AUCKLAND
DISTRICT HEALTH BOARD
Te Toka Tumai

Auckland DHB
Chief Executive's Office
Level 1
Building 37
Auckland City Hospital
PO Box 92189
Victoria Street West
Auckland 1142
Ph: (09) 630-9943 ext: 22342
Email: ailsac@adhb.govt.nz

7 July 2020

[redacted]

Re OIA Request – Policies on reporting of unsafe, harmful and criminal behaviour

I refer to your official information request dated 17 June 2020 to the MoH. The MoH transferred a partial request to Auckland DHB on 23 June 2020. You request the following additional information:

I request a copy of all DHB policies in regards to reporting unsafe, harmful, criminal behavior, including the re-routing and interception of private communications, and policies on how they document such incidents and how they are to safeguard against such incidents, as the Operational Framework does indeed require every DHB to have such policies."

We have attached the following policies:

- Incident Management - Guideline
- Workplace violence and aggression management
- Trespass notice
- Code Orange Policy
- Security
- Information Privacy and Security
- Protected disclosures

You are entitled to seek a review of the response by the Ombudsman under section 28(3) of the Official Information Act. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Please note that this response, or an edited version of this response, may be published on the Auckland DHB website.

Yours faithfully

Ailsa Claire, OBE
Chief Executive

Incident Management - Guideline

Document Type	Guideline
Function	Clinical Administration, Management and Governance
Directorate(s)	All Auckland District Health Board (Auckland DHB) directorates
Department(s) affected	All Auckland DHB departments & services
Patients affected (if applicable)	All Auckland DHB patients
Staff members affected	All Auckland DHB staff members
Key words (not part of title)	Adverse event, incident, Root Cause Analysis (RCA), Severity Assessment Code (SAC), accident, patient safety, harm, systems analysis, Just Culture
Author - role only	Director: Quality & Assurance
Owner (see ownership structure)	Chief Health Professions Officer
Coordinator	Clinical Policy Advisor
Date first published	28 February 2017
Date this version published	29 May 2018 - role titles 24/7 hospital functioning
Review Frequency	3 yearly
Unique Identifier	PP01/PCR/100 - v01.02 - minor version

Contents

Content Cont'd

Back to Contents

1. Purpose of guideline

Auckland District Health Board (Auckland DHB) recognises its responsibility in providing safe, effective and efficient healthcare for patients, and a safe environment for patients' families/whānau, staff, contractors, external personnel, students, volunteers and visitors.

The purpose of this guideline is to provide clear guidance on how to use the Auckland DHB Incident Management Framework, and outline its implications for reporting consistency with the National Reportable Events Policy, Worksafe New Zealand, Ministry of Health, ACC, the Health and Disability Commissioner and other regulatory requirements that may arise.

See Definitions and abbreviations in appendices

2. Summary

Auckland DHB is committed to ensuring a safety culture, following a systems approach that is embodied in the Incident Management Framework detailed below. In summary this will be achieved through:

1. Notifying of incidents when they occur or when they become apparent.
2. Informing patients, staff or their authorised representatives of any incident or accident which has created harm or has the potential to create harm to the patient or Auckland DHB staff.
3. Assessing each incident using the Auckland DHB Severity Assessment Code (SAC) (see appendices), excluding health and safety incidents.
4. Reporting of all incidents with a SAC of 1 or 2 to the Quality Department.
5. Immediately escalating to the appropriate manager or clinical leader an incident that is likely to result in media attention.
6. Ensuring all incidents are investigated. The nature of the investigation will be determined by the risk rating of the incident or the level of harm sustained by the person.
7. Ensuring that corrective actions and quality improvements are designed, implemented and evaluated to minimise the risk of recurrence of a similar incident.
8. Advising staff of actions taken to prevent recurrence of incidents and accidents and ensuring that these lessons are shared across Auckland DHB.

3. Scope

This guideline applies to any incident resulting in harm, loss or damage, to any person, property or environment, including near miss events occurring in any Auckland DHB-controlled site or location deemed to be an Auckland DHB 'Place of Work'.

This procedure is applicable to:

1. Any consumer or visitor within Auckland DHB places of work
2. All Auckland DHB workers (full-time, part-time, casual and temporary), and associated personnel (including contractors, students, visiting health professional etc.) working in, or contracted to provide a service on any Auckland DHB site.

Back to Contents

3. Any person undertaking work activity on an Auckland DHB controlled site, eg sales representative, stall holder.

Exceptions

This guideline does not apply to the management of complaints, unless an incident is identified as part of the complaint, in which case the incident will be investigated before the complaint process is completed.

1. Complaints from patients or their representatives are managed in accordance with the Consumer Complaint Management Policy (see associated Auckland DHB guidelines).
2. Staff complaints or grievances should be made in writing to the staff member's manager and not made on an Incident/Accident/Near Miss Notification Form (incident form).

4. Incident Management Framework

Incident management is a continuous process with many components. It is not simply about reporting incidents. The process involves 10 key steps - see Incident Management Framework flow diagram in appendices.

Step 1. Incident Identification

An incident is an unplanned event that results in, or has the potential to result in, injury, damage or loss. In this document the scope of an 'incident' also includes accident, and also applies to clinical and non-clinical events:

- Clinical: an event unrelated to the natural course of the illness and differs from the expected outcome of patient management.
- Product Fault: an event where a consumable product or medical device has failed in its intended purpose.
- Health and Safety: An event relating to a hazard, work injury or serious harm, involving employees, contractors, sub-contractors, students and volunteers.

An incident may be minor (eg medication error with no harm, piece of equipment goes missing, loss/unavailability of clinical record), moderate (eg additional monitoring, investigations or interventions as a result of incident, patient reacts to medication which should have been withheld) or serious (see serious adverse event/serious harm in Definitions and abbreviation).

Line managers are responsible for ensuring that staff understand what constitutes a patient "incident" and how it differs from a complication of care (see Definitions and abbreviations in appendices).

The first step in managing incidents is recognising and identifying them. Incidents may be identified:

- By direct observation or facilitated discussion
- By clinical staff or patient during or following patient care
- By a patient or family/whānau member expressing concerns or complaints to a staff member
- By the consumer liaison team when they are assessing complaints
- By the Quality Department

- From ACC reports
- From Coroner's report
- From clinical record audits
- From morbidity/mortality reviews

Note: If an incident results in, or is linked to a complaint, it must be investigated and managed in the first instance as an incident, but also responded to as per the Consumer Complaints Management Policy (see associated Auckland DHB guidelines).

If an incident is identified in the complaint, the incident must be reported in the Incident Management System by the Quality Department in conjunction with the main directorate involved.

Step 2. Immediate Action

Following identification of an incident it may be necessary to take immediate action to mitigate the harmful consequences of the incident. Such action would potentially include support for the person involved, their family and/or the staff involved in the incident. Immediate action may also be needed to make the local environment safe eg the removal of a hazardous substance. Call for assistance/advice as necessary.

On discovering an event, preventive or corrective action must be initiated immediately to ensure person(s) safety and wellbeing. This may include:

- Additional medical treatment
- Placing the patient in a safe environment
- Replacing faulty equipment
- Withdrawal of a service in the interests of patient safety

In the event of serious harm to a **staff member**, where possible the scene of the incident should be secured by the person in charge of the workplace and notified accordingly to Health and Safety policy (see associated Auckland DHB documents).

For all incidents resulting in harm or possible harm to a **patient**, the information about the event must be given to the person involved and/or carer as soon as it is practicably possible (at least within 24 hours of the event becoming known) in an open and honest manner. This process is called 'Open disclosure' and is described on the next section.

In some situations it is also appropriate to secure items such as the patient's clinical record or the equipment used as it may be required for the review of the event.

Step 3. Open Disclosure

Open disclosure of information to patients and their representatives has four key components:

1. Acknowledgement of and/or expression of regret to the person involved, family/whānau that the incident occurred,
2. An undertaking that an investigation will be done to determine why the event occurred,
3. Disclosure of the facts determined by the review to the person involved and their family/whānau where appropriate and
4. Providing support for those involved - patients, families, carers or staff - to cope with the physical and psychological consequences of what happened.

Back to Contents

The points below should be included when communicating with the patient and/or responsible person:

- Involve a senior staff member/manager to disclose SAC 1 & 2 events. When an event is scored at 3 or 4 the health professional with overall responsibility for the consumer's care (or their delegate) must disclose the incident.
- Factual explanation of what happened.
- Explain any potential consequences for patient.
- Outline what steps have been taken to manage the event and prevent reoccurrence.
- Timeframe for investigation, type of investigation and method of feedback to patient and/or responsible person (family/6hanau member or other person).
- Contact details of staff member who will maintain ongoing relationship with patient or responsible person (family/whānau member or other person).
- Consideration to the consumer's cultural and ethnic identity and first language, and the support they require.
- For Māori, please contact He Kamaka Oranga.
- For a Pacific patient and family, please contact the Pacific Family Support Unit.
- Provide copy of '*Your Rights*' (see other resources) leaflet which includes how to make a complaint & support services available.
- Provide consumer with information on the Health and Disability Commission (HDC) advocacy service.
- Advise that they may be eligible to make an ACC Treatment Injury claim for costs related to an injury arising from an event. Provide information on the claims process and initiate medical forms (ACC45 & ACC2152 - see Forms) as appropriate, as soon as possible.
- Disclosure and subsequent action must be detailed in the patient's clinical record.
- Provide an apology for any harm suffered. This is Auckland DHB's opportunity to say "*We are sorry that this happened to you*". The apology is about acknowledging the seriousness of an incident and the distress that it caused. It is not about apportioning blame for the event happening. Further information about open disclosure is provided by the Health & Disability Commission (see also Feedback and Learning)

The focus of open communication is to answer questions in a manner that satisfies the person of the honesty of the communication. It primarily encompasses communication between health care providers and patients/carers and may include a factual explanation of what happened, the potential consequences and what steps are being taken to manage the event.

Step 4. Notification/Reporting

Any employee of Auckland DHB who identifies an incident can and should notify it by completing the Incident Form (see appendices) using the Incident Management System. The Incident Form should preferably be completed by the staff member involved in the incident, but may also be done by any staff member who becomes aware of the incident.

The Incident Form must be completed as soon as possible, preferably before the end of the working day/shift **but no longer than 24 hours**. Notifications must be legible and stated in an objective, factual and professional manner. Opinion and subjective comments should be avoided. Identification of staff involve should be avoided. If unsure, advice may be sought from the Quality Department.

Back to Contents

Note: An Incident Form must **not** be completed by patients, clients or visitors

Where the incident has:

- Resulted in patient harm arising from clinical treatment - an ACC Treatment Injury Form 2152 must also be completed (if relevant). The line manager receiving an incident form must review the incident and ensure that appropriate immediate interventions, open disclosure and corrective actions have been taken to minimise any further harm/loss.
- Involved a patient - documentation describing what occurred, any care provided to the patient and that the issue has been discussed with the patient/family is to be completed in the patient's clinical record, stating the number of the incident form used to notify the incident.

Note: A copy of the incident form must **not** be filed in the patient's clinical record.

- Involved a staff member, student, visitor or contractor - medical attention should be sought as required, and an incident form must be completed and sent to the Health and Safety Service at the earliest opportunity.
- Where the incident requires investigation and response from another service in Auckland DHB - the line manager receiving the incident form is responsible for:
  - forwarding to the other service(s) a copy of the incident form for their investigation and follow-up
  - forwarding to Quality and Patient Safety or Health and Safety as appropriate, documentation received should outline the other service's follow-up.

Where the other service does not respond to the line manager's request for follow-up, the line manager may elevate this request to their own manager to pursue.

Where the incident involves an external facility eg rest home and is felt to be sufficiently serious with a need to follow up, it is the line manager's responsibility to contact the facility to notify them of the issue. A copy should be sent to Planning and Funding for their information.

All incidents with a rating of SAC 1 or 2 must be notified as soon as possible (within 24 hours) to the ward/team manager and Quality Department. See Incident Management Process in appendices for the required process for SAC 1 and 2 incidents.

[1]**Note: Clinical Incidents** where serious harm has occurred must be reported to the Quality Department and **Non Clinical Incidents** must be reported to Health and Safety immediately during normal business hours and to the Clinical Nurse Manager/hospital coordinator after hours.

[2]**Note:** In case of any issue to access the Incident Management System to report an incident for more than 24 hours, a printed Incident Form (see appendices) can be filled and sent to the Quality Department during normal business hours and to the Clinical Nurse Manager/hospital coordinator after hours.

The charge nurse/midwife or the senior staff member on duty must be advised of any event involving a patient in their care which occurs outside of the patient's ward/unit.

Notification to other internal services, such as the following, may be required:

- Auckland DHB Communications
- He Kamaka Oranga (Māori Health)
- Cultural services (eg Pacific Health)
- Medicines Governance Committee
- Research Principal

Back to Contents

- Infection Prevention and Control/Microbiology
- Occupational Health and Safety
- Human Resources
- Legal Counsel
- Materials Management (for all device related incidents)

Step 5. Prioritisation of incidents

The notifier must make an initial assessment of the severity of the incident - as major, intermediate or minor - when the report is submitted to the line manager for confirmation. The line manager of the notifier is responsible for confirming the severity of the consequence, determining the likelihood and SAC rating.

The SAC contains four levels of severity. The definitions for consequence in the matrix must be used to ensure consistency in the rating of risk across Auckland DHB. The rating is determined by assessing the actual outcome or consequence of the incident that has been notified as far as it can be known at the time of notification (See Prioritising Matrix: Severity Assessment Code in appendices).

Each incident will be assigned a SAC score by the manager of the area concerned within three (3) working days of the incident having been reported, particularly if the SAC rating is 1.

If an incident is complex and the manager is unclear what SAC should be assigned or the type of investigation, they must escalate the case as follows:

- To the Quality Department representative (Clinical Effectiveness Advisor, Clinical Quality Facilitator) allocated to the directorate. They should advise about the SAC rating.
- If there is still a discrepancy or no clear SAC rating, the Quality Department representative should present the case in the next SAC 1-2 group meeting, asking for advice.
- If there is still a discrepancy, a clinical representative from the Directorate/Service should present the arguments at the SAC 1-2 group meeting and a final decision must be made.

Cases requiring escalation must be documented in a brief summary of the discussions and decisions. The final SAC rating must assigned within 15 working days of the incident having been reported.

Some events require mandatory external notification regardless of their risk rating. These incidents must be managed in accordance with the requirements of the policy, and must be escalated to the Quality Department and/or to OH&S if the incident is notifiable within one (1) working day to ensure appropriate external notification. Incidents requiring mandatory external notification are specified on the Severity Assessment Code and are listed in Prioritising Matrix. Severity Assessment Code (see appendices).

Step 6. Review (incidents involving patients)

It is the Director of the directorate responsibility to ensure that an appropriate review process commences as soon as possible and that preventative actions are implemented and noted on the Incident Management System. Clinical Effectiveness Advisors or Quality Facilitators are available as a resource to assist and provide advice.

When an event may involve more than one area, the Director of the area in which the event occurs must liaise with other senior staff members to ensure an appropriate review process occurs, for example when an incident involves both an operating room and a ward, or a ward area and medical staff members.

Back to Contents

Review Tools

There are several tools available to investigate incidents. The choice of tool will depend on the severity or outcome of the incident that is being investigated.

SAC 1 events

All events that are coded as SAC 1 will be investigated using a Root Cause Analysis (RCA), London Protocol (mental Health cases) or equivalent systematic method of review. This will be completed within 70 working days of the incident being notified, including submission to the Adverse Events Review Committee (AERC) for approval of methods, findings and recommendations. A summary report from the RCA will be forwarded to the Health Quality and Safety Commission (HQSE) i.e. Reportable Events Brief (REB) Part B (see other resources).

SAC 2 events

SAC 2 incidents must have a detailed investigation. This could take the form of a systematic review (such as RCA, Failure Mode Effect Analysis FMEA, London Protocol); however other appropriate and effective investigation methods may be used, such as a case review. It is possible to aggregate similar events and review together. The investigation must be completed within 70 working days. A copy of the report is to be sent to the Adverse Events Review Committee for approval of methods, findings and recommendations. A summary report will be forwarded to the Health Quality and Safety Commission (HQSE) i.e. Reportable Events Brief (REB) Part B (see other resources).

RCA is a mechanism to find effective solutions to identified problems, and will assist in developing an open and fair culture where the emphasis is on learning and not apportioning blame. Once root cause(s) have been established corrective action(s) must be agreed upon with a completion date and the persons responsible for the implementation of the corrective action(s).

The London Protocol differs from the Root Cause Analysis model with its emphasis on gaps and inadequacies within the system and its analysis of the chain of events and contributory factors leading to the adverse event rather than a focus on a single/small number of root cause(s). See The Principles of Root Cause Analysis (RCA) Investigation and London Protocol in appendices for more information on RCA and London protocol investigations.

Setting up a review team (SAC 1 and 2)

Review investigations must be facilitated by the lead directorate who will be responsible for its timely completion. A review leader must be provided with relevant training and/or support. Members of the Quality Department can advise on process and methods. Team members must be selected by the directorate for their expertise in the subject matter relating to the event. Directorates should consider including staff members outside the immediate clinical area, where appropriate, such as other clinical services, cultural advisors, facilities management, pharmacy, allied health and materials management. Staff members directly involved in the event (or their manager) must **not** be included in the review team. Directorate leaders must ensure team members are released from their usual work to undertake the review. The Quality Department will regularly report to the lead Director about the progress towards completion of reviews.

Final reports (SAC 1 and 2)

The final report must be agreed upon in conjunction with the key leaders in the service including the service directorates, service manager and clinical director/professional leader, prior to submission to the Adverse Events Review Committee.

The report and any associated documents such as interview notes, meeting notes, and timelines are to be stored electronically by the Quality Department.

Reports must not identify patients or staff members.

Any disagreement between the review team and key leaders in the service that cannot be resolved through the review process must be discussed at the Adverse Event Review Committee and final recommendations must be made.

SAC 3 and 4

A review of these incidents must be undertaken at the ward or service level and responsibility for their management must be assigned.

Review of these incidents must identify:

- System issues that need to be addressed
- Appropriate quality improvement action to prevent recurrence where possible

Potentially relevant tools include: barrier analysis, cause and effect diagrams, five whys, flow diagrams and change analysis.

It will not be possible to formally investigate all SAC 3 and SAC 4 events. It may be more efficient and just as appropriate to investigate multiple incidents as common incident types and to develop a common action plan.

The review, or decision to aggregate events, should be completed within 30 working days and documented in the '*outcome details*' section on the electronic reporting database.

Staff support

Ensure staff safety and support. Approaches might include defusing, debriefing and involving professional bodies as outlined in the Critical Incident Stress Management policy (see associated Auckland DHB documents).

The Employee Assistance Programme (EAP) is available to staff members for support and debriefing. See the Occupational Health & Safety intranet site.

Māori staff members may be offered whānau support throughout the process.

Protected quality assurance activity (PQAA)

Although the initial notification of an event has no special protection, some subsequent review processes (eg departmental clinical audit) may be undertaken as PQAA but protection is limited to new information regarding the clinical care provided by individual health practitioners.

Auckland DHB's primary investigation into an adverse incident, such as an RCA, will not be carried out as a PQAA.

Staff members must be well informed about the use of information provided for any review they are asked to be involved in. Staff members may be requested to write additional factual

Back to Contents

information as part of the review process. Notes may be taken as review teams gather more information about an event, however audio-visual recording of discussions should not occur.

A staff member may seek advice from Auckland DHB Legal Counsel or their professional body. See Protected Quality Assurance Activities policy in associated Auckland DHB documents for more information.

Medico-legal involvement

Where an event has resulted in a review by the Coroner, the RCA or equivalent review may be submitted to the Coroner before the inquest. Consult with Auckland DHB Legal Counsel.

For any event that may have medico-legal implications, (i.e. there is a significant adverse outcome for the patient/client and criticism of clinicians is likely) documentation other than a factual account in the clinical record and the standard notifications should be made only with legal/professional advice.

Medical defence organisations and/or professional indemnity insurers require notification of potential claims. This is the responsibility of the individual professional involved.

Advice can also be sought from Auckland DHB Legal Counsel. Legal advice must not delay submission of the event via Incident Management System.

Performance Issues

Although the review process seeks for to identify systems and process gaps, it may in the process find potential performance issues. In this case, the team review could discuss any concerns with the Clinical Effectiveness Advisor allocated to the case and then with the Quality Manager who will be manage this with the directorate lead. The final report must not refer/describe any performance issue

Step 7. Coding

This is a process of capturing relevant information about the incident to ensure that the complete nature of the incident is documented and understood. The electronic Safety Management System provides a coding system for incident categories i.e. location of the incident, responsible manager, causal and contributing factors, actions to develop and lessons to be learnt from the incident.

This information is recorded using different sources of classification that is normally validated.

Converting relevant information in to categories or codes allows for easy analysis and facilitates reports and dashboards.

Step 8. Analysis

The Incident Management System provides the ability to summarise events occurring within a service, directorate or within Auckland DHB.

The following types of analysis should be considered:

- Summary of the frequency of incidents - allows prioritisation for the allocation of resources
- Descriptive summaries
- Trend analysis can identify changes that suggest new problems (or, if improving, that safety measures are working). A cluster of events that suddenly arises suggests a need for inquiry and immediate action

- Identify correlations eg causal factors such as communication, workloads, teamwork, equipment, environment and staffing

Monthly service level reports are to be discussed at service/quality meetings and other relevant forums to discuss trends and identify where further action is required.

Step 9. Action

Implementation of recommendations from the reviews are required to develop better systems to ensure improved practice. The Adverse Events Review Committee will review the reports from SAC 1 and SAC 2 investigations and decide whether they should be accepted in conjunction with the directorate. The directorate will consider the allocation of appropriate resources to implement the agreed recommendations. The acceptance of the recommendations is recorded in the minutes of the Adverse Events Review Committee.

Recommendations from SAC 1 and SAC 2 reviews must include timeframes for completion and must have an assigned person(s) responsible for the implementation of recommendations. The recommendations are added to the Auckland DHB-wide corrective action database for tracking of implementation. An audit of recommendations must occur 90 days after the completion of the RCA or formal review. A report showing progress will be submitted by the Quality Department to the relevant Directorate(s) and the Auckland DHB Clinical Board quarterly.

The Adverse Events Review Committee is a sub-committee of the Auckland DHB Clinical Board. It provides organisational governance of all Auckland DHB SAC 1 and 2 events to ensure:

- Appropriate investigation options are implemented
- Process is clear and transparent
- Reporting is accurate and timely
- Implementation of recommended actions from all SAC 1 & 2 occurs
- External reviews are appropriately commissioned and executed
- Organisational learning is facilitated

Step 10. Feedback and Learning

To staff members

Feedback must be provided to relevant staff members on the results/outcomes of investigations for all events. This must occur in a timely manner. For a SAC 1 event the feedback must be undertaken by senior staff and be based on the final RCA report. The RCA report must be provided to the relevant clinical team and presented at relevant staff meetings.

Directorates should provide ward staff members/clinical and management teams regular reports on aggregated data and outcomes of reviews. Feedback should include the changes made and the improvements achieved as a result of these changes.

To patient/responsible person (family/whānau member or other person)

Patients or family members must be provided with an opportunity to discuss the outcome of the investigation unless there are exceptional reasons for not doing so. The meeting should be face to face if possible and may include the provision of the report and other summary material. The patient/family should be provided with an opportunity to meet again to discuss any questions they may have as a result of the outcome meeting or reading the report.

Back to Contents

Feedback should usually be made to the individual patient and/or responsible person (family/whānau member or other person). This must occur formally for SAC 1 and SAC 2 events. When discussion with the consumer is not possible or appropriate - such as when they have died or been significantly compromised - his or her next of kin, designated contact person, or representative must be informed.

Cultural support and processes and/or emotional support must be considered when arranging the feedback meeting for patients or families. Details about the incident and any harm experienced and any other subsequent clinical actions must be fully documented in the patient's clinical record.

If not previously, notified consumers must be advised at this point that they may be entitled to compensation through the ACC Treatment Injury claims process. Appropriate medical forms (ACC45 & ACC2152 - see Forms) must be initiated.

Directorate leaders must be involved in decisions on who provides feedback to patients and their families and on when and what information is to be provided. Details of staff members involved in the event must **not** be included in any feedback. The Consumer Liaison Department may be asked to facilitate feedback to the patient or family.

5. Incident Management Timelines

	Milestone	Working days	Accumulate working days	Directorate accountability	Quality Department accountability	Team review accountability
1.	**Incident identification**			Mitigate/control risks, communicate with the patient, family and other stake holders		
2.	**Incident reporting**	0	0	To report the incident in the Incident management system	Provide access to the safety management system	
3.	**Incident SAC rating**	5	5	Determine the SAC score, for complex cases seek advice from the Quality Department	In cases where the directorate seeks clarification/advice on the SAC rating, the case would be presented at the next SAC1-2 meeting. This will be presented by the CEA allocated for that directorate. All CEAs by directorate oversee incident forms for their directorates. If a CEA finds that a serious or major event is not classified correctly, it can be presented at SAC 1-2 - the directorate is then informed of any changes	

4.	**REB A sign off**	3	8	Director to sign off the REB A form and send it to the CEA	Once the SAC score is confirmed as 1-2, the CEA prepares the REB Part A form and sends it to the directorate for sign off	
5.	**Team confirmation**	5	13	Director to confirm the names of the clinical team involved in the review	CEA will request names from the directorate for the review team	
6.	**First meeting**	10	23		Prepare the timeline for the case. Send invitation of participation to the review team members. Book meeting room laptop and projector. Prepare the slides for the first meeting. Make contact with the team members to allow an opportunity to respond to questions before the meeting. CEA to send the RMPro incident form, timeline, terms of reference and agenda to the review team before the meeting	Participation/ engagement in the meeting. Contribution of material relevant to the case. Discussion and correction of the timeline. The aim of meeting one is to complete the simple flow diagram, agree on the actions (eg interviews, data analysis, etc.) and agree on dates for the next meeting
	Time between 1st and 2nd meeting				Collect information sent by the team members. Configure templates for the detailed flow diagram and causation flow diagram. Book meeting room, laptop and projector. Prepare slides for the second meeting and ensure contact is made with members of the team in order to help and support with the interviews.	Interview staff as agreed. Research relevant issues and other relevant analyses. Locate policies/ procedures
7.	**Second meeting**	15	38		Facilitate in the development of the detailed flow diagram and on the causation flow diagram. Allocate sections of the report (findings) to each team member	Participation/ engagement in the meeting. Contributes with material relevant for the case eg interviews notes, policies, data, processes etc. Develop and contribute to the detailed flow diagram and to the causation flow diagram

	Time between 2nd and 3rd meeting				Start report writing for sections: details of the incident, brief description of the case, insert the detailed flow diagram, insert the causation diagram if completed. Book meeting room , laptop and projector, prepare slides for the third meeting	Contribute to the report by completing the allocated report findings
8.	**Third meeting**	5	43		Develop and complete the causation diagram. Develop recommendations and discuss residual risk	Participation in the meeting. Complete the causation flow diagram, contribute to the discussion on recommendations
	Draft 1	5	48		Collect all the information from the review team and put together all a first draft of the report. Send the draft to the team for their first review	Review the draft and contribute while ensuring all changes are tracked
	Final draft approved	15	63			Approve the final draft
	Send draft report to the staff involved and to the services involved				Send the approved draft to the staff involved for errors of fact and then to the service clinical directors for comments	Comment on feedback received from the draft report
	Send to the directorate for Pre - approval	5	68	Pre-approve the case/send comments or feedback to the review team.	Send to the director (others involve in the assessment at the directorate level) for analysis and pre-approval	To revise and review the report if requested by the director/ directorate level. In cases where the team do not agree with the comments (or some of them) the case shall be presented and discussed (points of disagreement in the AERC)
	Ready to include in the next AERC agenda pack	2	70	To be present during the presentation, and be accountable for the implementation of the actions	Include the case in the next AERC agenda pack	To present the case at the AERC meeting and to respond to any questions received from the committee

6. Supporting evidence

[1] Vincoli, J. W. (2014). *Basic guide to system safety* (3rd Ed.). John Wiley & Sons.

[2] Backlund, A. (2000). The definition of system. *Kybernetes, 29*(4), 444-451.

[3] Miller, J. G. (1995). *Living systems*. University Press of Colorado.

[4] Marx, D. A. (2001). *Patient safety and the" just culture": a primer for health care executives*. Columbia University, New York.

[5] McKinnon, R. C. (2012). *Safety Management: Near Miss Identification, Recognition, and Investigation*. CRC Press.

[6] Meadows, S., Baker, K., Butler, J. & Agency FOR Healthcare Research Quality Rockville MD. (2005). *The Incident Decision Tree: Guidelines for Action Following Patient Safety Incidents*.

7. Legislation

- Health and Disability Commissioner (Code of Health and Disability Services Consumers' Rights) Regulations 1996
- Health Practitioner Competence Assurance Act (2003)
- Health and Safety Employment Act 1992
- Health and Safety at Work Act (2015)

8. Associated Auckland DHB documents

- ACC Treatment Injury
- Adverse Event Review Committee
- Child Abuse Neglect, Care & Protection
- Critical Incident Stress Management
- Deceased (Tupapaku) +/- Referrals to the Coroner for an Adult, Child, Infant, Neonate or Stillbirth
- Documents & Records Retention
- Health and Safety
- Health Practitioner's & Registered Social Worker Competence & Reporting Obligations
- Open Disclosure following an Adverse Event
- Protected Disclosures
- Protected Quality Assurance Activities
- Security
- Sexual Misconduct Allegation from a Patient against an Auckland DHB Employee - AED/APU Initiated

9. Other resources

- Health and Disability Commissioner *'Your Rights'* leaflet
- Kiosk - A Quick Reference Guide for Staff
- Learn from Adverse Events (Quality Department)

Back to Contents

- New Zealand Health and Disability Services. *National Reportable Events Policy 2012*. Retrieved http://www.hqsc.govt.nz/our-programmes/reportable-events/publications-and-resources/publication/320/
- New Zealand Medicines and Medical Devices Safety Authority (Medsafe)
- Occupational Health & Safety
- Office of the Health and Disability Commissioner. *Open Disclosure*. Retrieved http://www.hdc.org.nz/decisions--case-notes/open-disclosure
- Reportable Event Brief (REB)
- Root Cause Analysis (RCA)
- Severity Assessment Code (Includes Matrix)
- Worksafe New Zealand. Retrieved http://www.worksafe.govt.nz/worksafe/

Patient information

- Your Rights when receiving a Health or Disability Service (HDC)

Forms

- Medsafe Serious Harm Form
- ACC forms ACC45
- ACC2152: Treatment Injury Claim

10. Disclaimer

No guideline can cover all the variations required for specific circumstances. It is the responsibility of the health care practitioners using this Auckland DHB guideline to adapt it for safe use within their own institution, recognise the need for specialist help, and call for it without delay, when an individual patient falls outside of the boundaries of this guideline.

This guideline will align with the Health Quality & Safety Commission (HQSC) National Reportable Events Policy therefore this guideline will be updated as and when HQSC update their National Reportable Events Policy.

11. Corrections and amendments

The next scheduled review of this document is as per the document classification table (page 1). However, if the reader notices any errors or believes that the document should be reviewed before the scheduled date, they should contact the owner or the Clinical Policy Facilitator without delay.

12. Appendices

12.1 Definitions and abbreviations

Accident	Referred to in this policy as an incident. An accident is an event that causes any person to be harmed or in different circumstances, might have caused any person to be harmed (referred to as a near miss)
Adverse event	An incident that has resulted in unanticipated death or loss of function not related to the natural course of a consumer's illness or condition
Apology	An expression of regret
Clinical leader	Clinical leader in this document refers to the role in its broadest sense: a clinician who has designated responsibility and accountability for clinical professional leadership. For example: Level 2 and 3 leadership positions for medical staff members Level 2 and 3 leadership positions for nursing staff members Level 3 Allied Health Professional Leaders Other designated roles
Consumer	A person receiving care/treatment from Auckland DHB
Contractor/Sub-contractor	Person engaged by Auckland DHB (other than a Auckland DHB employee) to do any work for gain or reward
Contributing factor	This is a circumstance, action or influence (such as availability of staff members or increased workload) which is thought to have played a part in the origin or development of an incident, or increase the risk of an incident
Handler	The person responsible for confirming the SAC rating in the case and for completing the management section of the incident report into the Incident Management System
Harm	Refers to illness, injury or both and includes physical or mental harm caused by work-related stress
Hazard	It is a potential source of harm or adverse health effect on a person or persons
Health Practitioner	A registered doctor, nurse or allied health professional
Incident	In this guideline the term "incident" is used generically to refer to incident or accident. An incident is an unplanned event that results in or has the potential to result in injury, damage or loss. This applies to clinical and non-clinical events. • **Clinical:** an event unrelated to the natural course of the illness and differs from the expected outcome of patient management • **Product Fault:** an event where a consumable product or medical device has failed in its intended purpose • **Health and Safety:** An event relating to a hazard, work injury or serious harm, involving employees, contractors, sub-contractors, students and volunteers

Back to Contents

	An incident may range from minor (eg medication error with no harm, piece of equipment goes missing, loss/unavailability of clinical record), moderate (eg additional monitoring, investigations or interventions as a result of incident, patient reacts to medication which should have been withheld) or serious (see serious adverse event/serious harm in Definitions and abbreviations)
Incident Management System	This is the Auckland DHB electronic reporting system available to staff members to report an event or incident
Incident with harm	An unplanned event that results in injury, or loss. This applies to clinical and non-clinical events
Incident with no harm	An unplanned event that reaches the patient, employee or organisation without any injury, or loss but has the potential to result in injury, or loss
Intentionally unsafe acts	Events related to patients that result from any act or omission with intention to cause harm or with reckless disregard for the safety of others. This includes assault, abuse or deliberate neglect
Just Culture	A just culture approach recognises that even competent professionals make mistakes and acknowledges that they can develop shortcuts, workarounds and routine violations - yet declares intolerance for reckless behaviour. The approach sometimes distinguishes between human error, at-risk behaviour, and reckless action - three categories which involve increasing degrees of wilfulness and disregard (Marx, 2001)
Licensed user	This is a senior staff member that is responsible for the follow-up of events in their area and has full access to the Auckland DHB electronic reporting system (Risk Monitor Pro)
London Protocol	An incident investigation model developed by the Clinical Risk Unit, University College, London, which starts by examining the chain of events that led to an accident or adverse outcome and considering the actions of those involved. It then looks further back at the conditions in which staff members were working and the organisational context in which the incident occurred.
Near miss	An unplanned event with the potential to result in injury, or loss but was timely stopped before it reached the patient, employee or organisation. Any event that could have had adverse consequences but did not and is indistinguishable from an actual incident in all but outcome. A near miss may occur when a sequence is interrupted hence no actual incident eventuates. The difference between the accident and the near miss incident is purely a matter of chance as the outcome of a near miss incident cannot be determined and is very difficult to predict (McKinnon, 2012, p.98)
Notification	Completion of the Auckland DHB Incident Form following identification of an incident and sending it to the Quality and Patient Safety, Product Coordinator or Health and Safety Service as appropriate.
Notifiable event	Any events that arise from work that results in the death of a person, a notifiable injury/illness or a notifiable incident
Open disclosure	Timely and transparent approach to communicating, engaging with, and supporting consumers and their families (whānau) when things go wrong - refer to the Open Disclosure following an Adverse Event Policy in

Back to Contents

	associated Auckland DHB documents An apology is made and, if an investigation is to take place, those concerned are advised. An open disclosure approach also includes support for staff members and the development of a culture where staff members are confident that the associated investigations will have a quality improvement rather than a punitive focus
Reportable event	Any event that must be reported to the Health Quality & Safety Commission (HQSC) for (national) aggregation, analysis, and action. This includes SAC 1 and SAC 2 events. All reportable events require a Reportable Event Brief (REB) to be completed.
Reported severity	The first assessment of the severity of a reported event, done by the staff member completing web based form (Risk Monitor Pro).
Review methods	**Root Cause Analysis (RCA)** A systematic, no blame process whereby factors that led to an incident are identified in order to establish the contributing factors/ hazards/ causes. **London Protocol** This outlines a process of incident investigation and analysis. It is designed to be a structured process of reflection on incidents, providing insight to the health care system and can be adapted for use in many contexts, and used either quickly for education and training or in substantial investigations of serious incidents
Risk	The possibility (likelihood) of suffering harm or loss (consequence) from a hazard
Risk Monitor Pro (RMPro)	This is the Auckland DHB electronic reporting system available to staff members to report an event or incident
Root cause analysis (RCA)	Root Cause Analysis is defined as a systematic iterative process whereby the factors which contribute to an incident are identified by reconstructing the sequence of events and repeatedly asking *'why?'* until the underlying root causes (contributing factor/hazards) have been elucidated
Serious harm	An event related to staff, visitor or contractor that amounts to or results in permanent loss of bodily function, or temporary severe loss of bodily function or as outlined in the HSE Act 1992: 1. respiratory disease, noise-induced hearing loss, neurological disease, cancer, dermatological disease, communicable disease, illness caused by exposure to infected materials, decompression sickness, poisoning, vision impairment, chemical or hot-metal burn of eye, penetrating wound of eye, bone fractures, laceration, crushing 2. Amputation of body part 3. Burns requiring referral to a specialist registered medical practitioner or specialist outpatient clinic 4. Loss of consciousness from lack of oxygen 5. Loss of consciousness, or acute illness requiring treatment by a

Back to Contents

	registered medical practitioner, from absorption, inhalation, or ingestion of any substance 6. Any harm that causes the person harmed to be hospitalised for a period of 48 hours or more commencing within seven days of harm occurrence
Serious Adverse Event Review Committee	Auckland DHB has a Serious Adverse Event Committee. This panel review and approve recommendations from RCAs and provide a report to the Clinical Board and/or other relevant committees
Serious adverse event & Sentinel event	An event has resulted in, or has the potential to result in, serious lasting disability or death, not related to the natural course of the consumer's illness or underlying condition
Serious Incident Review	A process followed by Mental Health to review serious incidents involving mental health and addiction service consumers
Severity Assessment Code (SAC)	A numerical rating allocated to an event based on the type of event, the actual outcome or consequence of the event and the likelihood or recurrence of a similar event
Serious harm to employees	See Occupational Health & Safety Intranet site
System	A system is a set of interacting units with relationships among them (Miller, 1995, p. 17; Backlund, 2000)
System failure	A fault, breakdown or dysfunction within the system
System safety	It is an specific, driving purpose to eliminate system faults or failure risk and subsequent recognised accident/incident and/or hazard potential through design and implementation of controls (Vincoli, 2014, p.9)
Staff/employee	Refers to all staff covered under the Health and Safety Employment Act 1992. This includes all employees, loaned employees, students and contractors working in Auckland DHB
Worker	Any person who carries out work in any capacity for CM Health (fulltime, part-time, casual and temporary), including associated personnel (contractors, students, visiting health professional etc.) working in, or contracted to provide a service on any Auckland DHB site
Workplace	Any place where work is carried out for or on behalf of Auckland DHB whilst a person is deemed at work

Back to Contents

12.2 Mandatory External Reporting Responsibilities

External Reporting to Auckland DHB

- **Health Quality and Safety Commission HQSC:**

  SAC 1 & 2 events are required to be reported to the HQSC within 15 working days of being reported or within five working days of the SAC score being confirmed. Any matter that requires direct notification to a national agency under existing legislative reporting requirements or policy directive, regardless of its SAC rating, is to continue being reported to that agency.

  Following the identification of a SAC 1 or a SAC2 event the Quality Department representative completes a Reportable Event Brief (REB) (see other resource) in conjunction with the Directorate leader(s). The Quality Department forwards the REB to the Health Quality and Safety Commission.

- **Department of Labour and WorkSafe**

  Serious harm to employees:
  Service or clinical manager notifies OH&S and Dept of Labour, verbally as soon as possible, and completes a serious harm form and submits to OH&S (see Occupational Health and Safety intranet site).

  Serious harm to patients (not related to treatment eg fall):
  Clinical manager or Quality Department representative (as agreed with service) highlight the case to Quality Department and Auckland DHB OH&S. OH&S must review the case and will discuss the case with the Chief Professional Officer and Legal Advisor before completing the online Worksafe New Zealand serious harm form.

- **Perceived breach of professional standards:**

  Director of the Directorate must report to professional body as outlined in Health Practitioners Competency Assurance Act 2003 (see Legislation)

- **Director of Mental Health, Ministry of Health:**

  All Mental Health SAC 1 & 2 events are sent to - the Director Mental Health Services Auckland DHB

- **Centre for Adverse Reactions Monitoring (CARM or Medsafe)**

  Medicine related SAC 1 & 2 events are sent to by the pharmacy manager

- **Ministry of Health – Medsafe**

  Medical Device SAC 1 & 2 events related to a medical device eg material, instrument, machine, appliance, implant are reported to the Materials Management who notify the Ministry of Health - Medsafe (see other resources)

- **National Radiation Laboratory**

  Radioactive Materials SAC 1 & 2 events related to incorrect administration of radioactive materials/radiation therapy are reported by the Principal Licensee Radiology/Radiation Oncology Manager

Back to Contents

- **Coroner Office**

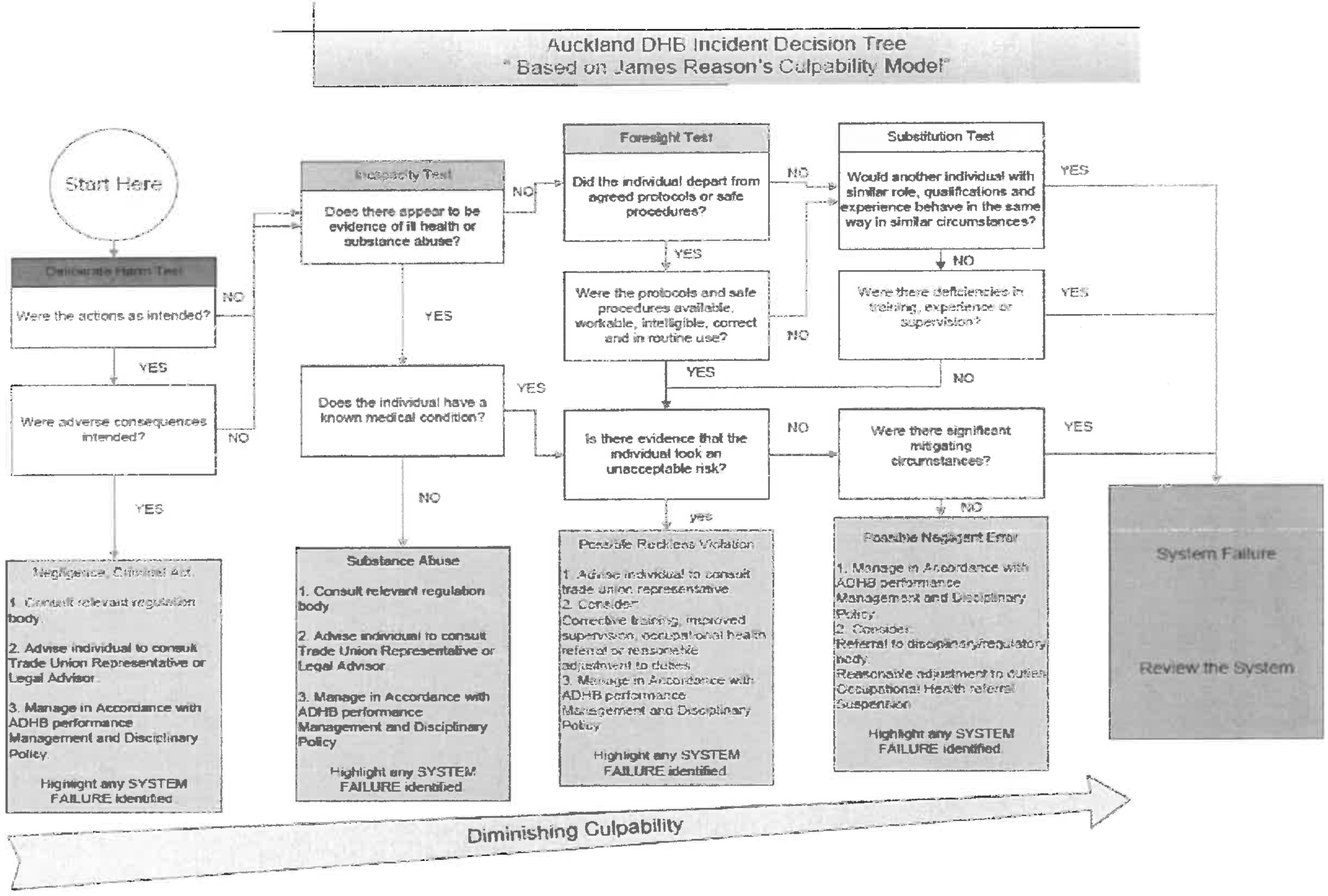
If a patient has died as a result of the adverse event, the case must be discussed by a senior doctor with the on call coroner

- **Insurance Brokers**

Auckland DHB Legal Counsel must report all potential/actual claims to the Insurance Brokers. Individual health professionals are responsible for reporting issues/incidents to their professional indemnity insurers or professional defence organisations.

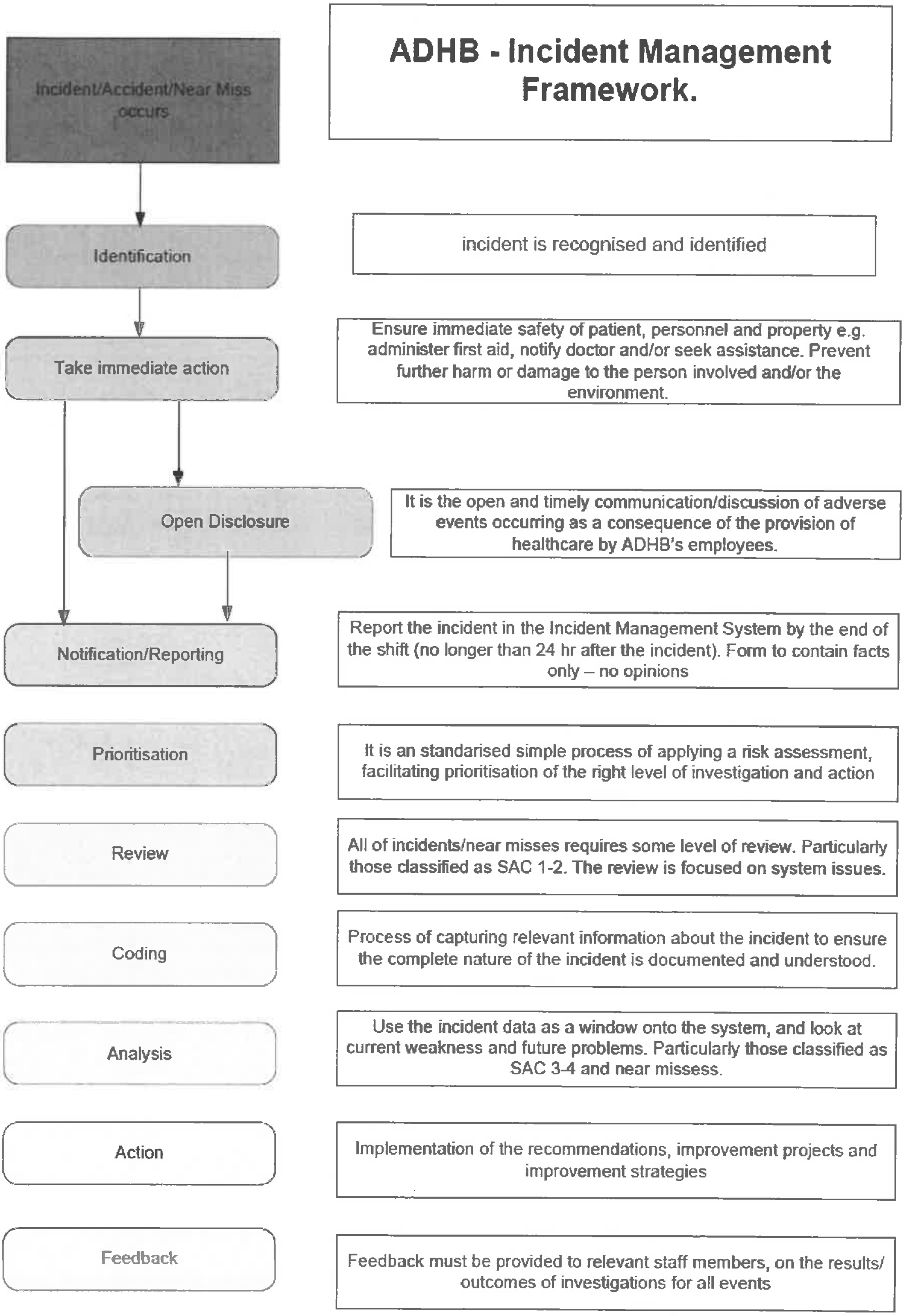
Back to Contents

12.3 Incident Decision Tree


Auckland DHB Incident Decision Tree
" Based on James Reason's Culpability Model"
Start Here
Deliberate Harm Test
Were the actions as intended?
NO
YES
Were adverse consequences intended?
NO
YES
Negligence, Criminal Act.
1. Consult relevant regulation body.
2. Advise individual to consult Trade Union Representative or Legal Advisor.
3. Manage in Accordance with ADHB performance Management and Disciplinary Policy.
Highlight any SYSTEM FAILURE identified
Incapacity Test
Does there appear to be evidence of ill health or substance abuse?
NO
YES
Does the individual have a known medical condition?
YES
NO
Substance Abuse
1. Consult relevant regulation body
2. Advise individual to consult Trade Union Representative or Legal Advisor
3. Manage in Accordance with ADHB performance Management and Disciplinary Policy
Highlight any SYSTEM FAILURE identified
Foresight Test
Did the individual depart from agreed protocols or safe procedures?
NO
YES
Were the protocols and safe procedures available, workable, intelligible, correct and in routine use?
NO
YES
Is there evidence that the individual took an unacceptable risk?
NO
yes
Possible Reckless Violation
1. Advise individual to consult trade union representative.
2. Consider:
Corrective training, improved supervision, occupational health referral or reasonable adjustment to duties
3. Manage in Accordance with ADHB performance Management and Disciplinary Policy
Highlight any SYSTEM FAILURE identified
Substitution Test
Would another individual with similar role, qualifications and experience behave in the same way in similar circumstances?
YES
NO
Were there deficiencies in training, experience or supervision?
YES
NO
Were there significant mitigating circumstances?
YES
NO
Possible Negligent Error
1. Manage in Accordance with ADHB performance Management and Disciplinary Policy
2. Consider:
Referral to disciplinary/regulatory body.
Reasonable adjustment to duties
Occupational Health referral
Suspension
Highlight any SYSTEM FAILURE identified
System Failure
Review the System
Diminishing Culpability

Back to Contents

12.4 Incident Management Framework



ADHB - Incident Management Framework.

Incident/Accident/Near Miss occurs

Identification

incident is recognised and identified

Take immediate action

Ensure immediate safety of patient, personnel and property e.g. administer first aid, notify doctor and/or seek assistance. Prevent further harm or damage to the person involved and/or the environment.

Open Disclosure

It is the open and timely communication/discussion of adverse events occurring as a consequence of the provision of healthcare by ADHB's employees.

Notification/Reporting

Report the incident in the Incident Management System by the end of the shift (no longer than 24 hr after the incident). Form to contain facts only – no opinions

Prioritisation

It is an standarised simple process of applying a risk assessment, facilitating prioritisation of the right level of investigation and action

Review

All of incidents/near misses requires some level of review. Particularly those classified as SAC 1-2. The review is focused on system issues.

Coding

Process of capturing relevant information about the incident to ensure the complete nature of the incident is documented and understood.

Analysis

Use the incident data as a window onto the system, and look at current weakness and future problems. Particularly those classified as SAC 3-4 and near missess.

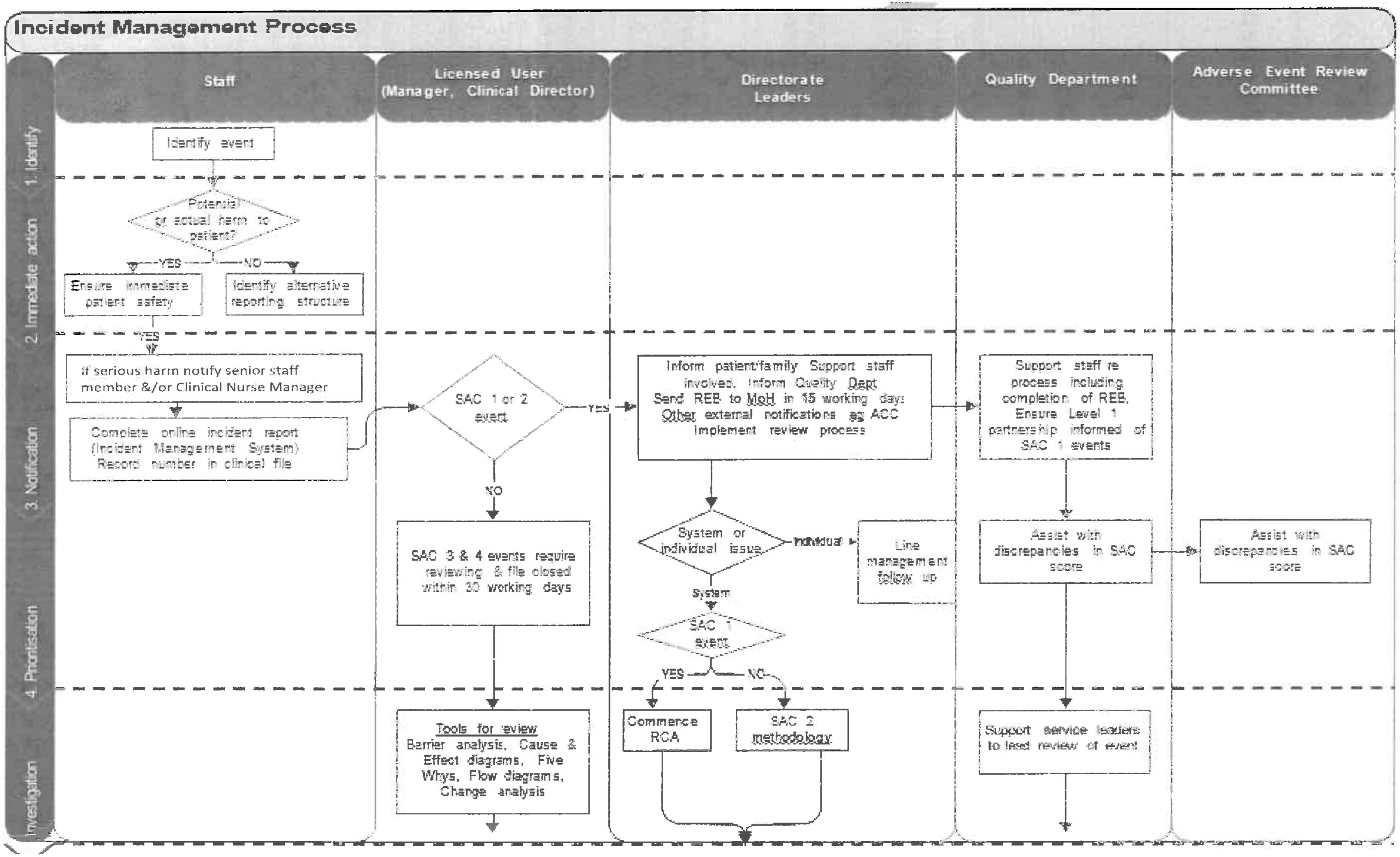
Action

Implementation of the recommendations, improvement projects and improvement strategies

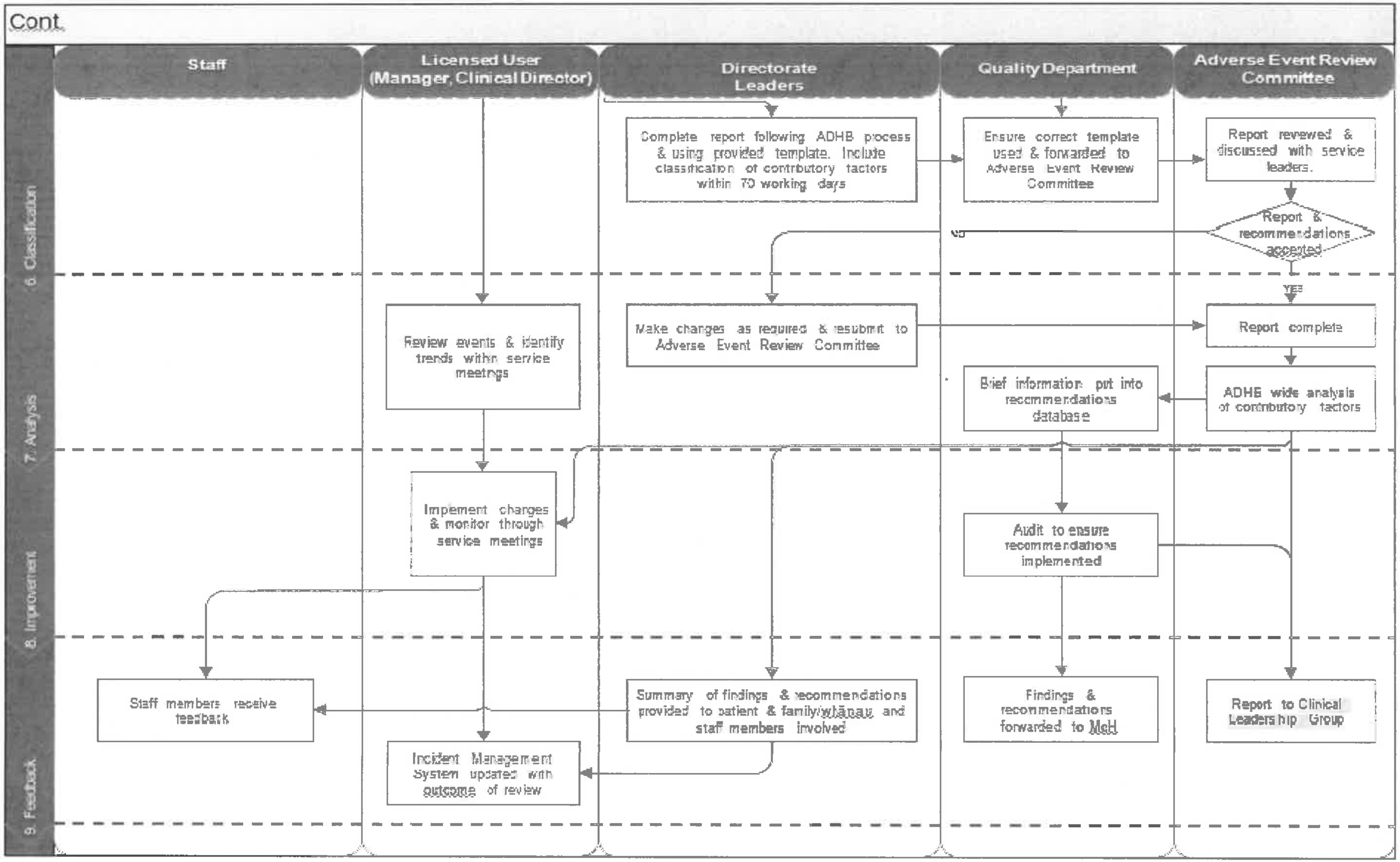
Feedback

Feedback must be provided to relevant staff members, on the results/ outcomes of investigations for all events

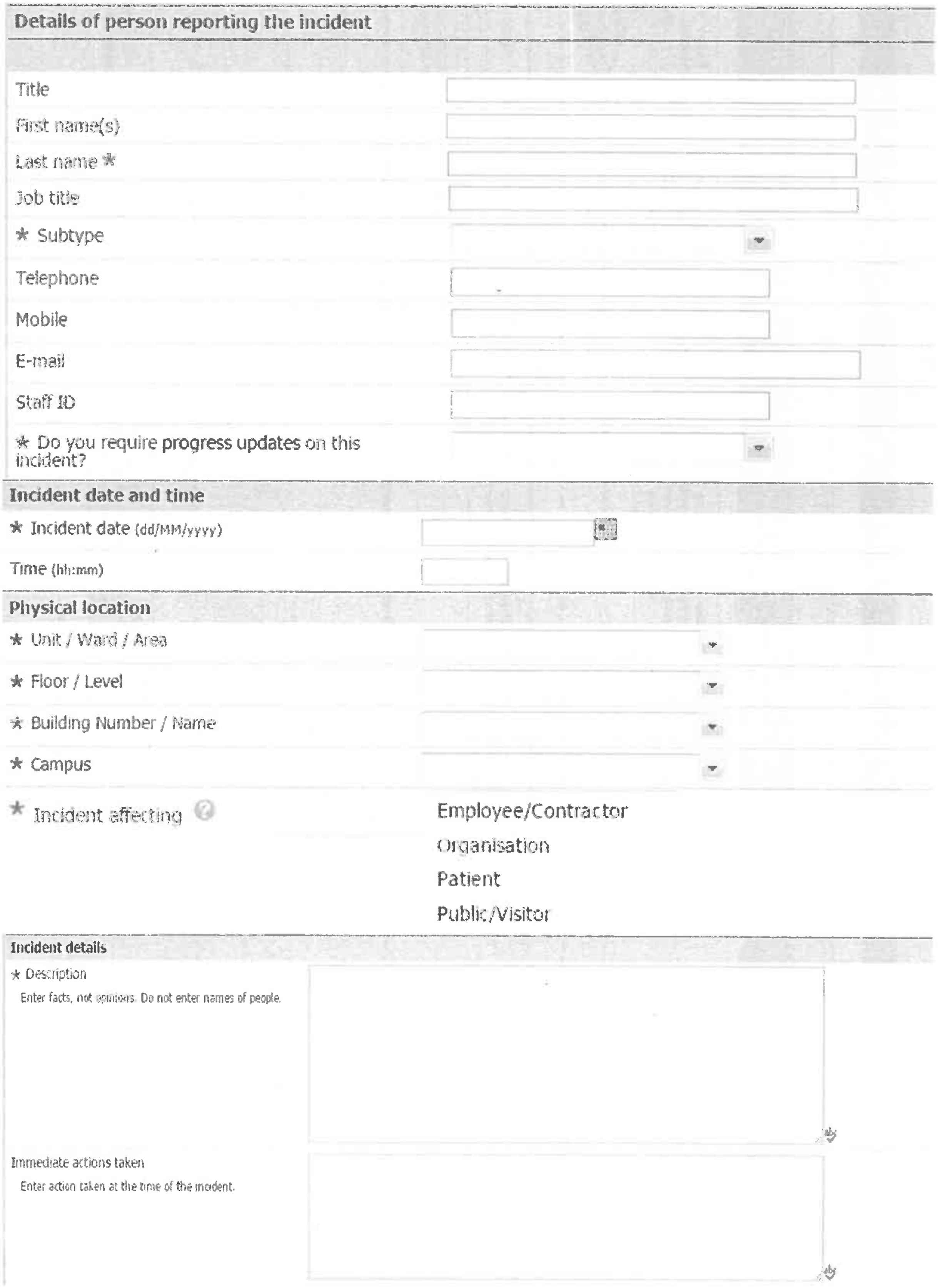
12.5 Incident Management Process


Incident Management Process
Staff
Licensed User (Manager, Clinical Director)
Directorate Leaders
Quality Department
Adverse Event Review Committee
1. Identify
2. Immediate action
3. Notification
4. Prioritisation
Investigation
Identify event
Potential or actual harm to patient?
YES
NO
Ensure immediate patient safety
Identify alternative reporting structure
YES
If serious harm notify senior staff member &/or Clinical Nurse Manager
Complete online incident report (Incident Management System) Record number in clinical file
SAC 1 or 2 event
YES
NO
SAC 3 & 4 events require reviewing & file closed within 30 working days
Tools for review
Barrier analysis, Cause & Effect diagrams, Five Whys, Flow diagrams, Change analysis
Inform patient/family Support staff involved. Inform Quality Dept Send REB to MoH in 15 working day: Other external notifications eg ACC Implement review process
System or individual issue
Individual
Line management follow up
System
SAC 1 event
YES
NO
Commence RCA
SAC 2 methodology
Support staff re process including completion of REB. Ensure Level 1 partnership informed of SAC 1 events
Assist with discrepancies in SAC score
Support service leaders to lead review of event
Assist with discrepancies in SAC score

Back to Contents


Cont.
Staff
Licensed User (Manager, Clinical Director)
Directorate Leaders
Quality Department
Adverse Event Review Committee
6. Classification
7. Analysis
8. Improvement
9. Feedback
Complete report following ADHB process & using provided template. Include classification of contributory factors within 70 working days
Ensure correct template used & forwarded to Adverse Event Review Committee
Report reviewed & discussed with service leaders.
Report & recommendations accepted
NO
YES
Review events & identify trends within service meetings
Make changes as required & resubmit to Adverse Event Review Committee
Report complete
Brief information put into recommendations database
ADHB wide analysis of contributory factors
Implement changes & monitor through service meetings
Audit to ensure recommendations implemented
Staff members receive feedback
Summary of findings & recommendations provided to patient & family/whānau and staff members involved
Findings & recommendations forwarded to MoH
Report to Clinical Leadership Group
Incident Management System updated with outcome of review

12.6 Incident Form (Hard Copy)



Details of person reporting the incident

Title

First name(s)

Last name *

Job title

* Subtype

Telephone

Mobile

E-mail

Staff ID

* Do you require progress updates on this incident?

Incident date and time

* Incident date (dd/MM/yyyy)

Time (hh:mm)

Physical location

* Unit / Ward / Area

* Floor / Level

* Building Number / Name

* Campus

* Incident affecting

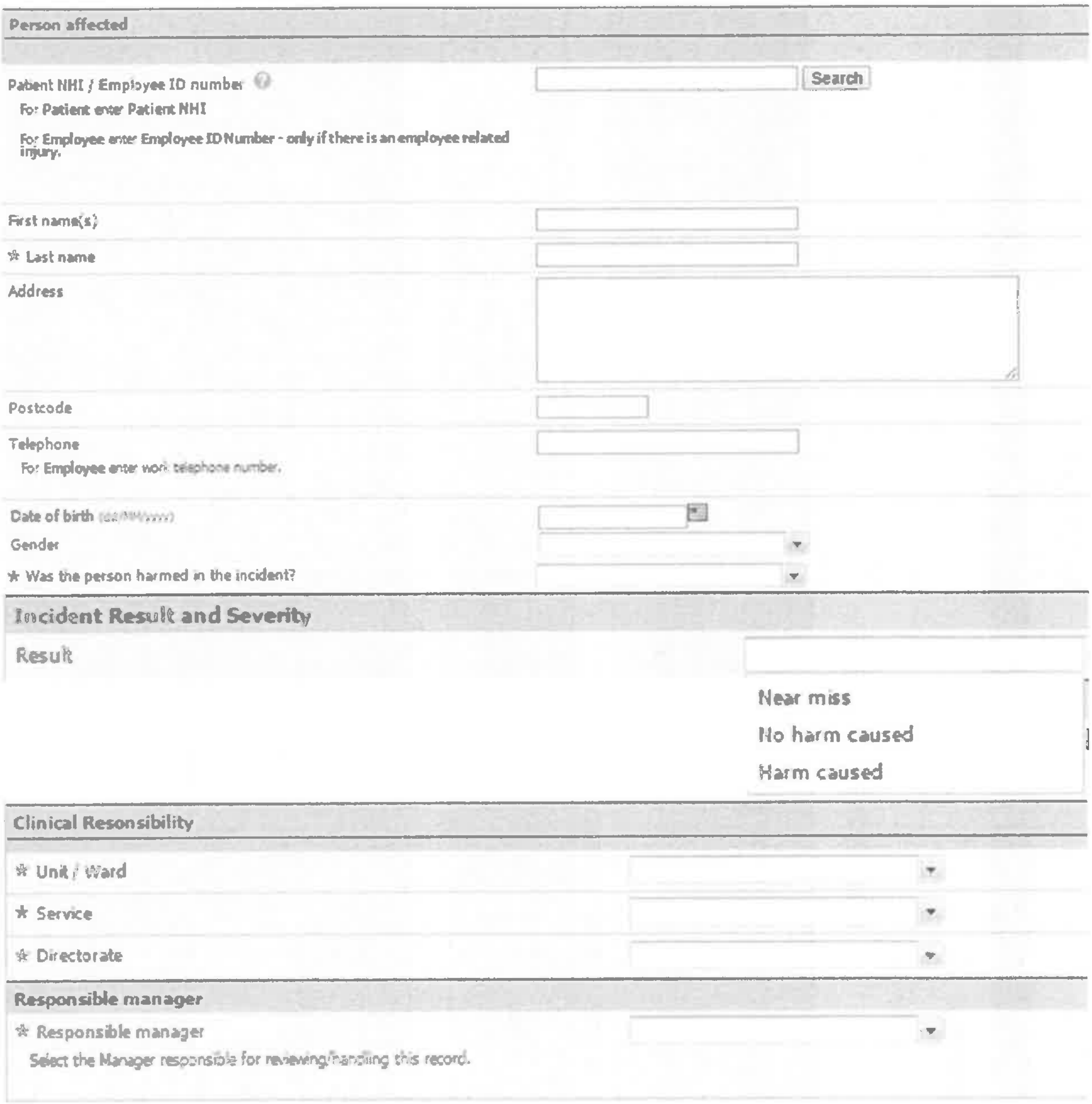
Employee/Contractor
Organisation
Patient
Public/Visitor

Incident details

* Description
Enter facts, not opinions. Do not enter names of people.

Immediate actions taken
Enter action taken at the time of the incident.

Back to Contents



Person affected

Patient NHI / Employee ID number
For Patient enter Patient NHI
For Employee enter Employee ID Number - only if there is an employee related injury.

First name(s)

☆ Last name

Address

Postcode

Telephone
For Employee enter work telephone number.

Date of birth (dd/MM/yyyy)

Gender

☆ Was the person harmed in the incident?

Incident Result and Severity

Result
- Near miss
- No harm caused
- Harm caused

Clinical Resonsibility

☆ Unit / Ward

☆ Service

☆ Directorate

Responsible manager

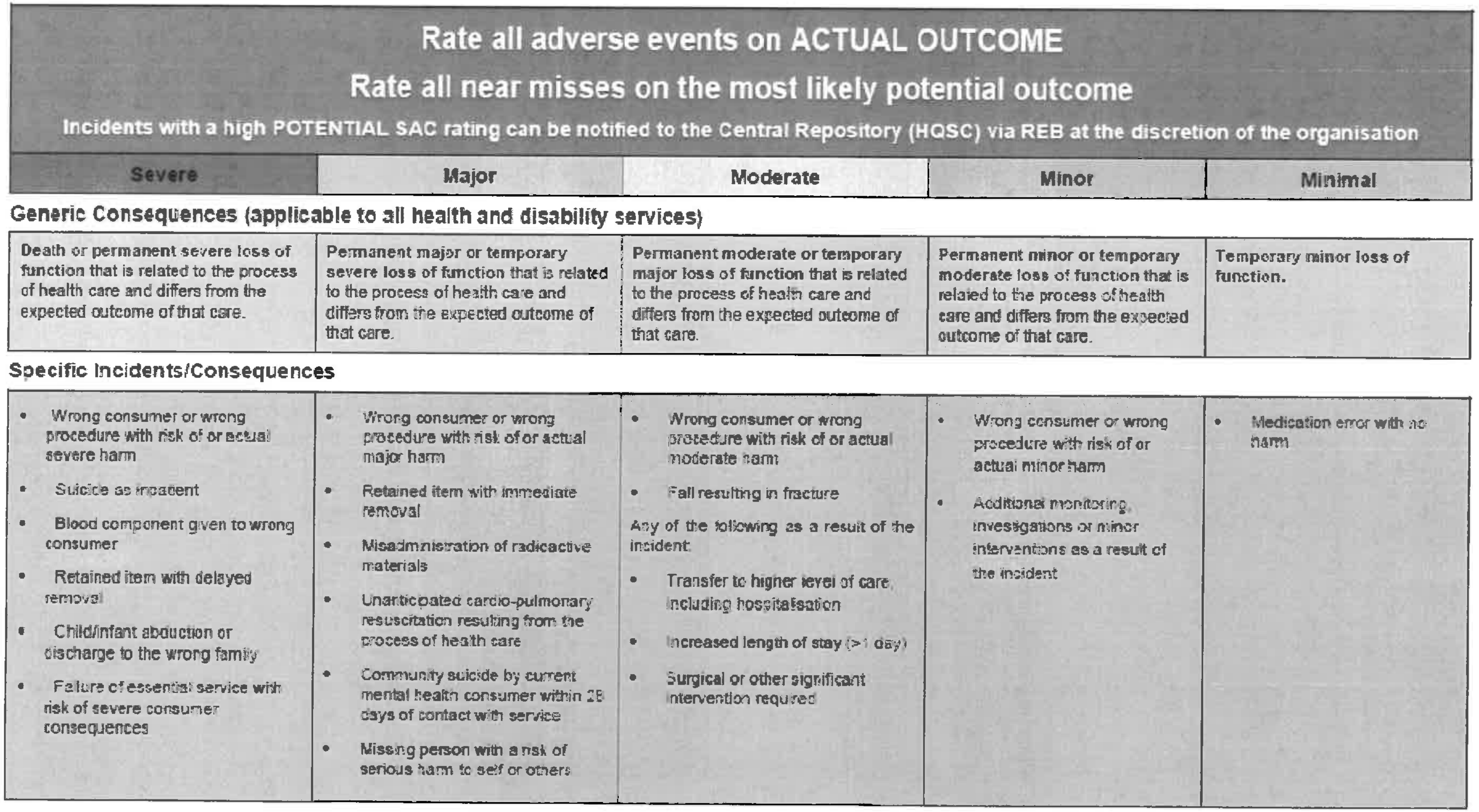
☆ Responsible manager
Select the Manager responsible for reviewing/handling this record.

Please complete and sent to the Quality Department

12.7 Prioritising Matrix: Severity Assessment Code

Step 1. Determine the consequences or outcome of the incident.

CONSEQUENCE TABLE



Rate all adverse events on ACTUAL OUTCOME

Rate all near misses on the most likely potential outcome

Incidents with a high POTENTIAL SAC rating can be notified to the Central Repository (HQSC) via REB at the discretion of the organisation

Severe	Major	Moderate	Minor	Minimal
Generic Consequences (applicable to all health and disability services)				
Death or permanent severe loss of function that is related to the process of health care and differs from the expected outcome of that care.	Permanent major or temporary severe loss of function that is related to the process of health care and differs from the expected outcome of that care.	Permanent moderate or temporary major loss of function that is related to the process of health care and differs from the expected outcome of that care.	Permanent minor or temporary moderate loss of function that is related to the process of health care and differs from the expected outcome of that care.	Temporary minor loss of function.
Specific Incidents/Consequences				
• Wrong consumer or wrong procedure with risk of or actual severe harm • Suicide as inpatient • Blood component given to wrong consumer • Retained item with delayed removal • Child/infant abduction or discharge to the wrong family • Failure of essential service with risk of severe consumer consequences	• Wrong consumer or wrong procedure with risk of or actual major harm • Retained item with immediate removal • Misadministration of radioactive materials • Unanticipated cardio-pulmonary resuscitation resulting from the process of health care • Community suicide by current mental health consumer within 28 days of contact with service • Missing person with a risk of serious harm to self or others	• Wrong consumer or wrong procedure with risk of or actual moderate harm • Fall resulting in fracture Any of the following as a result of the incident: • Transfer to higher level of care, including hospitalisation • Increased length of stay (>1 day) • Surgical or other significant intervention required	• Wrong consumer or wrong procedure with risk of or actual minor harm • Additional monitoring, investigations or minor interventions as a result of the incident	• Medication error with no harm

Step 2. Determine the frequency or likelihood of recurrence

Rate all adverse events on ACTUAL OUTCOME

Rate all near misses on the most likely potential outcome

Incidents with a high POTENTIAL SAC rating can be notified to the Central Repository (HQSC) via REB at the discretion of the organisation

Including equipment/non-patient related.

Severe	Major	Moderate	Minor	Minimal
• **Services:** Failure of essential service with risk of severe consumer consequences • **Environment:** Toxic release offsite with detrimental effect that caused death • Fire requiring evacuation • **Staff, contractor or visitor:** Death(s) of staff member contactor or visitor • **Equipment:** Major disruption to services due to break down or unavailability, with the risk of consumer harm	• **Services:** significant ongoing disruption to a key service; • **Environment:** Off-site release with no detrimental effects e.g. Ammonia gas leak that causes illness, medical treatment in neighbouring property • Fire that grows larger than an incipient stage • **Staff, contractor or visitor** Permanent disability or loss of function to staff member, contactor or visitor; requires major additional medical or surgical intervention • **Equipment:** Significant disruption to services due to break down or unavailability	• **Services:** Disruption to a key service • **Environment:** Off-site release contained with outside assistance e.g. Ammonia gas leak is an odour nuisance on neighbouring property • Fire at incipient stage or less • **Staff, contractor or visitor** Staff member, contactor or visitor requires extended treatment • **Equipment:** Disruption to key services due to break down or unavailability, causing delay to	• **Services:** Disruption to service • **Environment:** Off-site release contained without outside assistance e.g. Ammonia gas leak that can be contained or repaired by on site staff or an off site contractor • **Staff, contractor or visitor** Staff member or contractor requires short term treatment only with no lost time or restricted duties. Visitor requires short term treatment • **Equipment:** Minor disruption to services, due to break down or unavailability	• **Services:** Minimal disruption to service • **Environment:** Nuisance releases e.g. Ammonia gas leak that has been reported but is not serious enough to repair immediately, to be addressed at next scheduled maintenance. • **Staff, contractor or visitor** Minimal injury to staff member, contactor or visitor, first aid required • **Equipment:** No disruption to services, due to break down or unavailability

Likelihood Table

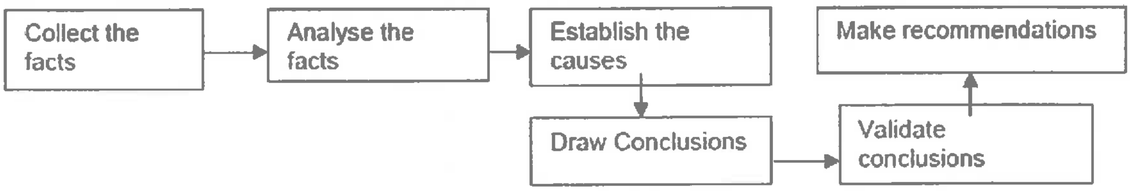
LIKELIHOOD CATEGORY	DEFINITION	CONSEQUENCE				
		Severe	Major	Moderate	Minor	Minimal
Almost Certain	Almost certain to occur at least once in next 3 months	1	1	2	3	4
Likely	Will probably occur at least once in the next 4-12 months	1	1	2	3	4
Moderate	Is expected to occur within the next 1 to 2 years	1	2	2	3	4
Unlikely	Event may occur at some time in the next 2 to 5 years	1	2	3	4	4
Rare	Unlikely to recur – may occur only in exceptional circumstances ie >5 years	1	2	3	4	4

Review Process

SAC 1 SAC 2	• Complete REB Part 1 and send to HQSC within 15WD • Formal review using RCA methodology / London Protocol • Complete REB Part 2 and send to HQSC within 70WD
SAC 3 SAC 4	• Review of incident within 30WD • May complete REB Part 1 and Part 2 and send to HQSC if considered relevant eg. Health sector issue or learning

Back to Contents

12.8 The Principles of Root Cause Analysis (RCA) Investigation and London Protocol



<u>What happened? How did it happen? Why did it happen? Recommendations</u>

Root Cause Analysis (RCA) is a problem solving methodology for discovering the real cause(s) of the problems, or difficulties identified. It fosters a systems based approach to the analysis rather than person centered approach, and has been shown to provide a means for identifying effective solution strategies to a broad range of problems.

The adoption of the RCA approach is a mechanism to find effective solutions to identify problems, and will assist in the development of an open and fair culture where the emphasis is on learning and not apportioning blame. Once root causes have been established corrective action(s) must be agreed upon with a completion date and persons responsible identified for the implementation of the action/recommendation.

The London Protocol differs from the Root Cause Analysis model with its emphasis on gaps and inadequacies within the system and its analysis of the chain of events and contributory factors leading to the adverse event rather than a focus on a single/small number of root cause(s).

All Severe/Major severity rated incidents and some moderate events should be subject to comprehensive investigation. The following sections provide guidance on the steps to follow when carrying out a RCA or London Protocol investigation.

STEP ONE: COLLECTING INFORMATION

All material facts relating to the incident must be gathered as soon as possible after the event. In determining what information to collect the investigator must consider the facts leading up to, as well as the incident itself. For complex events it is only by starting at the point the incident occurred and working backwards that the 'start point' for the incident can be identified. For some incidents the start point will be identified as the patient's admission to hospital (or even before).

Investigators will find it helpful to consider information from a range of sources including:

- The people involved in or witnessing the event
- The place or environment in which the event took place
- The equipment or objects involved in the event
- The paper work related to the event

All staff involved in the incident event must be identified and informed that an incident investigation is taking place. They must be informed that their assistance in investigating the incident would be appreciated and that the purpose of the investigation is to identify areas where systems failed rather than to focus on human error.

All staff involved in tragic or catastrophic incidents must be advised of the availability of confidential support (via the Employee Assistance Programme EAP) and counselling during what will be a stressful period, and told they can have a friend or union rep with them during interviews.

All staff involved and any witnesses to the event should be requested to provide a contemporaneous written record of what occurred and, if necessary, interviewed as soon as possible after the event.

During discussions with staff it is also important to try to determine custom and practice in the workplace in which the incident occurred. The information obtained can help identify the context in which risk factors exist. Where applicable, the investigator should visit the environment where the incident took place preferably before any changes are made, noting the layout and the conditions eg space, flooring, lighting, noise, staffing levels etc. Any piece of equipment involved in the incident should be immediately removed and preserved as evidence.

Other information sources include evidence of:

- Guidelines, policies and procedures
- Clinical records
- Incident reports
- Risk assessments
- Maintenance records
- Clinical audits
- Training records

STEP TWO: COLLATING INFORMATION INTO A NARRATIVE CHRONOLOGY
The simplest way of collating data about an incident is to construct a Timeline.

STEP THREE: IDENTIFYING GAPS
Mapping the chronology of events will start to identify Care Delivery Problems and Service Delivery Problems (CDP).

Care Delivery Problems are problems that arise in the process of care - usually actions or omissions by staff eg care deviated beyond safe limits of practice, failure to monitor, observe, act.

Service Delivery Problems are acts or omissions identified during analysis but not associated with a direct care provision i.e. associated with procedures and systems that are part of the process of service delivery eg failure to implement safe systems of work or environmental standards etc.

Further examples include:

- Delay in diagnosis
- Incorrect risk assessment (for example, of suicide or self-harm)
- Inadequate handover
- Failure to report faulty equipment
- Failure to carry our pre-operative checks
- Not following an agreed protocol (without clinical justification)
- Not seeking help when necessary
- Failure to supervise adequately a junior member of staff
- Incorrect protocol applied
- Treatment given to incorrect body site
- Wrong treatment given

STEP FOUR: EXPLORING PROBLEMS and IDENTIFYING CONTRIBUTORY FACTORS

The simplest way of identifying the principle contributory factors in any investigation is use of the *'Five Why's'* technique. It involves delving deeper into a problem asking *'why?'* for each primary cause identified, then asking *'why'* again in response to each answer until there are no more causes forthcoming. It is best suited for exploring simple non-complex problems. As a brief rule of thumb, it usually takes about five rounds of asking *'why?'* to identify the root cause of a problem. It may be necessary, however, to ask *'why?'* more or less than five times. Other tools which can be used to explore more complex problems further are the fish bone diagram, and reactive barrier analysis (all tools are available on the Quality and Patient Safety section of the Intranet).

STEP FIVE: GENERATING SOLUTIONS

For all root cause analysis investigations a final report should be completed and an action plan identified to reduce any highlighted risk(s).

Recommendations must be specific, measurable, attainable, realistic and timely i.e. SMART.

Any unresolved risks should be discussed at the relevant service quality committee and outstanding issues placed on the service Risk Register as appropriate.

Workplace Violence and Aggression Management

Unique Identifier	HS01/ASD/014 – v04.00
Document Type	Policy
Risk of non-compliance	may result in significant harm to the patient/DHB
Function	Administration, Management and Governance
User Group(s) • Organisation(s) • Directorate(s) • Department(s) • Used for which patients? • Used by which staff? • Excluded	Auckland DHB only Auckland District Health Board All directorates All departments All All staff
Keywords	
Author	Manager - Occupational Health & Safety
Authorisation • Owner • Delegate / Issuer	 Chief Executive & Endorsed by The Board Chief Health Professions Officer
Edited by	Document Control
First issued	February 2008
This version issued	11 February 2020 - updated
Review frequency	3 yearly

Contents

Back to Contents

1. Purpose of policy

The purpose of this policy is to outline the Auckland District Health Board (Auckland DHB) organisational responsibilities to workers who experience violence and aggression in the workplace.

Violence towards workers is a significant health and safety risk. This can take the form of physical or sexual assault, verbal abuse including telephone abuse, racial abuse and threatening behaviour.

These behaviours can originate from the general public, patients or co-workers. Violence and aggression is a significant hazard and as such the risks associated with them need to be managed effectively. This policy should ensure that all workers are able to provide care to patients within a safe environment and must be applied effectively in all appropriate situations.

2. Scope of the policy

This policy extends to all employees as well as students and independent contractors who work for Auckland DHB. Occurrences of worker-to-worker violence and aggression are to be reported to Human Resources and managed as per the Harassment & Bullying Policy.

3. Policy statements

Auckland DHB recognises its legal duty to provide a safe and secure environment for patients, workers and visitors. Violent or abusive behaviour will not be tolerated and decisive action will be taken to protect workers, patients and visitors.

It is the policy of Auckland DHB:

- To ensure risk assessment is completed in order to identify the likelihood workers will be exposed to violence and aggression.
- To identify measures to protect workers and those visiting its premises from the risk of violence and aggression.
- To ensure that staff receive training and resources to manage violence and aggression in the workplace.
- That all forms of intentional violence and aggression to workers are unacceptable: assailants will be reported to the Police where a criminal action has occurred; prosecution will be supported.

4. Definitions

The following terms are used within this document.

Term	Definition
Workplace violence	"Any incident in which an employee has been abused, threatened or assaulted in circumstances related to their work, involving explicit or implicit challenge to their safety, wellbeing or health." (Department of Labour, 2009). This can incorporate some

Term	Definition
	behaviours identified as harassment and bullying, for example verbal violence.
Physical assault	The intentional use of force by one person against another, without lawful justification, resulting in physical injury or personal discomfort.
Sexual assault	Any type of sexual contact that occurs without the explicit consent of the recipient, e.g. unwanted touching or groping, rape and attempted rape.
Non-physical assault	The use of inappropriate words or behaviour causing distress and/or constituting harassment. Examples include: • Offensive or sexually explicit language (including but not limited to homophobic or transphobic slurs). • Unwanted or abusive remarks. • Racially inappropriate language or remarks. • Intimidation and any other non-physical words or actions which cause distress or constitute harassment. The list is not exhaustive and it is a subjective test as to whether a person feels threatened, alarmed, harassed or distressed.
Intentional violence	This definition of violence applies to an aggressor who is knowingly aware of the intent of their actions.
Violence due to a medical or clinical condition	This is where the aggressor does not knowingly choose to present with violent behaviour which is often the result of them experiencing clinical instability. This may be a result of medication, anaesthesia, severe pain, dementia, illness or head injury.
Capacity	An individual is presumed to have capacity for the purpose of this guidance unless they are: • Unable to take in and retain the information material to the circumstances, especially as to the likely consequences of their behaviour in the effect it may have on them having or not having the treatment; or • Unable to weigh the information in the balance as part of a process of arriving at the decision.

5. Documentation

All relevant documentation referred to in this policy is available on the Health & Safety (H&S) intranet site.

6. Roles and responsibilities

6.1 Chief Executive

The Chief Executive is responsible for:

- Ensuring the effective implementation of this policy and the workplace violence prevention programme.
- Allocating sufficient resources to enable the policy to be delivered.
- Monitoring the overall effectiveness of the policy.

6.2 Director of the Directorate/Service Clinical Director

Directors of the Directorate/Service Clinical Directors are responsible for ensuring that arrangements are in place for:

- Monitoring of management of violence and aggression performance within their directorates and areas.
- Ensuring that hazard identification and risk assessments have been undertaken in accordance with the Auckland DHB procedures.
- Ensuring that violence and aggression related risk assessments and control measures are communicated to relevant workers where appropriate.
- Ensuring that hazards and risks are entered onto the Hazard Register as appropriate.

6.3 Operational managers

The first step to ensuring the safety of workers is to perform a risk assessment (see section 7) of the roles and tasks that workers are required to undertake which could lead to a situation of possible violence and/or aggression. Following this assessment, appropriate control measures must be implemented to ensure their safety.

Managers must also ensure that workers receive suitable and sufficient information, instruction (section 8) and training (section 9) in order to safely undertake their role. They must also ensure that risks are appropriately communicated to all staff who may come into contact with known or potential violent and/or aggressive patients/service users (section 8).

Managers must encourage workers to report all incidents of violence and aggression towards them as per Auckland DHB H&S incident occurrence reporting policy, including near misses.

Following an incident of violence or aggression managers must:

- Ensure the safety of their workers and provide post-incident support (section 11); and
- Ensure that a suitable and sufficient investigation is completed to ensure that all cause factors are identified, and to put procedure into place to try to prevent a re-occurrence (section 10). As part of this process they are also responsible for ensuring appropriate sanctions are put in place (sections 13 and 14).

Managers are also responsible for:

- Ensuring workers are aware of their responsibilities for health and safety and violence and aggression; responding to and, where possible, resolving incidents, ideally before they escalate.

Back to Contents

- Ensuring employees are aware of their role in a Code Orange and have clear knowledge and understanding of the process.
- Responding seriously and in a timely manner to any reports of workplace violence, abuse or threats.
- Recording details of the incident and giving all employees involved in the incident full support during the whole process.
- Undertaking self-assessment audits within their area when requested.

6.4 All workers

All workers have a responsibility to:

- Ensure their own safety and that no action or inaction causes harm to any other person.
- Follow the safe systems of work identified for the management of violence and aggression.
- Make full and proper use of control measures including personal protective equipment.
- Report any compliance failures, digressions, defects or concerns to their line manager. supervisor, Health and Safety Representative and/or Occupational Health & Safety.
- Report accidents and near misses.
- Attend training as required.

6.5 Occupational Health & Safety

Provide advice and support to managers in relation to the implementation of this policy.

7. Hazard identification and risk assessment

7.1 Identification of risk

Managers are responsible for ensuring that documented risk assessments (formally hazard control plans) are undertaken to identify and assess risks faced by workers. Following this, they must implement suitable and sufficient measures to eliminate or control the risks and evaluate, monitor and periodically re-assess the measures. Further information on the assessment of risk can be found in Appendix 1.

8. Communication of risk

Section 11 of the Health Information Privacy Code makes it clear that personal health information must be transferred to subsequent caregivers – in relation to the possibility that a patient or client will be violent towards a caregiver.

8.1 Security Alerts

Subsequent caregivers are to be alerted to the potential for violence or aggression from a patient/service user by posting a Security Alert (for individuals who have been assessed as a risk to caregivers) on patient information system by using CR0008 Clinical Alert Notification/Cancellation.

Back to Contents

9. Violence and aggression training

9.1 General training

All staff must receive training in how to safely manage and assess risk of violence and aggression in the workplace at Auckland DHB.

Key areas of training are to include:

- Auckland DHB policies and New Zealand legislation
- De-escalation and personal safety
- Auckland DHB Code Orange procedures
- Processes for reporting incidents of violence and aggression.

Personal safety and de-escalation training available at Auckland DHB:

- CALM online training (mandatory)
- Security for Safety online training (mandatory)
- MAPA 1-day De-escalation Training (for identified clinical staff)
- MAPA Advanced Training - De-escalation and Physical restraint (Security staff and identified Senior clinical staff)
- SPEC Training for Mental Health Inpatient staff.

The appropriate level of training required will be determined upon the level of risk that has been identified by the directorate/service risk assessment.

9.2 Restraint training

All workers who are required to use restraint at Auckland DHB must receive the MAPA Advanced training to ensure the safety of everyone involved.

All restraint training taught should place emphasis on de-escalation, last resort, least restrictive, pain free restraint techniques in alignment with the New Zealand Health and Disability (Restraint Minimisation and Safe Practice) Standards. It is essential that written policies and procedures regarding the use and practice of physical restraint are in place and all workers are fully aware of these and their roles and responsibilities.

10. Incident reporting and investigation

All health and safety incidents and near misses involving violence and/or aggression, including verbal abuse towards workers, must be reported in Datix as per current accident/incident procedures.

The relevant operational manager must suitably investigate all incidents. The operational manager is also required to assess whether workers involved in an incident require follow-up support.

10.1 Learning from incidents

The operational manager must keep the victim fully informed of the progress and outcome of the investigation.

Back to Contents

As part of the investigation, it is important to determine lessons that can be taken forward to minimise similar causes and explore more effective levels of support.

The findings should be communicated to other relevant departments and committees to ensure that Auckland DHB as a whole benefit from them.

11. Post-incident support

Workers are entitled to expect that their actions will be supported with understanding by their supervisors and managers and by Auckland DHB.

A worker who has been attacked may suffer psychological harm as well as physical injury, Confidential counselling services are available through the Employee Assistance Programme and workers can self-refer to this. For physically injured workers, the manager will provide support and assistance for workers in the event of criminal/civil proceedings. All and any support/advice offered should be documented.

12. Health monitoring

The manager must have a system in place to monitor employees who report suffering harm or have been in an incident that could have led to such harm to ensure that the employee is not suffering long term effects from an exposure to aggression or violence in the workplace.

13. Sanctions

Any action taken in response to violent or abusive behaviour should be carefully planned. It should take into account the clinical needs of the service users, the right of all service users to be treated in a safe and caring environment and the duty towards employees.
Actions implemented should be relevant to the circumstances. These can include:

- Drawing the person's attention to the fact that their behaviour is unacceptable.
- Treatment of service users in the presence of increased security or Police and/or alternative treatment facility/location/times/days, including suspension of routine appointments following medical advice.
- Reporting the behaviour to the Police.

Note: As excluding service users from clinical care has legal and ethical implications, it is important that the service user's clinical team meet and come to an agreed documented approach which will endeavour to continue to care/treat the service user and minimise the residual risk of further incidents of violence and aggression.

Visitors who display any unacceptable behaviour should be asked to stop and be offered the opportunity to explain their actions. Continued unacceptable behaviour may result in the individual being asked to leave the premises by a senior member of staff. Such action will need to be undertaken with minimal risk and should not be attempted without appropriate support. Depending on the location and circumstances this can involve the Police or security. Incident reports must be completed for all incidents of violence and aggression. Any request to leave and the visitor's response must be documented.

14. Trespass notice

Trespass notices should be regarded as a last resort after all other means of addressing the situation have been exhausted. They should not be routinely used to manage patient or visitor behaviour.

A Clinical Nurse Manager (or Service Manager/Charge Nurse if the Clinical Nurse Manager cannot be located in an emergency) has delegated authority to issue a trespass notices.

All Service Managers and Charge Nurses should make themselves familiar with the Trespass Notice policy.

15. Lone working

Working alone means the normal contact with other staff is not available. This may include working in isolated areas on-site or off-site, either during or outside normal working hours.

This could be outside a hospital or similar environment, or internally where staff care for patients or service users on their own. Other descriptions commonly used include community or outreach workers. Lone working may be a constituent part of a person's usual job or it could occur on an infrequent basis, as and when circumstances dictate.

By the very nature of their work, lone workers need to be provided with additional support, management and training to deal with the increased risks, as well as being enabled and empowered to take a greater degree of responsibility for their own safety and security.

Specific advice on managing the risk to lone workers are detailed in the Lone Worker Protection policy.

16. Self-defence

Section 48 of the Crimes Act 1961 states, "Everyone is justified in using, in the defence of himself or another, such force as, in the circumstances as he believes them to be, it is reasonable to use".

This recognises that people have a right to defend themselves against violence or threats of violence, so long as the force used is no more than is reasonable for that purpose. The law does not require people to wait until they have been attacked before taking action to protect themselves. But the law also acknowledges the attacker's right to life and bodily integrity and requires the force used in self-defence to be no more than is necessary to prevent the violence or threatened violence.

16.1 Reasonable force

If a worker is in significant danger, and is unable to retreat safely from the situation without the use of physical action, the principles of reasonable force would apply.

What might be considered as reasonable force will differ from case to case. The principle that should guide workers considering the application of reasonable force is to use the minimum intervention (in terms of force and time) necessary to reduce harm and damage. The force used must be consistent with the intended outcome, e.g. the force used to stop a very young child hitting another will differ significantly from that needed to prevent a violent attack from a physically strong adult.

17. Monitoring and review

Adherence to this policy should be monitored by a combination of local inspections and audits.

This policy will be reviewed in line with updated government regulations as and when available.

18. Legislation

- Crimes Act 1961
- Health Information Privacy Code 1994

19. Supporting evidence

- Department of Labour. (2009). Managing the Risk of Workplace Violence to Healthcare and Community Service Providers: Good Practice Guide. Department of Labour.
- Standards New Zealand. (2008). Health and Disability Services (Restraint Minimisation and Safe Practice) Standards NZS 8134.2:2008, Standards Council

20. Associated documents

- Code Orange Policy
- Harassment & Bullying
- Health & Safety
- Lone Worker Protection
- Occupational Health & Safety (OH&S) Occurrence
- Risk Management Policy
- Trespass Notice
- CR0008 Clinical Alert Notification/Cancellation.
- Restraint minimisation and safe practice for patients

21. Disclaimer

No guideline can cover all variations required for specific circumstances. It is the responsibility of the health care practitioners using this Auckland DHB guideline to adapt it for safe use within their own institution, recognise the need for specialist help, and call for it without delay, when an individual patient falls outside of the boundaries of this guideline.

22. Corrections and amendments

The next scheduled review of this document is as per the document classification table (page 1). However, if the reader notices any errors or believes that the document should be reviewed ***before*** the scheduled date, they should contact the owner or Document Control without delay.

Appendix 1: Hazard Identification and Dynamic Risk Assessment

Dynamic risk assessment

"The continuous assessment of risk in the rapidly changing circumstances of an operational incident, in order to implement the control measures necessary to ensure an acceptable level of safety".

During a dynamic risk assessment, the decision making process involves:

- Gathering the available information
- Analysing reviewing the risks and benefits presented by the incident
- Applying professional judgement to decide the appropriate course of action.
- The risk assessment should take into account the past, present and future:
  - **Past** - any previous incidents or known history of violence, verbal abuse or threatening behaviours towards staff
  - **Present** - the environment and any existing arrangements in place to manage the hazards faced by workers, such as the equipment available, communication systems in place and staff skills to manage challenging behaviour
  - **Future** – taking into account all the information available regarding the patient to ensure future interventions will give the patient the best possible chance of a positive outcome.

The risk assessment must consider:

- The acuity of the environment the person is working in to determine the level of risk and any other risk factors, such as lone working
- Assessment of working conditions and environment such as staffing numbers and security measures
- Whether workers have received suitable and sufficient training to defuse potentially violent situations
- The availability of tools to assess the possibility of an increased risk of violence

Assessment of an Individual

It is the responsibility of the service to ensure that there are appropriate methods in place to allow workers to conduct risk assessments for each patient/client at time of admission/referral.
This is to determine if there is any potential or actual risk of the threat to safety of ADHB workers while providing treatment/care, this may be a part of the initial clinical assessment. The level and means of assessment will vary by each service as appropriate to the service being provided.

When assessing risk, the following must be considered:

- Obtain information from those with recent responsibility for the patient/client (caregivers, family, GP, etc...).
- Ensure that patient care plans are updated regularly e.g.: after an incident and fed into Patient Alert system.
- Patient/client information should include: (if known)
  - Known tendencies for violence or aggression
  - Early warning signs the person is starting to become escalated
  - Triggers (both environmental and interpersonal) that may cause the person to become escalated

- Effective calming techniques, identified if necessary in consultation with family/whanau
- Cultural resources/interpreter services that may be useful to the person
- Mobility level
- Any handling aids required
- Presence of infectious disease
- Health care needs that may predispose the person to confusion (and risk of aggression)

There must be procedures in place for the ongoing assessment and reporting of changes in patient/client behaviour. Following the assessment and reporting, if the behaviour continues to be concerning, a behaviour management plan should be developed collaboratively with the person in question and communicated to all people providing care to them.

Appendix 2: Security Alerts

Auckland DHB staff are to be alerted to the potential for violence or aggression from a patient/service user by posting a Security Alert (for individuals who have been assessed as a risk to caregivers) on patient information system by using CR0008 (Clinical Alert Notification).

There are three levels of Security Alert:

Levels	**Description**
Level 1	• The patient/relative is demanding/distressed • Threats are perceived/implied
Level 2	• The patient/relative is: o verbally aggressive o physically threatening o threatening damage of theft of property • Previous level 1 or 2 • Patient unfit to leave department • Physically aggressive prior to admission • Police/prison escort
Level 3	• The patient/relative is: o physically aggressive o damaging property physically threatening o trying to leave and possibly committable

Process for Posting a Security Alert

Step	**Action**
1.	A clinical alert is identified
2.	Complete form (CR0008)
3.	Fax to Clinical Records (Fax. 6959)
4.	CRD workers record on CMS (CHIPS) and turn CRIS alert flag on
5.	File CR0008 in the front of the patients notes for current visit

Back to Contents

Appendix 3: Guidance Checklist for Managers Following an Assault on a Member of Staff

GUIDANCE CHECKLIST FOR MANAGERS FOLLOWING AN ASSAULT ON A MEMBER OF STAFF

The following points should to be considered & carried out by the Manager immediately following an incident:

- Call a code Orange
- Do you need to call the Police?
- Does the member of staff require medical assessment or attention?
- Do you need to cordon off any areas to preserve evidence for the Police?
- Have you obtained the names and contact details of any witnesses, this will include patients and visitors as well as staff members?
- Have you obtained photographic evidence of any injuries sustained by staff or damage caused by the perpetrator?
- If applicable, have swabs of saliva (DNA evidence) been taken or any blood stained clothing preserved?
- Does the member of staff feel fit to continue duties?
- Do they need assistance with transport to get home?
- Do they need recovery time after the incident?
- Has the member of staff had an opportunity to discuss the incident and talk about how occurred and how it was managed? (This will be needed to help with the manager investigation and form completion).
- Does the member of staff require specialist counselling (EAP)?
- Do other members of staff within the team who were affected by the incident require support?
- If applicable, is the member of staff happy to continue to provide care to the patient involved?
- Have the implications for the future health and safety of staff been considered?
- Is a change of working practice or working environment required?
- Has a H&S incident report (KIOSK) been completed?

Trespass Notice

Unique Identifier	PP01/PCR/043
Document Type	Clinical Guideline
Risk of non-compliance	very unlikely to result in harm to the patient/DHB
Function	Administration, Management and Governance
User Group(s) • Organisation(s) • Directorate(s) • Department(s) • Used for which patients? • Used by which staff? • Excluded	Auckland DHB only Auckland District Health Board All directorates All departments All patients and visitors who have trespassed onto Auckland DHB property Anyone with Delegated Authority to Issue Trespass Notices under this policy
Keywords	
Author	Legal Assistant - Legal Services
Authorisation • Owner • Delegate / Issuer	 Chief Financial Officer General Counsel
Edited by	Clinical Policy Facilitator
First issued	Yet to be determined
This version issued	22 October 2019 - updated
Review frequency	3 yearly

Contents

Back to Contents

1. Purpose of guideline

The purpose of this document is to ensure that the issuing of Trespass Notices is effective and follows the appropriate process.

2. Issuing trespass notices

2.1 Safety

Trespass Notices may be issued to ensure that staff and patients/families are safe from aggressive/violent patients/visitors.

2.2 Trespass

Trespass arises from the right of an occupier to control property. The Trespass Act 1980 creates two offences:

- **Warning to leave** – Every person commits an offence that trespasses on any place and, after being warned to leave by an occupier of that place, neglects or refuses to do so.
- **Warning to stay off** – Where a person has trespassed, or there is reasonable cause to suspect they are likely to trespass, the occupier may warn that person to stay off that place. Having been warned that person commits an offence if they trespass on the property.

A Trespass Notice is the means by which an individual is warned to leave and/or stay off. A warning to stay off applies for two years unless specified for a shorter period or revoked.

This policy focuses on rights and process under the Trespass Act however; there are also broad common law rights in relation to property enforceable by a civil action.

2.3 Last Resort

Trespass Notices should be regarded as a last resort after all other means of addressing the situation have been exhausted. They should not be routinely used to manage patient or visitor behaviour. Nor should they be used to penalize an individual.

2.4 Delegated Authority

A Clinical Nurse Manger (or Service Manager/Charge Nurse if the CNM cannot be located in an emergency) has delegated authority to issue trespass notices.

2.5 Records of Notice

For a Trespass Notice to be effective the steps outlined below must be followed and a careful record of service of the Trespass Notice must be kept.

2.6 Accompanying advice – medical attention

Service of a Trespass Notice should be accompanied with advice that the person may access emergency medical/maternity/mental health services if necessary, at any time despite the Trespass Notice. Medical attention should be provided to any person genuinely requiring it.

Back to Contents

2.7 Code of Rights

Issuing of a trespass order does not negate a provider's obligation to take reasonable steps to comply with the Code of Health and Disability Services Consumers Rights, e.g. provide information to patients or their legal representative; allow patients the presence of a support person. Compliance with the Code of Rights may not be possible where a trespass notice is required to address a greater risk.

2.8 Assessed for treatment

A person who persistently attends an Auckland DHB service seeking medical attention should be assessed for treatment before being asked to leave. This may not require a full examination if the person is well known to the service and his/her presentation is unchanged from last contact. The assessment should be documented.

It does however, require a conscious consideration of whether there has been any change from the usual presentation, which might indicate a need for medical attention, as well as an effort to listen to the persons concerns and address their expectations of the service.

2.9 Period of removal

Exclusion periods should apply as follows:

- Twenty four hours:
  - Where the purpose of the Trespass Notice is simply to **remove** an individual from Auckland DHB premises
  - This might be necessary to address immediate aggressive or abusive behaviour
- Two years:
  - Where there is an ongoing risk to individual or property
  - Short term measures have failed and
  - The risk cannot be averted any other way (such as by supervised access)
- Fixed period:
  - Ongoing risk for a defined period of less than two years.
  - This might be the period during which a particular patient is admitted.

Where less than two years the Trespass Notice is deemed to be revoked at the conclusion of the period stated on the Notice.

2.10 Photographs

In most cases, trespassing is associated with a particular service or patient and relevant staff will be able to identify the individual who has been served with a Trespass Notice. Where there is a significant risk of harm from a breach and it is essential for enforcement of the order a photograph of the subject person may be obtained and copied to those staff who need to see it, such as security and staff on duty in the relevant unit or service. The subject person should be provided a copy of the photograph unless this is not reasonably practicable or to do so would undermine its benefit.

2.11 Media

See *Media* policy. While we wish to foster a positive working relationship with the media, we also want to protect Auckland DHB's property rights. The privacy and welfare of our patients and staff are paramount. Media are not permitted on Auckland DHB premises without permission, which can only be granted by the Chief Executive, Chief Medical Officer, General Managers or their designated authority. Typically, this is arranged via the communications department. Where a member of the media arrives unannounced, they should be asked to leave, the communications department informed and, if they fail to leave, the Clinical Nurse Manager contacted. A trespass notice may be issued.

3. Serving a trespass notice – process

3.1 Purpose

The purpose of this process is to ensure that Trespass Notices are correctly issued and proper records kept of their issue.

3.2 Trespass notice form

To print a copy for use, see Appendix 1: trespass notice – warning to stay off

3.3 Process

This table described the process for serving a trespass notice.

Stage	Description
1 - Before issuing Trespass Notice	To identify need to serve a Trespass Notice, ask: • Is the safety of staff, patient or family put at risk by the presence of the person? • Have culturally appropriate steps been taken to manage the person's behaviour? Is an interpreter required? • Can the person be persuaded to leave of his/her own accord? • Has the person trespassed before or is there reasonable cause to believe they will come on to Auckland DHB premises after being warned not to? • Is a Trespass Notice the only way to ensure the person leaves/stays off the premises? • If the person is a patient, has any immediate need for medical assistance been met?
2	Notify Clinical Nurse Manager if not already present.
3 - Completing Trespass Notice	Clinical Nurse Manger (or Service Manager/Charge Nurse if the CNM cannot be located in an emergency) fills out appropriate portions of Trespass Notice with: • Name and address of person to whom Trespass Notice will be issued • Reason for issuing Trespass Notice (**Note:** The Trespass Act does not require a reason)

Back to Contents

Stage	Description
	• Name of particular department/service/hospital/site person is to stay out of • Identify the period during which the person must stay off the premises (24 hours unless there is reason for a longer period) • Name of Hospital/Service requesting Trespass Notice • Clinical Nurse Manager's signature and designation (**Note**: the signatory must be identifiable however they may use their staff ID or another identifier if concerned about their own safety) • Signs the Trespass Notice • Asks Legal Services for help if you have any questions or concerns about filling out the Trespass Notice • Takes copies of the Trespass Notice: o For the patient file if person is a patient or is visiting a patient o For Security o For your own file
4 - Serving the Trespass Notice on Person Present in Hospital or Service	Clinical Nurse Manager must: • Advise Security that they are going to serve a Trespass Notice • Have Security accompany them to serve the Trespass Notice if concerned for safety. • Call the Police for back up if there is a high degree of concern about safety. • Ask the person being served with the Trespass Notice to identify themselves e.g. "are you Joseph/Josephine Kiwi?" • Once the person has acknowledged their identity (or someone present has identified them), hand the Trespass Notice to him/her. • If the person will not take the Trespass Notice from you, leave it at their feet or immediately in front of them and bring their attention to this by saying "This is a Trespass Notice which I am serving on you". The Trespass Act allows an oral Trespass Notice. • Read the Trespass Notice to the person, making sure to read out any conditions on access. • Explain the effect of the Trespass Notice e.g. "This is a Trespass Notice. It requires you to stay out of or off the specified properties for 24 hours/specified period/two years. If you do not leave/stay off the property you will be committing a criminal offence and may be convicted and fined or imprisoned." • Tell the person that if they do not leave, Security will be called to remove them. • Advise the person that they may access emergency medical/maternity or mental health services at any time in spite of the Trespass Notice. • Give the person a reasonable time to leave. The amount of time will vary depending on the situation.

Stage	Description
	- If the person does not leave within a reasonable time, call Security, and the Police if required, to assist. Note that a person assisting in removing someone who is trespassing is permitted to use reasonable force to do so, but they must not strike or do bodily harm to that person. - Complete these steps away from patient, and the public and in a private area whenever possible.
5 - After Serving Trespass Notice	If the person served was a patient or visiting a patient, the Clinical Nurse Manager must: - Give the ward a copy of the Trespass Notice to put on the patient file - Record in patient record full name and position of person serving Trespass Notice - Document in patient record time of service, reading of Trespass Notice to person and giving of advice that s/he may access emergency treatment in spite of Trespass Notice If the person has no connection with a patient, the Clinical Nurse Manager should document events (including time and date of service, identification of person, reading out of Trespass Notice and advice re emergency services) on his/her own file. Send a copy of the Trespass Notice to Security.
6 - Serving Trespass Notice on Person who is Not Present in Hospital/Service	If the person is not present in the hospital or service, the Clinical Nurse Manager either - Telephone the person. If the recipient can reasonably be identified read the Trespass Notice to him/her; and then post the Trespass Notice to him/her by registered post; or - If no contact number, post the Trespass Notice to him/her by registered post; or - Waits for the person's next visit to the hospital and arranges for delivery of the Trespass Notice in accordance with step 4.
7 - Debrief	Clinical Nurse Manager: - Debriefs staff and patient/family if required and in particular explains why the Trespass Notice was issued and its consequences.

4. Breach of a trespass notice

4.1 Trespass

The purpose of this process is to ensure that staff have guidelines for dealing with breaches of Trespass Notices.

4.2 Process

This table describes the process for dealing with a **Breach of a Trespass Notice.**

Step	Action
1.	If a person returns to hospital or service after being issued with a Trespass Notice, staff should: • Assess if there is a valid clinical reason for their return • Call a Code Orange (or relevant security alert); • Remind the individual of the Trespass Notice and ask him/her to leave voluntarily; • If s/he will not leave voluntarily, call Security/the Police and have him/her escorted from the hospital; • If appropriate, notify Police after consultation with Legal Services. • Record events in the incident report and in relevant patient's clinical records.
2.	Debrief staff and patients/family if required.

5. Revoking a trespass notice

5.1 Purpose

The purpose of this process is to ensure that staff are aware that Trespass Notices may be revoked and of the procedure for revoking them.

5.2 Process

This table describes the process for Revoking a Trespass Notice. **Note:** A Trespass Notice is deemed to be revoked where the exclusion period has expired.

5.3 Principles

A Trespass Notice may be revoked in a number of situations including but not limited to:

- Where the individual has a clear need for medical treatment which requires him/her to be on Auckland DHB property
- Where the individual has demonstrated a willingness to behave appropriately while on Auckland DHB property

Step	Action
1.	Contact the Clinical Nurse Manager.
2.	Discuss revocation with staff/family involved when Trespass Notice served.
3.	Clinical Nurse Manager notes on the Trespass Notice that: • The Trespass Notice has been revoked; • The reasons for the revocation of the Trespass Notice; • The date of revocation **and** signs the revocation.

Back to Contents

Step	Action
4.	Clinical Nurse Manager sends a copy of the revocation to: • Security • Patient file (if the individual is a patient or the trespass order was placed on a patient's file - see Stage 5 of Section 3.3) • Person subject to the order • Other relevant staff

6. Police assistance in a trespass situation

Where a person been extremely aggressive/verbalising threats of harm or retribution to Auckland DHB staff who are managing the situation or is assessed as too dangerous to approach, Police assistance may be requested for the serving of the Trespass Notice.

If Police are not in attendance already, a call must be placed by the CNM to the Police via the 111 service.
The Police may serve either the Auckland DHB Trespass Notice on behalf, or a Police-generated Trespass Notice.

If a Police Trespass Notice is used, the CNM must ensure a copy is made for the Auckland DHB prior to serving for the various files.

The additional "seriousness" of a person being personally served a Trespass Notice by the Police will help to de-escalate the situation and minimises the risk of further misbehaviour.

In this situation, the Police will escort the trespassed person off Auckland DHB property on request.

For repeat offenders, it is very useful to have Police involvement as they record their actions and will review their file when informed by Auckland DHB that the incident is a repeat situation. This is particularly valuable as incidents will occur across different shifts and with different management on duty.

7. Legislation

- Trespass Act 1980
- Code of Health and Disability Services Consumers' Rights 1996
- Crimes Act 1961

8. Associated documents

- Media

Back to Contents

9. Disclaimer

No guideline can cover all variations required for specific circumstances. It is the responsibility of the health care practitioners using this Auckland DHB guideline to adapt it for safe use within their own institution, recognise the need for specialist help, and call for it without delay, when an individual patient falls outside of the boundaries of this guideline.

10. Corrections and amendments

The next scheduled review of this document is as per the document classification table (page 1). However, if the reader notices any errors or believes that the document should be reviewed ***before*** the scheduled date, they should contact the owner or Document Control without delay.

Appendix 1: Trespass notice – warning to stay off

AUCKLAND
DISTRICT HEALTH BOARD
Te Toka Tumai

WARNING TO STAY OFF

Trespass Act 1980

TO: [Name] ______________________________

OF: [Address] ______________________________

TAKE NOTICE that in accordance with the provisions of the Trespass Act 1980, you are hereby warned to:

LEAVE [if on the premises]; and

STAY OFF Auckland District Health Board's properties for the following period:
24 Hours [ ]
Other [ ] [specify] ____________________
2 Years [ ]

The properties being: ____

including any associated grounds.

Reason for issue of Trespass Notice / Comment:-

1. This Trespass Notice shall be issued and validated by the Charge Nurse Manager by placement of the Authorising Stamp and their Employee Number on this notice
2. A copy shall be filed in the Trespass Notice Register in the Charge Nurse Manager Office.

Charge Nurse Manager Employee No:

For AUCKLAND DISTRICT HEALTH BOARD

Dated this ____________ **day of** ____________________ **, 20_ _**

Specified Conditions of this Trespass Notice

1. If you require emergency medical, maternity or mental health services you may attend the relevant service in spite of this warning.
2. Unless (1) applies, this notice expires or it is otherwise revoked in writing, should you enter the places specified in this Notice you commit a criminal offence and may be liable to arrest, and upon conviction, to a fine of up to $1,000 and/or imprisonment for up to three months.
3. ADHB reserve the right to use a security photograph obtained during your hospital visit to assist in maintaining conditions of this Notice.
4. If you have any questions regarding this trespass notice please contact the Charge Nurse Manager via the ADHB switchboard 3670000.

Original: Serve to person being trespassed in accordance with the policy. If unable to give a copy, a verbal informing of Trespass is sufficient

Copy to: Ward/Unit Supervisor/Manager, Security, Trespass Register – Charge Nurse Manager Office
Patient Clinical Records [if person being trespassed is a patient or was visiting a specific patient]

Code Orange Policy

Unique Identifier	PP01/STF/076 – v03.00
Document Type	Policy
Risk of non-compliance	may result in significant harm to the patient/DHB
Function	Administration, Management and Governance
User Group(s)	Auckland DHB only
• Organisation(s)	Auckland District Health Board
• Directorate(s)	Auckland DHB wide
• Department(s)	All departments, services and units
• Used for which patients?	All patients and visitors
• Used by which staff?	All staff
• Excluded	
Keywords	N/A
Author	Director - Patient Management Services
Authorisation	
• Owner	Director - Provider Services
• Delegate / Issuer	Director - Patient Management Service
Edited by	Clinical Policy Facilitator
First issued	01 April 2007
This version issued	29 March 2019 - updated
Review frequency	3 yearly

Contents

Back to Contents

1. Purpose of policy

The purpose of this document is to explain the process of a Code Orange and to define Auckland District Health Board's (Auckland DHB) expectations and management of situations where staff have identified that their safety or the safety of others (including the environment) is at risk.

Auckland DHB staff have the right to work in a safe and respectful environment without fear of violence, aggression, abuse or harassment from patients, visitors, and staff.

In accordance with the Code of Health and Disability Services Consumers' Rights, when physical restraint is utilised it should ensure the safety and dignity of the patient is maintained.

2. Scope

The scope of this policy applies in emergencies where the patient, a visitor, family member or other member of the public has not responded to de-escalation or other techniques. This includes where the safety of visitors, patients, staff, or the environment is threatened and emergency assistance must be activated as soon as possible.

The scope of a Code Orange includes Auckland City Hospital site (Grafton, including Starship and Te Whetu Tawera) and Greenlane Clinical Centre. Other sites are expected to have equivalent, locally developed and managed processes, which are referenced in the associated documents section of the policy. The Code Black incidents are outside the scope of this policy.

3. Policy statements

A Code Orange is the Auckland DHB emergency call for assistance to limit or eliminate a risk when staff feel concerned about their own safety, the safety of a patient, others or the environment, or when an incident is impeding or obstructing the provision of clinical care.

During a Code Orange, personal restraint may occur. This is a serious intervention that requires appropriate justification. Restraint must only be used to protect patients, visitors, staff and the environment from harm for the least amount of time in the least restrictive safe way possible following alternative interventions such as de-escalation strategies.

Each episode of restraint must be documented in the clinical record and on the incident management system (Datix).

4. Definitions

Term	Definition
Code Orange	Refers to any situation in which a person feels threatened or intimidated by an individual's behaviour or is concerned about the safety of a patient, others, or the environment including, but not limited to, situations where patients, visitors and staff are perceived as: a. Aggressive, intoxicated or likely to self-harm. b. Unwelcome visitor. c. Manipulative, intimidating or displaying inappropriate behaviour. d. Refusing to respect the rights of others. e. Extremely distressed, confused or agitated. f. Displaying behaviours of concern with actual or potential to harm self or others. g. Obstructing or impeding the provision of clinical care.
Code Orange response team	Refers to a team of allocated staff that are responsible for responding to a Code Orange. The Code Orange team comprises of Clinical Nurse Managers, Liaison Psychiatry, Patient at Risk Team and Security. Other personnel maybe required at times. The Patient at Risk Team may not be immediately available to attend if attending another code. For a Code Orange at Auckland City Hospital (excluding Starship), the contact centre notify all the Clinical Nurse Mangers (Site, Medical, Surgical & Cardiac, Children's & Women's Health), Patient at Risk Team, Liaison Psychiatry team, and Security services. For a Code Orange at Starship, the contact centre notify all the Clinical Nurse Managers (Site, Medical, Surgical & Cardiac, Children's & Women's Health), Kai Tiaki (Māori Health Worker), Patient at Risk Team and Security Services. For a Code Orange at Greenlane Clinical Centre, the contact centre notify the Clinical Operations Coordinator/Clinical Nurse Manager, Security services, Clinical Charge Nurse and Health Care Assistants (located at Greenlane Clinical Centre).
Code Orange response team lead	The Clinical Nurse Manager is the team leader. All staff follow the direction of the team leader to ensure management of the situation is effectively co-ordinated. A Code Orange that occurs within mental health services will be led by the mental health clinical team.
CCTV	All aspects of the Closed Circuit Television (CCTV) System used by, for, or on behalf of the Auckland DHB for security purposes.
Injure	'To injure' means to cause actual bodily harm or psychological distress to a person, self, or physical damage to the environment.
Incident	An event where there is a credible imminent prospect of, or there has been a breach of security or imminent threat of harm, interference with or obstruction to the provision of clinical care.

Back to Contents

Term	Definition
Visitor	Persons including patient visitors, whānau, business visitors and members of the public visiting Auckland DHB sites.
Staff	All employees, Auckland DHB contractors, external contractors, and members of partner organisations working on Auckland DHB premises including students and volunteers.
Huddle	A group discussion with all staff involved in a Code Orange following the event that includes a post event debrief, and a documented action plan which is communicated to staff.
Patient	Services in the Auckland DHB usually refer to patients, clients, or service users according to the type of service and refer to an individual receiving care or treatment from Auckland DHB provider services.
Restraint	Restraint is the use of any intervention by a service provider that limits a patient's normal freedom of movement. Restraints can be categorised as personal restraint, physical or mechanical restraint, environmental restraint or seclusion (see Associated documents).

5. Principles

The key principles guiding the Auckland DHB response to a Code Orange are:

- **Respect:** All actions should demonstrate respect for the person and others during a Code Orange.
- **Dignity:** All actions should maintain the dignity and emotional safety of those involved and witnessing the event.
- **Engagement:** If possible, engage the patient and the visitor and obtain cultural advice to assist in calming and de-escalation of the situation.
- **Environment:** To limit people entering and exiting the immediate area in which the Code Orange is occurring, and attempt to restrict the movement of the person(s) causing the Code Orange.
- **Communication:** Ensure communication is effective between the Code Orange team and those in the immediate vicinity, with attempts to resolve the Code Orange as soon as it can be done safely and effectively. The Code Orange team when required will escalate to a Code Black, to Auckland DHB senior management or emergency services as soon as possible.
- **Documentation:** Staff act in accordance with associated policies and procedures (*Restraint Minimisation & Safe Practice* policy and *Workplace Violence and Aggression Management* guideline).
- **Safety:** Maintain clinical safety and care for patients during and following a Code Orange.

6. Ethical and legal considerations

In the event of a restraint occurring during a Code Orange, the team must ensure dignity and respect are maintained, and the least restrictive restraint is applied for the shortest duration, minimising any risk of harm. Any unauthorised restriction of a person's freedom of movement could be viewed as a false imprisonment and could result in an allegation of assault.

Auckland DHB is responsible for the provision of appropriate training to prepare clinical and security staff for the event of a Code Orange. Decisions made in response to a Code Orange will ultimately be made in situations with limited information and actual or potential hostile environments.

7. Cultural aspects

All staff need to understand Tikanga Best Practice and be culturally competent when attending a Code Orange. 'Tikanga Best Practice' is a policy founded on Māori concepts, views of health, tikanga (Māori values/practices) and Te Tiriti o Waitangi. Modules are available on Ko Awatea LEARN and may assist Code Orange staff more effectively with de-escalation and restraint management for Māori patients.

8. Staff training

To ensure all staff members understand the requirements of the Code Orange Response Team, mandatory training can be found on the Auckland DHB section of the Ko Awatea LEARN website and must be completed by all clinical staff and security staff. Modules include:

- Restraint Minimisation and Safe Practice.
- CALM Communications for Auckland DHB.
- Understanding Tikanga Recommended Best Practice.

Code Orange response staff must have completed the Code Orange Simulation Training, and both the foundation and advanced training course 'Management of Actual and Potential Aggression' (MAPA). Clinical staff are required to attend the advanced training course to understand the restraint being applied by security and to effectively lead a restraint episode, and at times, the clinical lead may need to assist with the restraint.

The Code Orange team will attend annual training courses on either the foundation and advanced MAPA refresher courses organised by the Head of Security Services along with regular refresher training workshops held at Auckland DHB throughout the year.

Only staff members trained in de-escalation and restraint may co-ordinate and manage a personal restraint event. Where physical/mechanical restraints are applied as part of a clinical procedure, staff members must have been trained in and competent with their safe application.

8.1 Staff safety

Auckland DHB is committed to taking all practicable steps to eliminate or reduce threats to personal safety of its employees caused by aggressive behaviour or overt actions of a patient, a visitor and other employees. Staff members' safety must be managed according to the *Workplace Violence and Aggression Management* guideline.

Back to Contents

9. Responsibilities

All staff members are fully conversant with their roles in the Code Orange team. The Clinical Nurse Manager is the team leader and is responsible for ensuring safety is maintained. For Code Orange events occurring in mental health units, the mental health clinical team will lead the response with support from the Code Orange response team.

The Clinical Nurse Manager (or mental health clinical lead) adheres to set roles and responsibilities, and the Code Orange team work under the instruction of the Clinical Nurse Manager to ensure a situation is effectively and safely coordinated.

9.1 Code Orange response team

The Code Orange response team is responsible for:

1. Responding to the Code Orange immediately as per response guidelines, standing operating procedure, and task cards.
2. Assisting with de-escalation.
3. Utilising calming and restraint techniques as per Auckland DHB policy if the Code Orange is potentially or actually hostile.
4. Complying with Code Orange response team lead directions who will decide how to manage the situation and instruct the team accordingly.
5. Debrief huddle following on Code Orange event.

9.2 Code Orange response team lead

The Code Orange response team lead is responsible for:

When attending a Code Orange, the team leader will receive a brief from the allocated nurse, and assess the safety of the situation.

In consultation with the Code Orange team, the team leader will ensure the safety of the patient, others, and environment is maintained by instructing the team of their responsibilities at the time:

1. The team leader will ensure the appropriate procedures for the current situation are followed by using de-escalation techniques prior to any restraint episode as an initial preventative measure.
2. Removing an aggressive patient or person to another area if safety can be maintained.
3. Evacuating the immediate area to ensure the safety of bystanders.
4. To provide emotional safety to people witnessing the event.
5. To allocate appropriate resourcing on the ward by ensuring the safety of others, staff, and patients.
6. To remain present throughout the event and evaluate when safety has being maintained for all involved in the Code Orange.
7. To inform senior management and emergency services as soon as possible when required.
8. To ensure if restraint is used it is the least restrictive and for the shortest duration possible.
9. To complete documentation of the Code Orange in the clinical notes if restraint has occurred. (see Documentation following a Code Orange).
10. Deciding when a Code Orange can be stood down and advising the Code Team and other parties that the Code has finished.

Back to Contents

11. To ensure a post Code Orange huddle occurs with the involved staff including the medical team, and staff whom need emotional support to enable a debrief and reassessment of patients plan of care.
12. Complete an incident (Datix) report.

9.3 Security Services

Security Services are responsible for:

1. Meeting emergency services when they arrive onsite, escorting emergency services to the incident if they are not already there, and providing emergency services with any required resources.
2. Ensuring the Security Control Room is equipped with floor plans, relevant policies related to security services, operations, evacuation procedures, key contacts, and communication technologies so it is available for use as primary incident control point.
3. Ensuring a secondary Security Control Room location is available and resourced.
4. Operating resource and systems as directed. For example, dispatching personnel, initiating the lock down, using CCTV to monitor and track the person(s) for whom the Code Orange was called, using other access control measures such as parking services.
5. Remaining available to support emergency services and/or incident management team until the incident is resolved.
6. Acting on the advice and instruction of the Clinical Nurse Manager (or other clinical lead).
7. Performing safe, least restrictive restraint if required and when directed.

10. Documentation following a Code Orange

Following a Code Orange, it is a requirement that documentation must be completed by the clinical lead. The reporting and recording of personal and physical restraint should be routine practice. Every situation when a Code Orange occurs must be recorded on an Incident Reporting Form (IRF 1) located in Datix, recorded in the clinical notes, and Code Orange logbook.

10.1 Clinical Nurse Manager documentation

All personal and physical restraint and Code Orange episodes must be reported and recorded immediately in the patients' clinical notes.

When restraint has occurred documentation must be appropriate and accurate. Record the restraint event on the CR0142 Post Code Orange Review, include:

a. A detailed description of what happened and names of who was involved
b. Contributing factors and time of the incident
c. The type(s) of restraint used and the duration
d. Alternative strategies used prior to restraint episode
e. Management plan following restraint
f. Relevant information following post restraint huddle

10.2 Security staff documentation

The security staff document all Code Orange events in the Code Orange logbook located in the Security Control Room (SCR).

Back to Contents

When restraint has occurred documentation must be appropriate, accurate, recording of the restraint event should include:

1. Date, location and time of code
2. Police event, CCTV coverage, persons assaulted
3. Type of restraint or intervention used
4. Length of the physical intervention
5. Name of Clinical Nurse Manager present
6. Clinical staff are responsible for completing Datix entries following Code Orange. Security may complete Datix if directed.

11. Legislation

- Health and Safety at Work Act 2015
- Health Information Privacy Code 1994 (revised 1998)
- Privacy Act 1993
- Trespass Act 1980
- Crimes Act 1961

Standards

- 8134.2:2008 Health and Disability Services (Restraint Minimisation and Safe Practice) Standards

12. Associated documents

- Behaviours of Concern (BOC) - Patient Observation
- Security Closed Circuit Television (CCTV) System Policy
- Code Black - under consultation
- Emergency Management
- Employee Assistance Programme
- Restraint Minimisation & Safe Practice
- Resuscitation - Paediatric Emergency Response Teams
- Security ID Card Policy
- Security (Physical) Policy
- Trespass Notice - Auckland DHB
- Weapons Management in AED
- Workplace Violence and Aggression Management
- 91 Paging System - Rehab Plus
- Health & Safety Hazard Identification and Risk Assessment
- CR0142 Post Code Orange Review

13. Disclaimer

No guideline can cover all variations required for specific circumstances. It is the responsibility of the health care practitioners using this Auckland DHB guideline to adapt it for safe use within their own institution, recognise the need for specialist help, and call for it without delay, when an individual patient falls outside of the boundaries of this guideline.

14. Corrections and amendments

The next scheduled review of this document is as per the document classification table (page 1). However, if the reader notices any errors or believes that the document should be reviewed ***before*** the scheduled date, they should contact the owner or Document Control without delay.

Back to Contents

Security (Physical) Policy

Unique Identifier	PP01/F&E/030 – v04.00
Document Type	Policy
Risk of non-compliance	may result in significant harm to the patient/DHB
Function	Administration, Management and Governance
User Group(s) • Organisation(s) • Directorate(s) • Department(s) • Used for which patients? • Used by which staff? • Excluded	Auckland DHB only Auckland District Health Board All directorates All departments All patients All staff
Keywords	n/a
Author	Head of Security Services
Authorisation • Owner • Delegate / Issuer	 Chief Health Professions Officer Chief Health Professions Officer
Edited by	Clinical Policy Facilitator
First issued	December 2002
This version issued	15 June 2018 - updated
Review frequency	6 monthly during the Security for Safety Programme. Every 2 years thereafter as per Government Protective Security Requirements (PSR) best practice.

Contents

Back to Contents

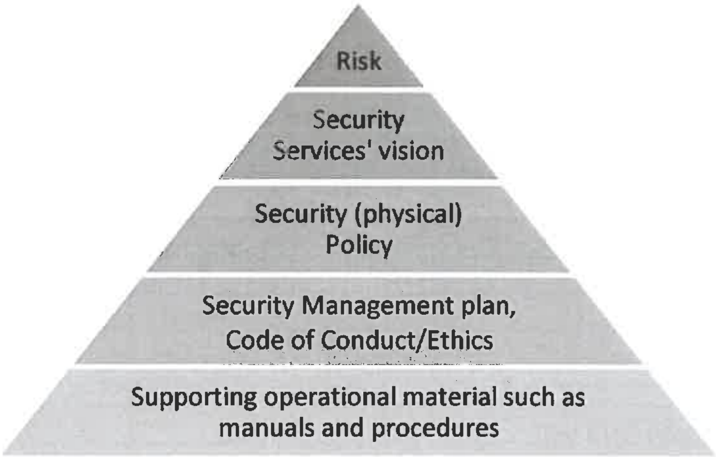
1. Purpose of policy

This policy:

- Outlines the security arrangements that support the Auckland District Health Board (Auckland DHB) in maintaining a safe and secure environment;
- Ensures the Auckland DHB provides security services that meet industry and legislative requirements (refer to associated documents for reference to these).
- Outlines key responsibilities

2. Introduction

- In order to maintain a safe and secure environment on Auckland DHB sites, security arrangements are in place.
- The Protective Security Requirements (PSR) outlines Government's expectations for security management. This policy covers one of the four PSR mandatory security requirements; physical security.
- This policy does not include detail covered elsewhere (refer to associated documents for related information such as *Closed Circuit Television (CCTV)* and *Security ID-Card* policies).
- The diagram below shows the relationship between this policy and other documentation/information. All are in accordance with legislation and the Health Board's values, are guided by the PSR, and seek to manage or mitigate security risk(s).



Risk

Security Services' vision

Security (physical) Policy

Security Management plan, Code of Conduct/Ethics

Supporting operational material such as manuals and procedures

3. Scope

This policy applies to everyone on all Auckland DHB sites, including those outside the main Auckland DHB locations.

This policy does not include the other three areas of mandatory security requirements in the PSR (Governance, Information and Personnel) as it is expected these will be covered elsewhere.

4. Definitions

The table below defines terms used in this policy.

Term	Definition
CCTV	All aspects of the Closed Circuit Television (CCTV) system used by, for, or on behalf of the Auckland DHB for security purposes. This includes the design, installation, operation and management of any hardware, equipment, software, cabling, associated IT and communications, control and monitoring centre and any information created by the system.
Incident	An event where there is a credible, imminent prospect of, or there has been a breach of security, or imminent threat of, harm.
Procedures	Generally - standard operating procedures, being the documented processes to be followed in association with security arrangements and security incident interventions.
Property	Buildings, plant and equipment, Auckland DHB vehicles, revenue, information, property and chattels, land, and such directly associated with DHB operations.
PSR	The Protective Security Requirements (PSR) outlines the Government's expectations for managing personnel, physical and information security. The PSR sets out what agencies must and should consider to ensure security is managed effectively, assures continuity of service delivery, manages risk, and ensures measure are in place to protect New Zealand's people, information, and assets. Content is provided by the Department of Prime Minister and Cabinet, the New Zealand Security Intelligence Service (NZSIS), and the Government Communications Security Bureau (GCSB).
The public	Members of the public who use the Auckland DHB's facilities.
Safety	Freedom from real and perceived harm from criminal threats.
Security	Protective arrangements intended to provide safety for people; and prevent property crime.
Security support	The primary purpose of Security Support work is to provide a security presence when a worker feels unsafe.
Service definition	The service definition articulates the elements and structure of a Security Service that will meet Auckland DHB organisational needs.
Standards	Mandatory performance requirements associated with any aspect of the security systems that must be met, which are linked to the requirements of the Privacy Act.
Visitor	Persons including patient visitors, whānau, business visitors and members of the public visiting the Auckland DHB sites.
Worker	"Worker" refers to all employees, Auckland DHB contractors, external contractors, and members of partner organisations working on Auckland DHB premises including students and volunteers.

Back to Contents

5. Policy statements

The principles of this policy are guided by the PSR for physical security. At Auckland DHB, this means:

- Physical security is governed by the Board;
- A structure remain in place to manage physical security, including a Head of Security Services reporting to a member of the Executive Leadership Team;
- Security risk and practice are successfully managed;
- Clear direction on physical security is provided through operationalising comprehensive policies, procedures, processes, plans, and codes of conduct/ethics for all aspects of physical security;
- All related matter is reviewed every two years (or earlier if necessary) to ensure they meet the ongoing needs of the Auckland DHB;
- An annual review and assurance system is in place;
- Training over and above that provided to all Auckland DHB workers will be provided to security workers so they are trained in all matter related to security;
- Measures are in place for reporting and investigating security incidents, and taking corrective action;
- Physical security considerations and requirements are integrated into facility selection, planning, design, development, and modification in order to mitigate security risk;
- All security workers - including any contracted security providers - will comply with this policy and all Auckland DHB security arrangements;
- Any and all security arrangements and activities must be consistent with health and safety requirements, and show a duty of care for the physical safety of visitors and patients.

6. Responsibilities

6.1 The Auckland DHB will:

- Work to ensure successful management of security risk and practice;
  - Noting, that Directorate Leadership teams are ultimately responsible for security risk and practice within their directorate and associated facility(-ies). For areas that are not part of a Directorate, the responsibility for security risk and practice is with the General Manager and/or Executive owner of that area.
- Work with external agencies as necessary and appropriate, including referring any criminal activity to the New Zealand Police for investigation.
- Have a team of trained, respected, and culturally aware security professionals.
- Ensure security systems such as access control and CCTV are available for appropriate strategic operation in accordance with this and related policies, standards, and legislation;
  - For example, to protect people from harm the Auckland DHB may use access control in accordance with the Auckland DHB *Restraint Minimisation & Safe Practice* policy and New Zealand Standard 8134:2008 Health and Disability Services (Restraint Minimisation and Safe Practice) Standards (see legislation and associated documents).

Back to Contents

- o Ensure tools are available and utilised as appropriate to support the work of Security Services. This may include computers, cell phones, landline phones (including those on independent lines), pagers, and radio networks.
- o Ensure access plans are developed with all directorates/departments, and that these will be:
  - Maintained, operationalised, and reviewed with both clinical and non-clinical leadership;
  - Scoped for the specific risks(s) identified for the directorate/department;
  - Owned by the directorate/department;
  - Reviewed every two years or sooner if necessary.
- o Ensure Security Management Plans are developed as necessary for areas and/or service, and that these will:
  - Be maintained, operationalised, and reviewed with both clinical and non-clinical leadership; for example Children's (NICU), Women's (Maternity), Emergency Department(s), and Community Sites;
  - Be scoped for the specific risk(s) identified for the area and/or service;
  - Be owned by Security Services;
  - Determine appropriate action to mitigate the risk(s);
  - Include roles and responsibilities, procedures, and risk profiles;
  - Be reviewed annually or sooner if necessary.

6.2 The Head of Security Services will:

- o Ensure this policy is implemented in its entirety;
- o Effectively communicate with and report to Auckland DHB leadership teams including, but not limited to, the Board, Executive Leadership, and clinical leadership;
- o Develop and maintain effective relationships with related agencies and key stakeholders such as the New Zealand Police;
- o Support the Auckland DHB in developing security safety strategies to mitigate security risk. This includes ensuring the provision of quality, customer-centric, professional advice to all levels across the Auckland DHB regarding physical security considerations and requirements;
- o Maintain a current understanding of the organisation's security and strategic priorities and integrate these into the management of security policies, procedures, and plans. This includes during critical/emergency incidents and special events;
- o Lead and coordinate resourcing as necessary and appropriate to effectively meet the needs of the Auckland DHB, while also ensuring no workers, including Security workers, are tasked with anything that may put them at undue risk of harm;
- o Ensure all security workers act in a manner that upholds the Auckland DHBs values, Security Services' values, Security Code of Conduct, and Security Code of Ethics;
- o Take responsibility for the development, maintenance, operationalisation and annual review of an organisational Security Management Plan. This plan will document security risks and shape security services/resources.
- o Ensure all security incidents and risks are recorded, actioned, analysed, and reported as required and are assessed against the Auckland DHB Risk Matrix. This includes use of systems such as the Datix Safety Management System.

Back to Contents

- Proactively communicate across the Auckland DHB to effectively promote healthcare security in a way that enhances security services and grows capability;
- Review (including via process testing) and investigate the performance of, and compliance with, Security arrangements;
- Ensure documentation is developed, operationalised, and maintained as necessary. This includes policies, procedures (such as Standard Operating Procedures (SOPs)), plans (such as Access Plans and Security Management Plans), and Codes of Conduct/Ethics;
- Ensure Security Services at Auckland DHB meet industry requirements, certification(s) of compliance (such as the Vulnerable Children Act (VCA) checks, Certificates of Approval (CoA)), and personnel specifications.
- Ensure all security workers are adequately trained to complete the tasks required of them. This includes in legislation (refer Associated Documents) and Auckland DHB policies and practical applications such as de-escalation;
- Manage Security Services contract(s) (if any) in a way that is mutually agreeable, within budget, and aligns with the Auckland DHBs values and Operational Plan;
- Manage complaints about security services or personnel. This includes listening to and investigating the complaint(s), participating in the Auckland DHB complaints process, and taking action as necessary
- Ensure administration of business systems/networks such as access control and CCTV;
- Manage all incidents of non-compliance where related to security.

6.3 Security Service workers will:

- Uphold the values, conduct, and ethics expected of them as expressed in documentation/ training;
- Proactively engage with all those on site to give assurance of a well-managed and well-maintained security-safe environment;
- Take responsibility for their competence with and confidence to complete any SOPs, including adequate record keeping;
- Manage key entrances in a way that demonstrates both a safe and welcoming environment, verifies access/identification, and screens for prevention of unwanted behaviour/activities;
- Issue access control privileges; including the administration of security ID cards and physical keys in accordance with related policies;
- Regularly patrol the premises, both physically and virtually, in order to provide a safe and secure environment. If patrols uncover something that weakens or potentially weakens security, security workers will action them as appropriate.
  - Physical patrols may include regular visits to clinical areas, checking doors/windows are secured, and checking vehicle areas and people ways.
  - Virtual patrols may include using CCTV to locate people who have absconded or have been abducted, to monitor/track suspicious or criminal behaviours, or to support the management of vehicle traffic flows.
- Process lost property and patient valuables in accordance with the Auckland DHB *Valuables, Property and Taonga* policy (see associated documents). Including good record keeping, safe storage and appropriate processes for reuniting items with their owners;

Back to Contents

- ○ Support the management of traffic flows including enforcement of parking legislation and Auckland DHB parking criteria;
  - This may include towing, if necessary and if in accordance with Auckland DHB procedures. For example, to allow exemptions for those in a time of extreme distress/critical need.
- ○ Provide response to security risk including but not limited to:
  - Alarm notifications, Code calls, and during critical/emergency incidents,
  - 'Security Support' work,
  - Security escort for both workers and patients/visitors. Note: No worker is permitted to escort anyone off site solely to smoke or vape.
  - Assistance during large cash collection(s),
  - Stations at key areas such as the Emergency Department(s).
  - Enforcing the Trespass Act 1980 (via Clinical Nurse Manager) as essential to provide a safe and secure environment (see legislation). Note: Trespass may only be done as a last resort in accordance with legislation, Auckland DHB *Trespass Notice* policy, and with advice that the person may access emergency medical/maternity/mental health services if necessary at any time despite the Trespass Notice (see associated documents);
- ○ Comply with all security related legislation, policies, procedures, and otherwise;
- ○ Assist all other workers, visitors, and patients onsite to comply with all security related legislation, policies, procedures, and otherwise which help the Auckland DHB to provide a healthy environment. This includes:
  - Supporting the Auckland DHB to uphold the Smokefree Environments Act and the Auckland DHB smokefree policy.
  - Appropriately escalating any non-compliance.

6.4 All workers

While the Auckland DHB manages safety and security risks, workers are ultimately responsible for their own safety and security while working at Auckland DHB. This includes:

- Participation in background checks and pre-employment screening, as required;
- Minimising security risk by being vigilant;
- Reporting any security breaches. For example, damage to hospital property, theft, unauthorised access to restricted areas, and suspicious behaviour;
- Ensuring they are familiar and in compliance with Auckland DHB security arrangements;
- Supporting all other workers, visitors, and patients to comply with security arrangements.

6.5 Visitors and patients

All visitors and patients must comply with Auckland DHB security arrangements. This includes:

- Not accessing or attempting to access restricted areas;
- Registering with Security, as required.

Back to Contents

7. Legislation

- AUS/NZ Standard ISO 31000:2009 Risk Management - Principles and guidelines
- Crimes Act 1961
- Crimes Act 1961
- Health and Disability Commissioner (Code of Health and Disability Services Consumers' Rights) Regulations 1996
- Health and Safety at Work Act 2015
- Health Information Privacy Code 1994
- Human Rights Act 1993
- Intelligence and Security Act 2017
- New Zealand Bill of Rights Act 1990
- New Zealand Standard 8134:2008 Health and Disability Services (Restraint Minimisation and Safe Practice) Standards
- Official Information Act 1982
- Privacy Act 1993
- Privacy Commissioner: Privacy and CCTV guidelines
- Private Security Personnel and Private Investigators Act 2010
- Protective Security Requirements
- Public Records Act 2005
- Smoke-free Environments Act 1990
- Trespass Act 1980

8. Associated documents

- Health & Safety Hazard Identification and Risk Assessment Guideline
- Behaviours of Concern (BOC) Patient Observation
- Security Closed Circuit Television (CCTV) System Policy
- Clinical Records Management
- Code Orange Calls
- Code Black (pending publication)
- Code of Rights
- Consumer Complaint Management
- Discipline & Dismissal
- Clinical Record Management
- Family Violence - Intimate Partner Violence Intervention
- Information Privacy and Security
- Key Management
- Lone Worker in Community Setting
- Media
- Occupational Health & Safety (OH&S) Occurrence
- Prison or Police Officer Escort
- Restraint Minimisation & Safe Practice
- Security ID-Card Policy

Back to Contents

- Smokefree (and vaping)
- Trespass Notice
- Valuables, Property and Taonga
- Workplace Violence and Aggression Management

9. Disclaimer

No guideline can cover all variations required for specific circumstances. It is the responsibility of the health care practitioners using this Auckland DHB guideline to adapt it for safe use within their own institution, recognise the need for specialist help, and call for it without delay, when an individual patient falls outside of the boundaries of this guideline.

10. Corrections and amendments

The next scheduled review of this document is as per the document classification table (page 1). However, if the reader notices any errors or believes that the document should be reviewed ***before*** the scheduled date, they should contact the owner or Clinical Policy Facilitator without delay.

Back to Contents

Information Privacy and Security

Document Type	Policy
Risk level (content)	High
Function	Corporate Administration, Management & Governance
Directorate(s)	Auckland District Health Board Generic
Department(s) affected	All Auckland DHB departments
Applicable for which patients, clients or residents?	N/A
Applicable for which staff members?	All Staff
Key words (not part of title)	
Author – role only	Chief of Intelligence & Informatics
Owner (see ownership structure)	Chief of Intelligence & Informatics
Edited by	Document Controller
Date first published	April 2007
Date this version published	02 March 2017 – updated
Review frequency	3 yearly
Unique Identifier	PP01/F&E/034 – v02.00 (PP01/PCR/010 Privacy of Patient Information is now included in this document)

Contents

1. Purpose of policy

The purpose of this policy is to ensure that the appropriate privacy and security measures are in place to protect patient privacy and to safeguard Auckland DHB patient and other personal or business–related information, including appropriate use of Auckland DHB's information systems, networks, equipment and associated infrastructure.

2. Scope

This policy applies to:

- All patient and other personal or business–related information that is collected, created, received, stored, accessed or retained in the course of Auckland DHB business activity, which must be protected according to its level of sensitivity, criticality, or value, regardless of the media on which it is stored or its location.
- All locations from which Auckland DHB information is accessed, including home and offsite/remote use.
- All approved users of Auckland DHB patient and other personal or business–related information including:
  - Auckland DHB Employees (including full time, part time, casual or temporary staff)
  - Agents
  - Contractors
  - Students
  - Visiting health professionals
  - Volunteers

In this policy staff means any of the above, who may collect, create, receive, store, access or utilise Auckland DHB patient and other personal or business–related information, information systems, networks, equipment or associated infrastructure.

3. Responsibilities

Auckland DHB has a responsibility to comply with all legislation, standards, codes and guidelines relevant to the appropriate management of patient and other personal or business–related information.

It is the responsibility of all staff who collect, create, receive, store, access, use, maintain or support patient and other personal or business–related information (systems), regardless of the format of the information, to ensure that information is accurate, stored securely, protected from loss, damage, unauthorised access, alteration or corruption at all times.

All staff are required to:

- Have read, understood and signed the Auckland DHB Staff Agreement – Privacy, Security & Confidentiality of Patients & Other Personal or Business-Related Information, and Appropriate Use of ADHB Systems & Technology – prior to commencing their role.
- Have an appropriate level of understanding of their obligations relating to the use of patient and other personal or business–related information for the area/service in which they work. If in any doubt, they should seek clarification from their Line Manager.
- Undertake appropriate training relevant to their role.
- Adhere to professional standards and legal duty to keep patient and other personal or business–related information safe and secure.
- Familiarise themselves with the contents of this and all associated policies relating to the management of patient and other personal or business–related information.

4. Definitions

Term	Definition
Business-related information	Any information about ADHB business that does not relate to an identifiable individual or an individual patient (e.g. financial or procurement records).
Corporate record	Any documentation or evidence of activity created by or related to ADHB business, excluding patient information. The term 'corporate record' encompasses personal and other business-related information.
Information	In this policy 'information' refers to patient and other personal or business–related information unless otherwise specified.
Information system	An electronic system used to create, store or provide access to patient and other personal or business–related information.
IT equipment	Hardware (including personal computers and portable devices, such as laptops and cell phones), computer software, printers and facsimile machines.
Malware	A software application that is malicious in nature and intended to compromise information security.
Patient Information	Identifiable information about an individual patient's health or about health services provided to an individual patient, stored within the ADHB clinical record.
Personal information	Any information about an identifiable individual (e.g. personnel/ HR records).
Portable device	An electronic device that is easily physically relocated, such as a laptop or tablet computer.
Removable storage device	An electronic device connected temporarily to a computer to accept or deliver data, such as a USB (Universal Serial Bus) or backup device.

5. Information privacy and security principles

The following principles provide a framework for the management of patient and other personal or business–related information at Auckland DHB.

- Patient and other personal or business–related information will be classified to the appropriate level and in accordance with relevant legislative, regulatory and contractual requirements and Auckland DHB policy.
- All users must handle patient and other personal or business–related information appropriately and in accordance with its classification level.
- Patient and other personal or business–related information should be secure and only available to those with a legitimate need for access.
- Patient and other personal or business–related information will be protected against unauthorised access.

5.1 Privacy of patient information

The Health Information Privacy Code 1994 is a Code of Practice issued by the Privacy Commissioner that gives extra protection to patient information because of its sensitivity.

The 12 rules of the Code substitute for the 12 privacy principles in the Privacy Act 1993.

Auckland DHB has implemented policies, procedures and systems to ensure the privacy of patient information is protected, aligned with the rules in the Code as summarised below:

- Rule 1: Only collect health information if you really need it.

- Rule 2: Get it straight from the people concerned where possible.
- Rule 3: Tell them what you're going to do with it.
- Rule 4: Be considerate when you're getting it.
- Rule 5: Take care of it once you've got it.
- Rule 6: People can see their health information if they want to.
- Rule 7: They can correct it if it's wrong.
- Rule 8: Make sure health information is correct before you use it.
- Rule 9: Get rid of it when you're done with it.
- Rule 10: Use it for the purpose you got it.
- Rule 11: Only disclose it if you have a good reason.
- Rule 12: Only assign unique identifiers where permitted.

6. Patient privacy - collection, use and display of patient information

- Information for patients about the purposes for which Auckland DHB collects information, and patient rights with respect to their information, will be prominently displayed in patient waiting areas.
- The patient registration process requires all patients to complete a Patient Registration Form (CR0001) which contains a General Privacy Statement, explaining the purpose for the collection of information and the purposes for which patient information may be used.
- By signing the Patient Registration Form patients consent to the collection and use of their information, including sharing of information with other healthcare providers involved in their care.
- Patients may decline permission for use of their information for teaching, presentation or publication. This must be documented in the clinical record and the refusal honoured.
- When collecting information from a patient staff must take all care to ensure that this is done in a location and in a manner that respects the patient's privacy.
- In multi-bed rooms staff should respect patient privacy by obtaining verbal consent for conducting discussions with the patient in the area, and then talking quietly with curtains drawn.
- Staff must check with the patient whether they wish family/whanau to be present for any discussion regarding their care or treatment.
- Wherever possible patients are to be asked on admission to a ward if their name may be displayed on room doors, and above or on beds/cots.
- Patient details that are displayed in public-facing areas (such as room doors, above or on beds/cots) are only to show the patient name, room and the name of the responsible clinician.
- Electronic whiteboards displaying information other than the patient name, room and the name of the responsible clinician must be located and positioned so that they are not public-facing.
- Patients may request that no information be given to persons enquiring; not even that they are in hospital or attending a visit or general information. In response to general enquiries, unless specific consent is given by the patient or their representative, only information about their presence, location and general condition (e.g. satisfactory) may be released.
- Conversations between staff concerning individual patients are to take place in a private location. Conversations must not take place in pubic lifts, in the cafeteria, on the staff shuttle or using a phone in a public area.

7. Information classification

Staff must be aware of the different categories applied to information in order to ensure information security, privacy and legal compliance.

7.1 Categories of information

All Auckland DHB information (including information entrusted to Auckland DHB from third parties) falls within one of the following four classifications.

Classification Grade	**Classification Description** (see notes below)
C1	Unclassified
C2	Internal Use Only/ Commercial : In Confidence
C3	In Confidence
C4	Medical : In Confidence

7.2 C1 (Unclassified)

This is information that may circulate freely in the public domain and, therefore, does not require any special protection. This information might include:

- Published advertising material
- Public statements or announcements
- Published job vacancies

Information marked with this classification must still contain appropriate statements relating to copyright etc.

7.3 C2 (Internal Use Only/ Commercial: In Confidence)

This is information for which unauthorised disclosure, particularly outside the organisation, would be inappropriate and inconvenient. If this information were to be disclosed to a third party, it could provide a commercial advantage. This is routine business information, which the Auckland DHB simply wishes to keep private. This information might include:

- System design information not covered in higher classifications
- Employee contact details
- Organisational charts
- Minutes of department meetings
- Internal Auckland DHB memos or briefings

"**C2 Internal Use/ Commercial in Confidence**" must be marked or communicated with any material to which it applies.

7.4 C3 (In Confidence)

This is information for which unauthorised disclosure (even within Auckland DHB) could cause significant harm to the interests of the Auckland DHB by virtue of financial loss, loss of profitability or opportunity, embarrassment or loss of reputation. This information might include:

- System information for systems with an Information Classification of C3 or higher
- Patient information
- Negotiating positions
- Personnel information e.g. payroll information, contract information
- IS security testing & review information

"**C3 In Confidence**" must be marked or communicated with any material to which it applies.

7.5 C4 (Medical: In Confidence)

This is information for which unauthorised disclosure (even within Auckland DHB) could cause serious damage to the interests of the Auckland DHB by virtue of serious financial loss, severe loss of profitability or opportunity, grave embarrassment or loss of reputation, and some level of public statement by the MOH. This information might include:

- Patient identifiable data
- Patient Clinical or Medical information

"**C4 Medical: In Confidence**" must be marked or communicated with any material to which it applies.

(Reference: healthAlliance Security Functional Standards V6.2, p10-11)

8. Access controls

8.1 Access to patient information/clinical records

- Staff access to patient information in the clinical record is restricted to only those clinicians involved in the current active care and treatment of the patient, and to other authorised staff whereby access to specific information is required as part of their role.
- Staff as part of their role at Auckland DHB, are likely to have access to electronic systems containing a broad range of patient information. Staff must not misuse their access privileges to access the clinical record or view information about themselves, a family member, friend or any other Auckland DHB patient for which they are not directly involved in providing current active care and treatment.
- Regular audits are conducted to review access by all users of Auckland DHB clinical systems. All potential access breaches (i.e. inappropriate or unauthorised access transactions) are investigated as per the Board Policy - Discipline and Dismissal, and could result in disciplinary action up to and including termination of employment.

Further information regarding access to patient information/clinical records is contained in the Clinical Record Management Policy, including policy statements regarding the following:

- Access for clinical research/clinical trials
- Access for clinical audit
- Access for medical student examinations
- Patient access – release of information

8.2 Access to Information systems containing patient and other personal or business-related information

- Only authorised staff that have a justified and approved business need will be given access to restricted areas containing information systems or stored information.
- Each staff member (if/as appropriate to their role) will be issued with a personal logon for access to the Auckland DHB network and information systems containing patient and other personal or business-related information.
- There is a documented user registration and de-registration procedure for access to the Auckland DHB network and information systems to ensure that access is provided only to current, authorised staff.
- Line Managers must approve user access to the Auckland DHB network and information systems prior to an access request being processed by the IS Service Desk.
- Information system access privileges for all users are based on assigned roles and demonstrated need for access. Access privileges shall be modified or removed as appropriate when a member of staff changes their role or leaves Auckland DHB employment.

8.3 Use of Passwords

- Passwords are the primary security credentials used to identify, authenticate and authorise access to the DHB network and information systems.
- Passwords are automatically classified as C3 - In Confidence and must be protected appropriately.

- Staff are responsible for keeping all passwords confidential.
  - Passwords must never be disclosed to or shared with another person.
  - Logon/user names and passwords must not be sent by public, external email.
  - Staff must not record their passwords in any way that they could be accessed by another person.
  - Staff must not ask any other staff for their password.
  - Staff must not let anyone observe the entering of a password.
- Each staff member must log on to any information system using their own logon to avoid working under another staff member's logon.
- All staff will be held accountable for all computer/device activity and transactions made using their personal logon, whether or not they are present at the time.
- Staff must select passwords that conforms to the selection criteria below.

8.4 Selection criteria for passwords

- Have a minimum length of 8 characters.
- Have complexity enabled consisting of at least three of the four following character sets:
  - lowercase characters (a-z)
  - uppercase characters (A-Z)
  - digits (0-9)
  - special characters such as !@#$%^&*
- Do not base passwords on any of the following details:
  - family names
  - initials
  - car registration numbers
  - user name
  - more than two consecutive identical characters
  - obvious phrases or sequences such as '12345678'

The best type of password is one that is made up from a 'Passphrase' such as "WeLikeApples10!".

8.5 Suspected disclosure of password

If you suspect your password has become compromised you must change it immediately and report an incident, as noted in Section 11 of this Policy.

9. Information privacy and security

Staff must ensure that patient and other personal or business-related information, regardless of the format in which it is created, used or stored, is accurate, stored securely, protected from loss, damage, unauthorised access, alteration or corruption, and that confidential information is protected at all times. The safeguards outlined in this and associated policies are in place to ensure the security and privacy of patient and other personal or business-related information.

9.1 Storage and transport of clinical records

- Clinical record storage methods should ensure that access is restricted to authorised persons only at all times.
- Clinical records shall be stored in such a way so as to protect them from physical damage and/or electronic corruption.
- Clinical records must never be removed from Auckland DHB, e.g. to private rooms, the staff member's home, or other institutions.
- When transferring paper-based clinical records from one location to another, patient privacy must be maintained by ensuring that no patient identification details are visible during transfer.

- When transferring paper-based records between Auckland DHB campuses (e.g. from Auckland City Hospital to Rehab+) clinical records are to be transported in a secure file or locked case.
- Under no circumstance should clinical records be left in an unattended vehicle or in any unsecure location.
- Patient information from, or for, a clinical record must never be permanently stored:
  - on Auckland DHB owned or personal cell phones, computers, portable devices or removable storage media including, but not limited to, smart phones, laptop computers, tablets, personal digital assistants (PDAs), USB/flash drives and memory cards
  - in a personal or shared drive on the Network
  - in an unprotected location.

9.2 Use of cloud storage for patient and other personal or business-related information

In accordance with advice issued by the National Health IT Board (NHITB), no patient information is to be stored in a cloud that is based off-shore. The NHITB states that:

> *"Unless exemption is granted by the National Health IT Board, all personally identifiable health information and core operational data must be fully domiciled in New Zealand.*
>
> *The NHITB recognises that off-shore and/or cloud technology may offer a low-cost option for storing information but says this has to be considered alongside the requirements health and disability support service providers have under the Privacy Act 1993, Health Information Security Framework (HISF) and Health Information Privacy Code 1994 (the Code) to protect information they hold from loss, misuse and/or unauthorised access, use, disclosure or modification. Sending or storing health information overseas means that it would be controlled or accessed outside New Zealand's jurisdiction. Under the Code, a service provider is responsible for information they have in a cloud." (Disability Support Services e-newsletter, February 2013, p. 4.).*

Auckland DHB prohibits the use of cloud storage to store or transmit any ADHB C2, C3 or C4 classified information unless prior exemption from the NHITB has been granted.

9.3 Privacy and security controls – information systems and electronic devices

- Monitors, keyboards and workstations must be positioned in such a way that restricts access to or viewing of patient and other personal or business-related information to authorised staff only.
- Cell phones, portable devices and removable storage media that may contain patient and other personal or business-related information must be appropriately secured (i.e. locked away in filing cabinets or offices) when not in use, and should not be left unattended in meeting rooms or unlocked offices.
- All removable data storage devices must be encrypted and password protected.
- When a computer/device is switched on, it is essential that staff log out or 'lock' the screen before they leave the computer/device unattended.
- At the end of a session/shift, or when leaving Auckland DHB controlled premises staff must do a full shut down of the computer/device to ensure it is secured.

9.4 Privacy and security controls – sending patient and other personal or business-related information classified as C2, C3 or C4 via facsimile

- When sending patient and other personal or business-related information classified as C2, C3 or C4 to any recipient via facsimile (fax), a fax header sheet must be attached. The header sheet must state who the information is intended for and must also include the following standard, approved Confidentiality Statement and Disclaimer:

> *"Information contained in this message includes confidential patient or other personal or business-related information. If you are the intended recipient you are required to keep this information private. If you are not the intended recipient your use or retention of this information will breach the Privacy Act. If you have received this message in error please destroy it and notify the sender by telephone immediately."*

- Saved speed-dial numbers should be used for common fax recipients to prevent numbers being misdialled. These numbers should be tested periodically.
- When sending a fax to a new recipient, where practicable staff should verify the fax number before sending patient and other personal or business-related information classified as C2, C3 or C4.
- Fax machines should be located in a secured area where only staff who are authorised to use the machine to send and/or receive faxes can access it.

9.5 Privacy and security controls – sending patient and other personal or business-related information classified as C2, C3 or C4 via email

Use of email for sending patient and other personal or business-related information classified as C2, C3 or C4 to recipients outside the Northern Region DHB secure Network is not encouraged, as this is a non-secure means of transmission of information. However, it is recognised that from time to time it may be necessary to support timely exchange of information with recipients outside the Northern Region DHB secure Network (including patients) via the use of email. This communication mechanism may therefore be used by exception, and should not be adopted as standard practice.

Recipients outside the Northern Region DHB secure Network are identified via a pop up message that appears when the recipient's email address is entered into the 'To' field in the email system.

The following safeguards must be adhered to when transmitting patient and other personal or business-related information classified as C2, C3 or C4 in or attached to an email to recipients outside the Northern Region DHB secure Network.

- Ensure you have the correct email address for the intended recipient. Where practicable, verify the email address by sending an email first to confirm with the intended recipient that it is appropriate to use that email address.
- No patient or other personal or confidential business-related information (including information that identifies an individual patient) must be displayed in the subject line of an email.
- Send patient and other personal or business-related information classified as C2, C3 or C4 in an attachment (Word, Excel etc.) with encrypted password protection. The password should be sent to the intended recipient, preferably by phone or other non-email communication.
- Wherever possible, patient names should be excluded from email messages. Patients should be referred to by their NHI number only.
- Limit email content to the minimum amount of information necessary to meet the intended purpose.
- If communicating with a patient via email, ensure you have the patient's consent to do so and record this in the patient's clinical record. Consider whether a copy of the email communication should be sent to the Clinical Records Department for scanning into the 3M ChartView clinical record. This is a requirement if the email pertains to the care or treatment provided to the patient.

9.6 Privacy and security controls - use of answering machines/voicemail

- Avoid leaving messages about or for a patient on an answering machine/ voicemail unless you have specific consent to do so.
- When urgent contact is to be made the only information that is acceptable to leave is a telephone number and the name of the person to phone back.
- Auckland DHB voicemail must always be password protected so it can only be accessed by authorised staff.

- The password for voicemail should not be the same as the owner's telephone extension number.

10. Security of IT equipment

In order to minimise loss or damage and to avoid interruption to Auckland DHB business activity, all IT equipment, including hardware (personal computers and portable devices, such as laptops and cell phones), computer software, printers and facsimile machines and information storage areas must be physically protected from security threats and unauthorised access.

- Where possible IT equipment should be positioned away from public accessible areas, preferably in secure locations.
- At the end of each day/work shift, all portable devices and confidential hard copy information must be appropriately secured (i.e. locked away in filing cabinets, offices etc. as appropriate).
- All printers and fax machines should be cleared of papers as soon as they are printed.
- Information held electronically must be stored in the appropriate drive on the Auckland DHB network. Information should not be saved to the Desktop, C Drive or 'My Documents'.

10.1 Disposal of IT equipment and personal or other business-related information

- The IS Service Desk must be informed of any IT equipment that needs to be disposed of. Under no circumstances must staff pass on or dispose of IT equipment themselves.
- Staff should refer to the Corporate Information Management Policy and DHB General Disposal Authority for guidance on the retention periods that apply to personal or other business-related information.
- On a day-to-day basis confidential waste (i.e. information classified as C2, C3 or C4) must either be shredded or disposed of in the designated confidential waste bins.
- The secure disposal of information classified as C2, C3 or C4 that has reached the end of the required retention period as per the DHB General Disposal Authority must be managed via secure destruction.

10.2 Return of equipment and removal of access rights

- All IT equipment, including hardware (personal computers and portable devices, such as laptops and cell phones), computer software, working materials, confidential information, and other property issued to staff must be returned upon termination of their employment contract.
- It is the responsibility of the Line Manager to inform the IS Service Desk when a staff member has left Auckland DHB so that network and information system access rights can be removed.

10.3 Remote access

All computers which have remote connections with the Auckland DHB network and information systems must have virus-scanning software installed with the latest security patches and updates applied.

10.4 Electronic Mail and Internet Use

Please refer to the Electronic Mail and Internet Usage Policies.

11. Privacy and security incident management and response

Privacy and security incident management procedures are in place to ensure a quick, effective, and orderly response when privacy and security incidents occur, to enable monitoring and learning from such incidents, to mitigate the risk of and avoid recurrence.

Privacy and security incidents include but are not limited to:

- Loss or theft of hard copy patient and other personal or business-related information or equipment such as laptops or USB/flash drives on which information is stored.
- Malicious software or virus attack on the network, IT equipment or information systems.

- Inappropriate access controls allowing unauthorised use of patient and other personal or business-related information.
- Attempts to gain unauthorised access to the network, IT equipment or information systems.
- Denial of service - an attack that prevents or impairs the authorised use of the network, IT equipment or information systems.

Staff are required to report any observed or suspected incidents to their Line Manager.

All incidents must be reported by the Line Manager to the IS Service Desk and logged via Risk Monitor Pro, including:

- Full contact details of the user (name, contact number and email address)
- IT equipment type, model and serial number
- A short summary of the incident.

12. Software installation

To comply with the law on the use of licensed products and minimise the risk of computer viruses, ADHB only permits the installation of approved software on Auckland DHB owned or managed devices. Software which does not have a legitimate licence for its use, or may be used for malicious purposes (i.e. hacking tools, etc.) must never /be installed or used on an Auckland DHB owned or managed device.

12.1 Installing software

- If a user requires access to new software they must submit a request to the IS Service Desk.
- Software must not be downloaded and installed by users.
- If the requested software is not in the approved software catalogue the IS Service Desk will acquire the software.
- The IS Service Desk will arrange for new software to be installed on specified device/s so that care can be taken to mitigate the risk of viruses.

12.2 Antivirus software

All devices (desktop, laptops etc.), whether connected to the network or stand-alone, must have the healthAlliance approved antivirus and malware scanning /detection software installed and active at all times.

13. Modems or network devices on workstations connected to internal networks

Computer users are prohibited from connecting modems or any network device to workstations which are simultaneously connected to a local area network (LAN) or another internal communication network unless approval has been obtained from healthAlliance.

14. Personal use

IT equipment and information systems are provided for the conduct of official Auckland DHB business. Limited personal use may be permitted at the discretion of the Line Manager, provided such use is not excessive or inappropriate and does not result in expense or risk to ADHB or otherwise violate this policy.

15. Prohibited use

- Using or attempting to use another individual's user name or password.
- Engaging in any activity that might be harmful to IT equipment or information systems, or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files, or making unauthorised modifications to or sharing of Auckland DHB information.

- Using Auckland DHB information systems for commercial purposes or personal gain.
- Attempting to gain access to Auckland DHB information systems or patient and other personal or business-related information to which the staff member has no legitimate access rights.
- Engaging in any other activity that does not comply with this or related policies, or applicable legislation.

16. Legislation

- Copyright Act 1994
- DHB General Disposal Authority (DA262)
- Health Information Privacy Code 1994
- Official Information Act 1982
- Privacy Act 1993
- Public Records Act 2005

17. Associated Auckland DHB documents

- Cellphones
- Clinical Record Management
- Corporate Information Management
- Electronic Mail
- Internet Usage
- Patient Registration

Clinical Forms

- Patient Registration Form (CR0001)

18. Corrections and amendments

The next scheduled review of this document is as per the document classification table (page 1). However, if the reader notices any errors or believes that the document should be reviewed *before* the scheduled date, they should contact the owner or the Document Controller without delay.

PROTECTED DISCLOSURES

Overview

Content

This document covers the following topics relating to Protected Disclosures.

Purpose

The purpose of this policy is to define the process by which employees of Auckland District Health Board (ADHB) may raise concerns about serious wrongdoing within ADHB. The policy is based on the Protected Disclosures act 2000, commonly known as the 'Whistleblowers Act'.

Scope

This policy applies to all employees.

Associated Documents

The table below indicates other documents associated with this policy.

Type	Document Titles
Board Policies	• Complaints Management • Conduct Standards • Conflict of Interest • Fraud Policy • Sponsorship, Donations, Gifts & Corporate Hospitality • Health Practitioner's & Registered Social Worker Competence & Reporting Obligations • Incident Management Policy
Legislation	Protected Disclosures Act 2000

PROTECTED DISCLOSURES

Definitions

Definitions The following terms are used within this document.

Term	Definition
Appropriate Authority	An appropriate authority includes: • The Commissioner of Police • The Controller and Auditor-General • The Director of the Serious Fraud Office • The Inspector-General of Intelligence and Security • An Ombudsman • The Parliamentary Commissioner for the Environment • The Police Complaints Authority • The Solicitor-General • The State Services Commissioner • The Health and Disability Commissioner • The head of any public sector organisation • A professional regulatory body which has disciplinary powers An appropriate authority does not include: • A Minister of the Crown or • A Member of Parliament
Employee	The term 'employee' includes: • current and former employees, • individuals seconded to ADHB, • independent contractors engaged by ADHB to work for it, • anyone concerned in the management of Auckland District Health Board • a person who works for the organization as a volunteer without reward or expectation of reward for that work.
Protected Disclosure	A disclosure made by an employee about serious wrongdoing in or by Auckland District Health Board which the employee believes on reasonable grounds to be true or likely to be true and which the employee wishes to disclose in confidence for the purpose of investigation and to attract the protection of the Protected Disclosures Act 2000.

Continued on next page

PROTECTED DISCLOSURES

Definitions, Continued

Term	Definition
Serious Wrongdoing	Serious wrong doing includes: • An unlawful, corrupt, or irregular use of public funds or resources • An act or omission or course of conduct which constitutes a serious risk to public health or safety or the environment • An act or omission or course of conduct that constitutes a serious risk to the maintenance of the law • An act, omission or course of conduct which constitutes an offence • An act, omission or course of conduct by a public official which is oppressive, improperly discriminatory or grossly negligent, or that constitutes gross mismanagement Serious wrong doing would not ordinarily include matters of clinical practice. Incidents or competence/safety concerns should be reported on Risk MonitorPro (incident reporting software) and may require notification under the Health Practitioner Competence (Obligations) policy. They can also be appropriately addressed by a patient complaint or ACC claim for compensation for treatment injury. Serious wrongdoing is also very unlikely to include matters relating to an individual's employment by Auckland District Health Board.

PROTECTED DISCLOSURES

Process for Making a Protected Disclosure

Process

This table describes the process for making a Protected Disclosure.

Step	Action
1	An employee who wishes to make a protected disclosure must make it to the Group Manager – Quality.
2	On receipt of a protected disclosure the Group Manager – Quality records receipt of the protected disclosure. Either: • Investigate the matter him/herself or • Refer the matter for investigation by: – The Internal Auditor – ADHB Legal Department • Notify: – The Chief Executive or other senior manager as appropriate – The General Manager of the service in which the wrongdoing is alleged to have occurred.
3	Allegations of serious wrongdoing may be reported to Auckland District Health Board's insurers by the ADHB Legal Department.
4	The investigation will occur in liaison with the General Manager of the Service and other appropriate staff and will be undertaken in accordance with the Complaints Management policy in so far as it is applicable. The principles of natural justice will be adhered to in conducting the investigation. These principles require any person alleged to be involved in serious wrongdoing to be informed of the complaint and given an opportunity to respond to it.
5	The results of the investigation will be reported back to: • The Chief Executive or other senior manager as appropriate • The General Manager of the service in which the wrongdoing is alleged to have occurred • The ADHB Legal Department

Continued on next page

Process for Making a Protected Disclosure, Continued

Step	Action
6	The Group Manager – Quality will inform the employee (if the employee has agreed to be identified) of the results of the investigation within a reasonable time of receiving the protected disclosure.
7	An employee may refer the matter directly to the Chief Executive if the employee believes, on reasonable grounds that: • The Group Manager – Quality may be involved in the serious wrongdoing; or • It is inappropriate to make the disclosure to the Group Manager – Quality due to their relationship or association with the person who may be involved in the serious wrong doing.
8	An employee may refer the matter directly to an appropriate authority if the employee believes that: • The Chief Executive may be involved in the serious wrongdoing; or • The urgency of the matter or some other exceptional circumstance justifies it • ADHB does not take action or recommend action on the matter within 20 working days.
9	An employee may make a protected disclosure to a Minister of the Crown or to an Ombudsman if the employee: • Has already made substantially the same disclosure to the Group Manager – Quality or to an appropriate authority; and • Believes on reasonable grounds that ADHB has either decided not to investigate or has not made progress with the investigation within a reasonable time or has investigated but not taken or recommended any action in respect of the matter; and • Continues to believe on reasonable grounds that the information is true or likely to be true.

PROTECTED DISCLOSURES

Protection from Retaliatory Action & Liability

Protection

If an employee makes a protected disclosure in accordance with this policy, they will have the following protections:

- If the person is an 'employee' within the meaning of the Employment Relations Act 2000 (i.e. Not an independent contractor), then in the unlikely event of retaliatory action by ADHB against the employee for making the disclosure (for example, dismissal from employment), the employee may have grounds for a personal grievance action against ADHB.
- The employee will be protected from any civil or criminal proceeding or any disciplinary proceeding by reason of having made the disclosure. The employee may not be protected from civil or criminal proceeding or disciplinary proceedings if they were personally involved in the serious wrongdoing they disclose. In these circumstances, the employee's co-operation in reporting the wrongdoing will be taken into account in decisions on any action that may be taken against them.

Confidentiality

Any person to whom a protected disclosure is made must use best endeavours not to disclose the identity of the person making the protected disclosure unless the person making the disclosure consents in writing to his or her identification; or the person to whom the disclosure is made reasonably believes that disclosure is essential to effective investigation, or to prevent serious risk to public health or safety or to the environment, or to ensure the principles of natural justice are adhered to. If disclosure of the person's identity is necessary in order to investigate or prevent serious risk or ensure natural justice is complied with, the person will be advised of this.

Note: Confidentiality applies only to disclosures made under this policy. Confidentiality cannot be guaranteed where the employee's identity has been disclosed via other processes, for example where the employee has identified concerns to colleagues.