

SECURITY INCIDENT REQUIRING CONTROLLED HOSPITAL ACCESS - CHW

POLICY AND PROCEDURE[®]

DOCUMENT SUMMARY/KEY POINTS

- CHW is required to ensure, in consultation with staff and key stakeholders, that all reasonably foreseeable security risks associated with access to and egress from buildings are identified, assessed, eliminated where reasonably practicable or, where they cannot be eliminated, effectively minimised.
- In the event of a security incident, the Hospital may be required to control access to parts of the building.
- The extent of the area affected may be:
 - A ward or department
 - The whole of Hospital
- The control of access may be at one of the following levels:
 - Monitored - movement of staff, patients, visitors, and public is monitored but not restricted. This may be used when screening for a particular individual.
 - Restricted - movement of staff, patients, and visitors for essential purposes only. No public access.
 - Lockdown - no movement of staff, patients, and visitors.
- The decision to control access to the whole Hospital (Lockdown) is authorised by the Hospital Disaster Controller (HDC) in consultation with the Security Manager and Chief Executive.
- The decision to control access to a ward or department is authorised by the Nursing Unit Manager or Department Head in consultation with Security Manager and Clinical Stream Director.
- Security staff are responsible for implementing and maintaining the controlled access.
- Controlled access to the Hospital continues until directed by the Hospital Disaster Controller.

Approved by:	SCHN Policy, Procedure and Guideline Committee	
Date Effective:	1 st January 2025	Review Period: 3 years
Team Leader:	Manager	Area/Dept: Corporate Services

CHANGE SUMMARY

- Due for mandatory review. No major changes to practice

READ ACKNOWLEDGEMENT

- All CHW managers, security staff and other relevant staff as identified are to read and acknowledge they have understood the contents of this policy.

TABLE OF CONTENTS

Policy	3
Procedure	4
Controlled Access - Security Risk Management	4
Controlled Access Design	5
Controlled Access to Whole Hospital	5
Controlled Access to Staff Accommodation	5
Controlled Access to CHW Emergency Department	5
Controlled access to a Department	6
Fire Doors and Alarms	6
Additional staffing	7
Notification of Controlled Access	7
Staff Responsibilities	7
Stand-down - returning to normal status	7
Conclusion	8
Further Information	8
Appendix 1 Hall Ward Evacuation Plan	9

Policy

- The Hospital will ensure that there are documented and effective access and egress control procedures and perimeter control, for the implementation of controlled access to a ward or department and/or whole of Hospital.
- The Hospital will ensure a security risk management approach is taken for all reasonably foreseeable risks associated with access and egress. Consultation with staff and key stakeholders will occur for the identification, assessment and, where reasonably practicable, elimination of risks or, where they cannot be eliminated, effectively minimised.
- The Hospital secures access to all perimeter entry/exits points after hours and controls access during business hours to high risk areas based on the level of risk, safety of staff, vulnerable areas and securing vulnerable patients and others in the workplace.
- The Hospital secures access to ward areas. Office areas are secured overnight when they are not in use.
- In the event of a security incident, the Hospital may be required to control access to some areas.
 - The extent of the area affected may be:
 - A ward or department
 - The whole Hospital
 - Controlled access may be at one of the following levels:
 - Monitored - movement of staff, patients, visitors and public is monitored but not restricted. This may be used when screening for a particular individual.
 - Restricted - movement of staff, patients and visitors for essential purposes only. No public access.
 - Lockdown - no movement of workers, patients and visitors.
- The decision to control access (Lockdown) to the whole Hospital is authorised by the Hospital Disaster Controller (HDC) in consultation with the Security Manager and Chief Executive.
- Notification of an incident is displayed by Security staff at Hospital entrances. Staff are notified via the Disaster alert paging system, computer pop up communication, text messaging and/or their Manager. To maintain controlled access, staff entering the Hospital must use authorised swipe card identification.
- Outlying areas of the Hospital are informed of the situation by Security staff, including NETS, the Medical Centre and Ronald McDonald House. Retail facilities within the Hospital are also informed, as directed by the HDC.
- Security staff are responsible for implementing and maintaining the controlled access. In the event of controlled access to the whole Hospital, the Security Manager and Manager, Corporate Services indicate the number of extra Security staff required and

advise the HDC. Security staff brief the support staff on the required procedures, ensuring they are in a safe situation. Local staff maintain controlled access to a ward or department.

Controlled Access continues until indicated by the appropriate authority or advised by the HDC that it is no longer required. Security staff are informed about the change in status. Access then returns to the normal level.

Procedure

Controlled Access - Security Risk Management

CHW Management will ensure, in accordance with the [Security Manual \(Protecting People and Property\)](#), that access control systems are in place to minimise the risk of unauthorised entry.

Factors that may impact the risk of unauthorised entry include; vulnerable areas, securing vulnerable patients, the nature of items stored (e.g. drugs, confidential records, cash). A security risk management approach is taken when determining if access controls are required, in consultation with staff and key stakeholders. Utilisation of the WHS risk assessment tool will assist document identified risks, assessment of risk, determine risk level and consideration for effective control strategies where risks cannot be eliminated.

Access control measures involve:

- Planning and developing local procedures in consultation with relevant key stakeholders to implement and assess appropriate security control measures is required for the risk management of any persons or individuals who currently have an AVO (Apprehended Violence Order) in place and/or is a registered sex offender.

Controls and measures may include:

- Additional Security personal to escort and monitor each visit
- Lockdown of wards
- Visiting restrictions
- Sign in and sign out at the Security department
- Appropriately securing the facility's access points, including doors and windows
- Appropriately controlling access to the facility's perimeters (e.g. fences, roads, traffic, and pedestrian access and flow)
- Providing safe egress, especially after hours and during emergencies
- Controlling egress to vulnerable areas
- Providing clear signage
- Staff identification systems that allow all staff to be identified

In relation to access, the following risk control strategies should be considered:

Perimeter doors are locked and access is restricted to the minimum number of necessary entry points in the building, especially at night. Perimeter doors are to meet the building

design standard AS4145.2-2008/Amdt1-2009 /Amdt2-2015 Locksets – Mechanical locksets for doors in buildings.

Fire isolation exit doors meet the requirements of the Building Code of Australia and relevant Australian Standards.

Controlled Access Design

In accordance with the Security Manual, security related risks should be considered during planning and design of new or refurbished work areas for the prevention and management of controlled access. In particular, controlled access systems must be considered for high-risk areas, securing vulnerable patients and vulnerable areas, based on a security risk management approach.

The planning and design stages of new or refurbished work areas should consider crime prevention through environmental design principals as part of the project, to assist in managing risks associated with access control.

Controlled Access to Whole Hospital

Security will lock and secure all external access managed via the access control system. The remaining external doors and those deemed necessary to the management of the incident will be manually locked and secured by Security staff.

The single entry door adjacent to the Hospital's main entry, Forecourt airlock, Kids Garden airlock and the staff entrance at the Clinical Genetics corridor will be the access/ egress points for all staff who have authorised swipe identification card access capability.

Signs notifying staff and visitors that an incident is underway will be displayed by Security at Hospital entrances.

Controlled Access to Staff Accommodation

The CHW staff accommodation has controlled access for authorised staff with a key or authorised swipe identification issued by the Security Department.

The staff accommodation area must be secure at all times, provide safe access and egress, be well lit, and windows, doors and locks properly secured.

Controlled Access to CHW Emergency Department

Controlled access to the CHW ED is managed by Westmead Hospital Security, supported by CHW Security, as required.

Controlled access to a Department

- Depending on the area involved, access can be restricted with approval as noted above
- Security will secure key-operated internal perimeter doors, as necessary
- The requested department's main entry doors will be secured
- Egress in the event of a fire will be maintained (see below)

Time frame

- Securing the doors via the access control system takes approximately 5 minutes
- Manually securing the external perimeter doors takes between 20-25 minutes
- Where specific departments require controlled access, the time required for the completion of this task will depend on the size of the area to be secured

Access

There are various levels of control access as noted above:

- Monitored - movement of staff, patients, visitors and public is monitored but not restricted. This may be used when screening for a particular individual.
- Restricted - movement of staff, patients and visitors for essential purposes only. No public access.
 - Access to wards or swipe card controlled areas is via programmed staff ID cards, to allow access via the card holder only
 - Access to key operated departments within CHW will be provided by Security staff or staff in possession of departmental master keys
 - The Medical Centre can be accessed via programmed staff ID cards
 - Access for families to the wards can only be provided by staff working in that area who identify the family
- Lockdown - no movement of staff, patients and visitors

Fire Doors and Alarms

Impact on fire protection systems:

- The external fire doors will be secured from the outside however this will not prevent use of the doors as an exit during an emergency, except in Hall Ward ([Appendix 1](#))
- The single door at the Hospital main entry will be staffed by Security staff (or delegate) to enable controlled access
- In the event of fire alarm activation, all doors in the affected area secured by electric door locks will automatically release, except in Hall Ward ([Appendix 1](#)). The unsecured doors will be physically resecured by Security staff once the fire alarm has been reset by Fire and Rescue NSW

- If the doors in the affected area do not release to close automatically, staff should press the clear cover on the white manual call point holding the door back which releases the door

Additional staffing

Where there is insufficient Security staff available, the Hospital Disaster Controller will provide additional staff to assist with access control. The staff will be briefed by Security staff, ensuring they are in a safe situation.

Notification of Controlled Access

- When access is controlled to a ward or department, staff are notified by their Manager. Patients and visitors in those areas are informed by local staff
- When access is controlled to the whole Hospital, staff are notified via the Disaster alert paging system, the computer communication system, text messaging and/or their Manager. Managers are to ensure their staff are made aware of the controlled access situation. Signs notifying staff and visitors that controlled access is in place are displayed at Hospital entrances

Staff Responsibilities

- Notify Security staff immediately in the event of a breach during controlled access
- Use the duress alarm or call the emergency number 2222, should assistance be required. Refer to CHW Emergency Guide (Flip Chart) located near telephones
- If in doubt, do not provide access, contact Security Department immediately on 9845-2000
- Security staff dealing with aggressive people should refer to the [Code Black](#) policy
- Report all incidents relating to breach of controlled access on IIMS+
- Complete relevant training in relation to Hospital Security

Stand-down - returning to normal status

Security will return the secured doors to their normal operating status via the access control system, as directed by the Hospital Disaster Controller or for controlled access of a department, by the Department Head and the Clinical Stream Director.

Conclusion

The processes for controlling Hospital access are designed to run in conjunction with any directives from the Hospital Disaster Controller. They aim to provide a reasonable level of security for staff, patients and visitors. Due to the layout of the Hospital, absolute access control may not be possible. Staff should advise Security staff if breaches occur during controlled access.

Further Information

Refer to:

- Disaster Response Plan – CHW HealthPlan:
<http://webapps.schn.health.nsw.gov.au/epolicy/policy/4116>
- NSW Health Policy and Standards for Security Risk Management in NSW Health Agencies – Protecting People and Property:
<https://www.health.nsw.gov.au/policies/manuals/Pages/protecting-people-property.aspx>
- Australasian Health Facility Guidelines-Part C, Design for Access, Mobility, OHS & Security C.0006 – Safety and Security Precautions, Revision 5.0, 1 March 2016.

Copyright notice and disclaimer:

The use of this document outside Sydney Children's Hospitals Network (SCHN), or its reproduction in whole or in part, is subject to acknowledgement that it is the property of SCHN. SCHN has done everything practicable to make this document accurate, up-to-date and in accordance with accepted legislation and standards at the date of publication. SCHN is not responsible for consequences arising from the use of this document outside SCHN. A current version of this document is only available electronically from the Hospitals. If this document is printed, it is only valid to the date of printing.

Appendix 1 Hall Ward Evacuation Plan

ASSEMBLY POINT – Hall Ward Secure Grassed Area

Fire Wardens: NUM or Team Leader

Code Red:

When the alert tone sounds, all staff should check the area for signs of smoke and fire. If found, dial 2222 and report to Manager or person in charge.

Ensure that R.A.C.E and Code Red emergency procedures are followed:

REMOVE	people from immediate danger (behind smoke and fire doors)
ALERT	raise the alarm by dialling 2222 and state Code Red, the exact location and your name and title
CONTAIN	the fire by closing any doors or windows
EXTINGUISH	only if it is safe to do so using appropriate equipment and if you have been trained
EVACUATE	to a safe area or exit the building and proceed to a designated assembly point

IF THERE IS NO FIRE IN THE AREA, WAIT FOR FURTHER INSTRUCTION FROM SECURITY. WHEN IN DOUBT, GET OUT

1. Team Leader and one allocated staff member should check all patient waiting areas and treatment/consultation rooms as well as staff offices in Hall Ward to check if they are occupied and advise occupants that the unit is on Code Red standby, and they should await further instruction on whether to evacuate.
2. If it is a false alarm, Security will advise a stand down before the evacuation tone begins.
3. If it is a genuine evacuation, Security will advise. However, if Security has not yet arrived at the fire panel by the time the evacuation tone begins, the Team Leader must make the decision on when to evacuate. If in doubt; evacuate.

When the decision to evacuate is made, the Team Leader will take command and:

1. Identify safest exit route to evacuate. DO NOT USE LIFTS
2. If safe to do so, notify adjoining areas of all incidents of fire/smoke
3. Supervise the preparation of staff for evacuation
4. Collect staff list/roster and patient fireboard to assist with roll call
ONLY IF SAFE TO DO SO
5. Check all isolated areas
6. If safe, turn off all services (medical gases, electrical equipment etc)

7. If safe, the person in charge is to complete a final check of the area when the last staff member has been evacuated to make sure nobody has been left behind and notifies the NSWFR of any persons unaccounted for
8. Proceed to the evacuation assembly point and conduct a roll call (maintain written record)
9. Liaise with responding emergency services

If the pager system is down:

Hall Ward to utilise mobile/ward phones to communicate.

When the Fire/smoke alarms are activated:

Fire doors unlock - to mitigate the risk, if safe to do so, allocate a staff member to stand in front of the doors to prevent patients from absconding.

Main entry door to Hall Ward unlock but remain closed.

Doors into patient areas remain locked during fire alarm and must be opened with a swipe card or key.

Internal and External Fire Evacuation process:

All staff must direct all patients to the evacuation assembly point: Hall Ward Secured Grassed Area

Location of Keys:

- Casual keys/swipes are located in a locked cupboard in the NUM's office, which is signed in an out by the casual staff member. If the NUM is not available, Security are able to open the NUM office door.
- Hall Ward staff have a swipe card and their own universal key which opens all doors. Staff also have a smaller key which opens cupboards on the unit. The Hall Ward CSO has a key register and maintains a record of all staff who have keys. Security also have a record of staff with a universal key.
- The S4/S8 key is carried by the team leader of each shift
- If the swipe card access deactivates during a fire alarm, individual staff are to use their allocated ward keys to open doors in order to exit to the assembly point

Role of ward staff members:

- Team Leader to allocate staff to assigned duties
- Allocated staff member to review the patient fireboard and staff roster to ensure all patients and staff are accounted for
- Allocated staff members to move patients to fire exit and evacuation assembly point