear identification badges?** |  |  |  |  |  |  |  |
| **Are all waste bins locked?** |  |  |  |  |  |  |  |
| **Is there lone working at the site and have health risk assessments been included in the lone working risk assessment? Is there a Lone Working policy** |  |  |  |  |  |  |  |
| **Are prescriptions stored in a locked area.** |  |  |  |  |  |  |  |
| **Is there a Security Policy in place to include opening & closing procedures and are staff aware?** |  |  |  |  |  |  |  |
| **Are there Lockers provided for staff personal belongings?** |  |  |  |  |  |  |  |
| **Do the staff have access to panic alarms?** |  |  |  |  |  |  |  |
| **Are all data consoles locked and key access restricted?** |  |  |  |  |  |  |  |
| **Is there a Business Recovery Plan in situ?** |  |  |  |  |  |  |  |
| **Is there a staff list on who has access to key holding and fobs?** |  |  |  |  |  |  |  |
| **Are emergency drug cupboards locked as part of the closing procedure?** |  |  |  |  |  |  |  |
|  |
| **Are patient notes rooms locked at all times?** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  | **LIKELIHOOD** | | |  |  |  |
| **RISK RATING Severity x likelihood** |  | **LOW** | **MEDIUM** | **HIGH** |  |  |  |
|  |
| **SEVERITY HIGH** |  | Medium | High | High |  |  |  |
|  |
| **SEVERITY MEDIUM** |  | Low | Medium | High |  |  |  |
|  |
|  |
| **SEVERITY LOW** |  | Low | Low | Medium |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **Review date:** |  |  |  |  |  |  |  |
| **Reviewed By:** |  |  |  |  |  |  |  |
| **Signature:** |  |  |  |  |  |  |  |