Integrated Private General Practice series

Information Sheet

09 Risk, Emergency and Business Continuity Planning

July 2024

This information sheet describes the key requirements of the RACGP standards for General Practice for managing business and clinical risks. Emergency (or disaster) management and business continuity planning are specific risk management actions that prepare and guide the practice through unexpected events that may otherwise significantly interrupt service delivery.

1. Overview

Risk management is an integral part of an organisation's business planning and operational management processes. It explores the challenges and opportunities an organisation faces in achieving its objectives and informs action to mitigate the likelihood of unexpected or unintended events, such as a natural disaster or significant IT failure.

Good risk management improves the business planning process, reduces unwanted surprises, improves resource allocation, strengthens performance, adds to staff communication and culture, improves accountability and supports good decision making.

The level and formality of risk management undertaken in the practice will vary based on its size and complexity. The process will involve identifying and assessing risk threats, prioritising actions to reduce a risk threat (or consequence), monitoring progress, communicating risks actions amongst staff and providing staff training. Risk management requires documented planning and regular consideration by the management team.

Each HHS maintains its own risk, emergency and business continuity policies and procedures that are integrated into its business and clinical service planning processes. The practice will be able to adopt some of these resources to meet the requirements of the RACGP Standard for General Practice.

2. Risk management

Risk management is a systematic process undertaken to identify risks within a practice and develop procedures to mitigate or eliminate those potential risks.

ISO 31000 Risk Management – Principles and Guidelines[1] defines risk as 'the effect of uncertainty on business objectives'. This includes both the risk of something bad happening, but also the risk of missing an opportunity to improve business outcomes.

[1] www.iso.org/publication/PUB100426.html

RACGP Core standard C3.1>C requires a practice to have a business risk management system that identifies, monitors and mitigates risks in the practice. There must be a documented risk management process and procedures to mitigate risks, including a risk register (or a log of risks in a small practice) and records of meetings where risks and actions to manage them are discussed.

Core standard C3.2>C requires the practice to nominate a staff member with appropriate skills to assume responsibility for leading risk management systems and processes. This can be documented in their role description.

Quality Improvement standard QI3.1>B requires practices to demonstrate they are making improvements to clinical risk management in order to prevent near misses and adverse events in clinical care.

Effective risk management is important to the practice because it supports safe and quality care, protects the reputation of the practice and its clinicians, avoids regulatory intervention, reduces financial risks and helps sustain ongoing services.

Common areas of risk which general practices should consider include:

- Clinical governance - patient safety, service quality, medical malpractice
- Staff workplace health and safety
- Workforce and succession
- Practice financial viability and sustainability
- Computer systems and security
- Confidentiality and privacy
- Medicare compliance / fraud
- Emergency / business continuity preparedness

Organisations use a number of tools to support their risk management system:

- A risk register to log identified risk threats, their assessment, planned risk actions and the responsibility for treatment actions (a sample register is at **Table 1**)
- A description of risk consequences to guide to determine the impact level of a risk threat (see **Table 2**)
- A description of likelihood ratings to assist in evaluating risk priorities (see **Table 3**)
- A risk assessment to score risks to prioritise action and review (see **Table 4**)
- A risk response planner to guide the urgency and level of review a threat may require for levels of risk ratings (see **Table 5**)

It may be appropriate to consult with experts if risks are not well understood (for example, consulting an IT security or cyber expert).

The practice should regularly review its risk exposures, progress in implementing risk action and the ongoing effectiveness of risk controls. These should be reported to the management team or risk committee on a regular (monthly) basis and the discussion recorded. Emphasis should always be placed on the highest risk threats.

3. Emergency and disaster planning

Emergency and crisis events may arise from natural disasters or other factors, may occur without notice and have an uncertain impact on the operation of the practice. Crisis or disaster events the practice may encounter include:

- Destruction of, or loss of access to, the practice building.
- Compromised practice systems or communications (possibly through network outages, critical system errors or cyber-attack).
- Unplanned workforce absences / departures.
- Disruptions to services (power, water).
- Mass casualty incidents and post natural disaster care.
- Pandemic or widespread illness in the local area.
- Community confidence in the practice and adverse media.

RACGP standard C3.3>A requires a practice to maintain an emergency response plan for unexpected events. This must be documented, staff trained, and be periodically tested/rehearsed. A team member should be allocated responsibility for maintaining the emergency plan.

The size and complexity of an emergency and disaster management plan can be tailored to suit the size and nature of the practice's operations. Its content should be informative and clear, using language that is easily understood by all practice staff. The plan will typically draw on the business impact assessments used in continuity/contingency planning (see next section).

The emergency plan will usually include:

- a clear statement of purpose;
- the roles and responsibilities for practice staff in managing the emergency (for example, evacuating the building, shutting down the computer, establishing the incident response team);
- an assessment of potentially disruptive events;
- the outcomes of business impact assessments (see next section);
- how the plan is activated in an emergency to trigger contingency plans;
- who will be involved in emergency management and who will be contacted (for information and for assistance);
- staff training requirements, including refresher training, and rehearsals;

- a list of emergency contacts;
- a list of critical records to be taken (where possible); and
- where a list of vulnerable persons and their needs is maintained.

The HHS will likely maintain a template for emergency and disaster planning, though templates can be sourced online.

4. Business continuity planning

Business continuity planning is an important part of risk management that focusses on how an organisation continues to carry on its activities in the event of an emergency, a natural disaster, or some other major disruption to normal operations.

A good business continuity process (sometimes referred to as business contingency planning) will consider both likely and unlikely events, assesses the disruptions these present, and set out the actions that the practice staff can implement if, or when, these situations arise.

It is never a good idea to attempt to plan for practice continuity in the middle of a crisis or natural disaster.

A business impact assessment should:

- Describe the critical event
- Consider the business impact (the effects on your activities)
- Develop a list of immediate actions to be taken
- Develop a list of potential medium term contingency actions
- Identify business recovery actions (when returning to business as usual)
- Document periodic review arrangements (including refresher training)

Exhibit 1 provides a sample template to assist in documenting critical incidents and continuity responses.

Importantly, some contingency actions may require the practice to seek the assistance of another organisation, such as arranging temporary space to relocate the practice during a flood and whilst repairs are carried out. These arrangements need to be documented and be periodically re-confirmed.

Exhibit 1: Assessment of a critical incident

Critical Incident:	**1. Loss of premises** *Inability to deliver services from the practice location*
Description	• Premises are damaged and unusable due to natural disaster or fire • Access to premises is temporarily impaired due to flood or road closure • Services are temporarily impeded due to loss of utilities, gas leak, bomb threat
Immediate / short term actions	• Make safe – evacuate premises, secure and relocate valuable items (time permitting) • Divert patients to hospital ED - display notices, email/SMS/Facebook messages, ABC radio
Medium term contingency plans	• Establish alternate clinic space in hospital outpatients • Use laptops and stand-alone printer for medical software • Arrange diversion of practice phone to hospital • Assess list of vulnerable patients for home visits/telephone calls
Recovery processing:	• Service and re-commission equipment • Re-stock supplies • Review missed appointments for patients with health care plans
Annual review	• Re-confirm contingency plan with the local hospital • Confirm the location in hospital for a back-up clinic remains available with access to suitable equipment • Test laptop and printer configuration • Test identification of vulnerable patients list

5. Information management and security

The RACGP highlights the widespread adoption of, and vital need for, clinical systems and electronic management of information in the delivery of safe and high-quality healthcare.

The disruption caused by downtime of the IT system can be challenging without the ability to readily access patient records, record current treatment, provision referrals or diagnostic tests or even generate billing for Medicare.

Moreover, inadvertent or intentional damage to the practice systems exposes the practice and patients to privacy breaches and/or ransomware attacks.

Prevention is always better than recovery.

RACGP standard C6.4>D requires practices to maintain business continuity and information security plans which should include the process by which information will be backed-up, a schedule for testing back-ups, secure offsite storage and written agreements with IT providers.

The RACGP has also developed further guidance on information security in general practice[2] to support best practice in managing computer and information assets. Secure computer and information management systems are essential for the necessary protection of business and sensitive, personal clinical information. Computer and information security is not optional, it is essential. It should be considered a fixed cost of doing business that requires financial and human resources being allocated to ensure the protection of information assets.

[2] RACGP information security in general practice www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice (accessed 9 June 2024)

Table 1: Risk Register (basic)

<Name of Practice> Risk Register									
Risk ID	Risk description	Existing controls	Current risk score	Additional risk actions	Responsible person	Due date	Planned risk score	Status	Comments
1	2	3	4	5	6	7	8	9	10

Column 1. If a risk is also included on the HHS Riskman system, include the Riskman ID as well

Column 2. A risk should briefly describe the problem affecting the practice, what is understood as the cause, and its effect(s) on patient outcomes.

Column 3. Controls include plans, policies, procedures, IT passwords, building keys, staff training, checking/reconciliations and audits amongst other things. They must be working (not just a documented procedure) and be effective.

Column 4. Assign the current risk score based on your assessment of the likelihood and impact of the risk event <u>if you did nothing further</u>. Is this acceptable?

Column 5. Where a risk score is not acceptable, list out the additional controls to be developed. These should meaningfully reduce the risk threat or consequence. This might include a change to a procedure, more training, additional reviews/monitoring or rehearsing plans.

Column 6. The responsible person should be the staff member who has the authority to complete the action.

Column 7. Due dates should reflect the urgency of addressing risks (the higher the risk, the shorter the timeframe) and must be regularly monitored. Do not amend a due date once it has been accepted, as this will highlight delays.

Column 8. This risk score is the remaining acceptable risk threat once all planned risk actions are complete. It is possible that a threat cannot be further reduced and may require continuous review by management.

Column 9: Update the status of risk actions (Not commenced, In-progress, Completed, Delayed) prior to each management meeting where risk is discussed.

Column 10. Keep all previous monthly comments until risk actions have been completed to enable management to review the entire ‘story’.

Table 2: Risk consequences

	Negligible	**Minor**	**Medium**	**Major**	**Extreme**
Continuity of practice operations	Limited disruption causes manageable delays to non-critical functions	Disruptions within maximum acceptable outages (MAO), workarounds in place and acceptable	Disruption in one area exceed MAO, workarounds in place, rapid recovery expected.	Widespread disruptions exceeding MAO, prolonged recovery and backlog processing expected	Widespread disruptions significantly exceeding MAO, no workarounds, prolonged recovery and back-up processing expected
Clinical safety and quality	No harm, near miss.	Minimal harm, first aid treatment only	Temporary harm	Likely permanent harm	Death or permanent disability
Financial	Adverse variation <0.5% budget	Adverse variation 0.5% to 2% of budget	Adverse variation 2% to 5% of budget	Adverse variation 5% to 10% of budget	Adverse variation > 10% of budget
Legal and regulatory	No long term consequences, claim or prosecution unlikely	No long term consequences anticipated, claim or litigation possible	Long term consequences, potential regulatory investigation, possible claim or litigation.	Long term consequences, investigation likely, potential serious claim or prosecution. Possible criminal conviction	Long term consequences, investigation, serious claim or litigation. Possible criminal conviction carrying penalty of imprisonment
Reputation	Isolated complaints from individuals that can be managed locally.	Complaints and/or negative local community and/or media attention.	Negative regional media coverage. And community concerns. May be noted in state-wide media.	Sustained negative state-wide media coverage. Loss of community confidence. May be noted in national media.	Sustained negative national media coverage. May be noted in international media.
Workplace health and safety	No injury. First aid treatment only. No time lost.	Medical treatment injury. A full shift/workday has not been lost.	Lost time injury or serious injury or illness without permanent impairment.	Serious injury or illness with permanent impairment.	Reportable fatality (as defined by s35 Work Health & Safety Act (QLD) 2011).

Adapted from the Department of Health risk management toolkit[3]

[3] https://qheps.health.qld.gov.au/csd/business/risk-and-audit-services/risk-services/toolkit

Table 3: Risk Likelihood

Likelihood	Description
Almost certain	Current controls will almost certainly not prevent the risk from occurring
Likely	Current controls are not likely to prevent the risk from occurring
Possible	Current controls will possibly prevent the risk from occurring
Unlikely	Current controls make the risk unlikely to occur
Rare	Current controls prevent the risk from occurring except on rare occasions

The risk of billing an incorrect item in a small, busy practice with an inexperienced practice team may be considered Possible, whereas systematically over-billing Medicare may be considered Rare.

Likelihood is usually subjective, with historical incidences (errors per month/year) guiding assessment. Some organisations use percentage thresholds (for example, Possible has a 50% chance of the risk event occurring).

Table 4: Risk assessment

		Consequence				
		Negligible	**Minor**	**Medium**	**Major**	**Extreme**
Likelihood	**Almost certain**	Medium (7)	Medium (11)	High (17)	Very High (23)	Very High (25)
	Likely	Medium (6)	Medium (10)	High (16)	High (20)	Very High (24)
	Possible	Low (3)	Medium (9)	High (15)	High (18)	High (22)
	Unlikely	Low (2)	Medium (8)	Medium (12)	Medium (14)	High (21)
	Rare	Low (1)	Low (4)	Low (5)	Medium (13)	High (19)

Table 5: Responding to risks

Risk score	Response to risk
Very High **(23 to 25)**	Immediately - commence treatment action within one month, complete within 3 months Include on HHS risk register (Riskman) Monthly review by the risk owner until effectively controlled Monthly updates to the management team and governing committee
High **(15 to 22)**	Commence treatment planning within one month, actions completed within 6 months Consider inclusion on HHS risk register (Riskman) Monthly review by the risk owner until effectively controlled Monthly updates to the management team and governing committee (as needed)
Medium **(6 to 14)**	Within 3 months evaluate risk actions based on cost/benefit and resource prioritisation Quarterly review by risk owner Updates to management committee as needed
Low **(1 to 5)**	Maintain effectiveness of existing controls and manage by routine procedures. Periodic monitoring and escalation if circumstances change As needed review by risk owner