Ombudsman
Fairness for all

Guide

Making official information requests

A guide for requesters

If you are seeking information from a Minister, or central or local government agency, you may be able to ask for it under either the Official Information Act 1982 (OIA) or the Local Government Official Information and Meetings Act 1987 (LGOIMA).

This guide sets out what information you can ask for, how to go about it and what the agency is required to do in responding to your information request.

Contents

What are the OIA and LGOIMA?

The OIA and LGOIMA are laws in New Zealand that allow people to ask for official information held by Ministers and central and local government agencies (agencies). These laws set out how agencies should handle requests for information and give a right to anyone not happy with the result to complain to the Ombudsman.

The OIA applies to information requests made to Ministers and central government agencies. The LGOIMA applies to local government information requests, and also sets out rights of access by the public to local government meetings. For information about how agencies process an information request, see The OIA for Ministers and agencies and The LGOIMA for local government agencies.

Principle of availability

The **starting point** is that, unless there is good reason for withholding information, it must be made available on request.[1] This is called *'the principle of availability'*.

Purposes of the Acts

The key purposes of the OIA and LGOIMA are to:[2]

- increase progressively the availability of official information to:
  - enable members of the public to participate in decision making more effectively; and
  - promote the accountability of agencies; and
- protect official information where this is necessary in the public interest or to protect personal privacy.

The key purposes of the OIA and LGOIMA reflect competing interests between making information available and protecting it where necessary. In line with these competing interests, agencies will need to balance:

- considerations which favour **releasing** information; and
- considerations which favour **refusing** requests for information.[3]

1 See s 5 OIA; s 5 LGOIMA.

2 See s 4 OIA; s 4 LGOIMA.

3 See ss 6, 7, 9 and 18 OIA; ss 6, 7 and 17 LGOIMA.

Who can request official information?

To be eligible to request official information under the OIA, you must be:[4]

- a New Zealand citizen or permanent resident;
- a person in New Zealand; or
- a corporate entity (that is, a company or an incorporated society) which is either incorporated in New Zealand or has a place of business here.

An agency is entitled to ask reasonable questions to check whether you are an eligible requester. While this may be clear with requests made by post (because of the post mark and/or return address), it may not be clear with requests made online. For more information see our guide to Requests made online.

There are no similar eligibility restrictions in LGOIMA.[5]

What if I am not entitled to make an OIA request?

Even if you are not entitled to make an information request under the OIA (for example, if you are overseas and not a New Zealand citizen or resident), you can still ask an agency for information. While the agency is not **required** to respond in terms of the OIA, it should still deal with your request in a reasonable manner.

Who can I request official information from?

The types of agencies that come under the **OIA** include:

- government Ministers in their **official** capacity;
- central government departments and organisations;
- the Police;
- crown entities;
- some state owned enterprises;
- district health boards;
- universities, polytechnics, colleges of education, wananga and other tertiary education institutions (but not private training establishments); and
- boards of trustees of state schools.[6]

[4] See s 12(1) OIA.

[5] See s 10(1) LGOIMA.

Agencies not covered by the OIA include:

- Parliament and its agencies (the Parliamentary Counsel Office and the Parliamentary Service);
- courts and tribunals;
- the Ombudsman; and
- the Independent Police Conduct Authority.

The types of agencies that come under the **LGOIMA** include:

- city, district and regional councils;
- council-controlled organisations;[7]
- local and community boards;
- licensing trusts; and
- airport authorities.

The agencies that come under the OIA and LGOIMA that you can request information from are listed in Schedule 1 of the Ombudsmen Act 1975, Schedule 1 of the OIA and Schedule 1 of the LGOIMA.

A list of the agencies subject to the OIA can also be found in the *Directory of Official Information*, which is published by the Ministry of Justice every two years. The directory is available on the Ministry's website (www.justice.govt.nz).

If you are unsure whether an agency is subject to the OIA or LGOIMA, please ring us on 0800 802 602.

6 State schools include integrated schools, designated character schools, correspondence schools, and kura kaupapa Māori, but do not include private schools or charter schools.

7 See s 74 Local Government Act 2002.

What is official information?

Official information means **any information held** by an agency subject to the OIA or LGOIMA.[8]

Official information is not just documents or papers. It includes information held in **any format**, such as:

- written documents, reports, memos, letters, notes, emails and draft documents;
- non-written documentary information, such as material stored on or generated by computers and databases, video and tape recordings, maps and photographs; and
- information which is known to an agency but which has not yet been recorded in writing or otherwise.

Is the information *'held'* by the agency?

It does not matter where the information first came from, as long as it is **held** by the agency. For example, the information could have been created by a third party and sent to the agency, or it could be in the memory of an employee of the agency.

However, an agency is not obliged to **form an opinion** or **create information** to answer an official information request.

There is a difference between:

- questions which can be answered by providing information already known to and held by the agency (official information); and
- questions which require the agency to form an opinion or provide an explanation and so create new information to answer the request (not official information).

Information held by employees

Information held by an officer, employee or member of an agency in their official capacity is considered to be held by the agency itself.[9]

Information held by independent contractors

Agencies sometimes have individuals or companies do work for them under contract.

Information which an independent contractor holds in their capacity as a contractor to the agency is considered to be held by that agency.[10]

---

8 There are some exceptions; see s 2 of the OIA and What is not official information?.

9 See s 2(4) OIA; s 2(3) LGOIMA.

10 See s 2(5) OIA; s 2(6) LGOIMA.

Information held by unincorporated bodies set up by an agency

Under the OIA, if an unincorporated body is established under legislation or by an agency, in order to assist, advise or perform functions connected with any agency, the information held by the unincorporated body is deemed to be held by the agency that established it.[11]

For example, if a government department set up a board or committee to assist it on a particular issue, and that entity was not itself subject to the OIA, the information held by the board or committee would nevertheless be able to be requested under the OIA, as the information would be deemed to be held by the department.

Special categories of official information

Certain rules apply to three particular categories of information that you may be entitled to request under the OIA and LGOIMA. These are:

- internal rules or guidelines for decision making;
- statements of reasons for decisions; and
- personal information requests by corporate entities.

Internal rules or guidelines for decision making

The OIA and LGOIMA provide you with a **right** of access, on request, to any document which contains an agency's policies, principles, rules or guidelines for making decisions about people.[12]

The ability to refuse such a request is very limited.

Requests for statements of reasons

Under the OIA and LGOIMA, you also have a **right** to request a written statement of reasons for a decision or recommendation made about you by an agency.[13]

Requests for statements of reasons are often made by people who are concerned about a decision or recommendation that affects them personally. There are only limited grounds for withholding information from a statement of reasons.

Any request for a statement of reasons must be made within a *'reasonable time'* of the decision or recommendation.

---

[11] See s 2(2)–(3) OIA.

[12] See s 22 OIA; s 21 LGOIMA.

[13] See s 23 OIA; s 22 LGOIMA.

A statement of reasons should be full and comprehensive in explaining the decision making process and must include the following elements:

- the findings on material issues of fact;
- a reference to the information on which the findings were based; and
- the reasons for the decision or recommendation.

Personal information requests by corporate entities

Under Part 4 of the OIA and LGOIMA a corporate entity (ie a company or incorporated society) can request the information an agency holds about it.[14] Under the OIA this right can only be exercised by corporate entities that are incorporated in New Zealand or have a place of business here.[15]

The requirements for an agency to process such requests are more or less the same as for any other request for official information. However, as the corporate entity has a specific **right** to access any information about itself that can be readily retrieved, the reasons for refusing such requests are more limited.

What is not official information?

Official information does not include:[16]

- information held by a Minister:
  - in their private capacity;
  - in their capacity as an MP (electorate information); or
  - in their capacity as a member of a political party (caucus information).
- library or museum material for reference or exhibition purposes;
- information held by an agency solely as an agent, or for the sole purpose of safe custody, on behalf of a person who is not subject to the official information legislation;
- information held by the Public Trustee or Maori Trustee in their capacity as a trustee;
- evidence or submissions to a Royal Commission or a commission of inquiry;
- certain information related to inquiries established under the Inquiries Act 2013;

[14] See s 24 OIA and s 23 LGOIMA.

[15] See s 24(2) OIA.

[16] See s 2 OIA; s 2 LGOIMA.

- any correspondence or communication between any agency and the Ombudsman or the Privacy Commissioner, in relation to their investigations;
- victim impact statements; and
- evidence, submissions or information given or made to the Judicial Conduct Commissioner, a Judicial Conduct Panel, or the Judicial Complaints Lay Observer.

Personal information about yourself

If you are an individual, you can ask for any personal information an agency holds about you under the Privacy Act.[17] The OIA and LGOIMA do not apply to such requests.

Deciding whether information is covered by the Privacy Act or the OIA/LGOIMA can sometimes be difficult. This is primarily because the same document can contain information about more than one person.

Whether the Privacy Act or the OIA/LGOIMA applies will depend on who is asking for the information and who it is about. If the information is about the person requesting it, then it will be covered by the Privacy Act. If the information is about someone else, then the OIA or LGOIMA will apply.

A good example is where a person makes a request for a file that contains information about them and other people. Generally:

- information solely about the person requesting it should be considered under the Privacy Act;
- information about other people should be considered under the OIA or LGOIMA.

If you are seeking information on behalf of someone else with their informed consent, then you will generally be considered to be acting as that person's 'agent', and this will be dealt with as a request for personal information under the Privacy Act.

Having determined which Act applies, the agency must make a decision on your request in accordance with the particular requirements of that Act.

Enquiries about the application of the Privacy Act should be made to the Privacy Commissioner, whose contact details are:

Ph: 0800 803 909
Email: enquiries@privacy.org.nz
Website: www.privacy.org.nz
Post: PO Box 10 094
The Terrace

[17] See Principle 6 and Part 5 of the Privacy Act. See also s 12(1A) OIA and s 10(1A) LGOIMA. As discussed above, corporate entities can seek their personal information under Part 4 of the OIA or LGOIMA.

Wellington 6143

Making a request

Making a request is easy. Simply contact the relevant agency and ask for the information you are seeking.

What should a request for official information look like?

You do not need to use legal language when requesting official information.

A request does not need to be in writing—you can make requests in person or over the telephone.

You do not have to specifically state that your request is being made under the OIA or LGOIMA.

However, it may be helpful to make your request in writing and for you to be very clear that you are making a request for official information under the OIA or LGOIMA—it helps the person receiving the request to identify it quickly and make sure it goes to the right person within the agency to be actioned.

If you do make an oral request, it may be helpful for you to make a note of what you requested, when you made your request, and who you spoke to at the agency. This may be useful for future reference.

If an agency considers that your oral request needs to be clarified in writing, it is entitled to ask you to do so.[18] If you are unable or unwilling to do so, the agency is required to make a written record of its understanding of your request and to provide you with a copy of that written record.[19] Your request will not be 'received' by the agency until you have confirmed that the agency's understanding of your oral request is correct. This means that the maximum time limit for responding to your request will not start counting until you have provided your confirmation.

There is also no requirement for you to give the reasons why you want the information. However, it can help an agency to better identify the information you are seeking, or to assess any public interest considerations favouring release of that information. An agency can ask for your reasons, but it cannot insist that they be supplied.

See our template letter for making an official information request.

[18] See s 12(4) OIA; s 10(4) LGOIMA.

[19] See s 12(5) OIA; s 10(5) LGOIMA.

Due particularity—your obligation as a requester

Be as specific as you can in identifying the information you want. Be open to communicating with the agency and helping the person responsible for answering your request to understand what it is you are looking for.

The information you are requesting must be specified with *'due particularity*'.[20] This means that the person receiving the request must be able to identify the information you have asked for.

A request that lacks due particularity will not be valid and the requirements of the OIA and/or LGOIMA will not apply.

Reasonable assistance—the agency's duty to you

If the agency can't understand what you are asking for it has a duty to provide you with reasonable assistance.[21]

Reasonable assistance is more than telling you that the request is not specific enough. Instead the agency should help you to make your request clear enough so that it can understand what you are looking for.

Remember though, that if an agency has to come back to you to help you make a request it can understand and work with, this will take longer. It is best to be as specific as you can at the beginning about what it is that you want.

Broad requests

Sometimes, requests are made for large amounts of information because the requester does not know exactly what type of information they are most interested in receiving or does not know how that information is held by the agency.

Requests which are unclear, or are too broad, may result in delays, charges, or even refusals. Risks with keeping your request too broad include:

- the agency could decide that the requested information hasn't been *'specified with due particularity'* and may need to seek clarification, which can affect the time taken for a decision to be made on your request;
- the agency may need to extend the maximum time limit for making a decision on your request;
- you could be faced with charges for the collation and supply of all the information you have asked for;

[20] See s 12(2) of the OIA; s 10(2) LGOIMA.

[21] See s 13 OIA; s 11 LGOIMA.

- you could end up with a lot of information that you don't want or need; and
- your request could be refused because the information cannot be made available without substantial collation or research.

Who do I send my request to?

Anyone in an agency can receive a request for official information but, if there is a specific person or team within an agency that is responsible for handling information requests, it may speed the process up to send your request directly there.

You can check the agency's website or ring the reception and ask who to send your information request to. Some agencies have online request forms or email addresses dedicated to official information requests, others do not.

If you are in doubt about who to send your request to, address it to the chief executive of the agency concerned. You can also write *'Request for official information'*, or *'OIA/LGOIMA request'* in the heading or subject line.

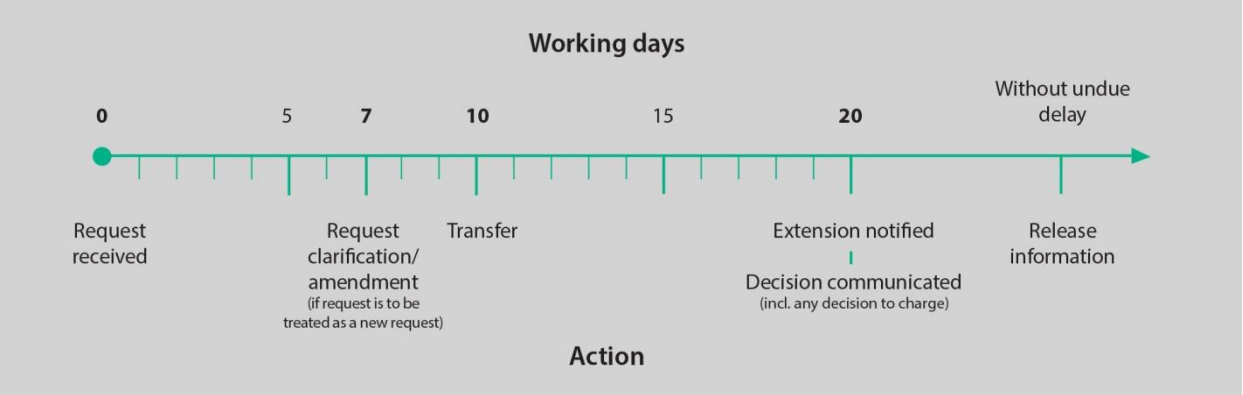
An agency's consideration of your request

Are there time limits?

The OIA and LGOIMA specify time limits for:

- transferring a request to another agency, if required;
- making a decision on a request; and
- extending the time limits, if required.

The OIA and LGOIMA also require information to be released without undue delay.



Transferring a request

An agency must transfer your request (or part of it) if the information you requested: [22]

- is not held by the agency, but is believed by the person dealing with the request to be held by another agency; or
- is believed by the person dealing with the request to be more closely connected with the functions of another agency.

Transfers can be between any agencies that are subject to the OIA or LGOIMA.

Any decision to transfer a request to another agency for response must be made promptly and no later than 10 working days after the first agency received your request (unless an extension is made). The agency you originally made your request to must inform you of its decision to transfer the request.

Making and communicating a decision

An agency must make and communicate a decision on your request *'as soon as reasonably practicable*' and **no later than 20 working days** after it was received (unless an extension is made).[23]

If you decide to amend or clarify your request, the amended or clarified version will be considered to be a **new** request,[24] and the 20 working days will start from the day after this new request is received. The exception to this will be if the agency was the one that asked you to amend or clarify the request, and it did not do so within 7 working days of receiving your original request.[25]

The agency's decision must state:

- whether the request will be granted; and if so
- in what manner—for example, whether it will release documents to you, or instead provide you with a summary of the information, or invite you to inspect the records at the agency's offices; and
- if it will charge for supplying the information and, if so, how much.

[22] See s 14 OIA; s 12 LGOIMA.

[23] See s 15(1) OIA; s 13(1) LGOIMA.

[24] See s 15(1AA) OIA; s 13(7) LGOIMA.

[25] See s 15(1AB) OIA; s 13(8) LGOIMA.

Releasing information

If an agency decides to release information, it must to so without *'undue delay'*.[26] In some cases, the agency may be justified in releasing the information at a later date after the decision is made, if time is required to prepare the information for release.

How to count time

A tool to automatically calculate response times is available on the home page of our website: www.ombudsman.parliament.nz.

When counting working days, day 1 is the first working day after the day on which the request is received by the agency.

'Working day' means any day of the week other than:

- Saturday and Sunday;
- national public holidays (Waitangi Day, Good Friday, Easter Monday, Anzac Day, Queen's Birthday, Labour Day); and
- the period from 25 December to 15 January inclusive.

A regional anniversary is a working day.

A working day is not limited to 9am to 5pm. Therefore, if a request is received by email or other electronic means outside business hours, it will still be counted as being received on that day, and the count will start on the next working day.[27]

Extensions

An agency may extend the maximum time limit for transferring a request or making a decision and communicating it to you, if:[28]

- your request is for, or requires a search through, a large quantity of information and meeting the original time limit would unreasonably interfere with the agency's operations; or
- consultations needed to make a decision on your request mean than a proper response cannot be made within the original time limit.

The extension must be for a reasonable period of time in the circumstances.

[26] See s 28(5) of the OIA (s 27(5) of LGOIMA), which provides that any undue delay in releasing information is deemed to be a refusal of a request that an Ombudsman can investigate.

[27] See s 11 of the Electronic Transactions Act 2002.

[28] See s 15A OIA; s 14 LGOIMA.

The agency must notify you of the extension within 20 working days after the day it received your request. The notice must:[29]

- specify the period of the extension;
- give the reasons for the extension; and
- state that you have the right to complain to an Ombudsman about the extension.

While more than one extension may be made within the original 20 working days (if necessary), no further extensions may be made once the original 20 working day maximum time limit has passed.

Requesting urgency

You may ask that your information request be treated as urgent, and if so you must give the reasons for seeking the information urgently.[30]

If you do request urgency, the agency should assess whether it would be reasonable to give your request priority over other requests and its existing work. However, the agency's legal obligations in terms of the maximum time limits set out in the OIA and LGOIMA, to extend, transfer and make a decision on your request, remain the same.

Can an agency charge?

If an agency decides to grant your request (whether by releasing all or some of the information you asked for) you may be asked to pay a charge.[31] However:

- the agency can only charge for **supplying** information, not for the time taken to consider whether or not to grant your request;
- the charge must be *'reasonable'*; and
- the decision to release information should also advise if a charge is to be made.

In considering whether to charge, an agency may consider the cost of the labour and materials involved in making the information available, including any particular costs associated with responding to an urgent request, such as a need to engage additional staff.

If an agency decides to charge you, it will usually write to you first to explain how much the charge is likely to be and how it has been calculated. The agency may request that the charge, or a deposit, be paid before it releases the information.

[29] See s 15A(4) OIA; s 14(4) LGOIMA.

[30] See s 12(3) OIA; s 10(3) LGOIMA.

[31] See s 15(1A)–(3) OIA; s 13(1A)–(4) LGOIMA.

The Government has issued *Charging Guidelines* to be followed by agencies subject to the OIA. These can be accessed from the Ministry of Justice website (search under *'publications'* at www.justice.govt.nz).

Although these guidelines apply to central government agencies subject to the OIA, they may also be referred to by local government agencies. Some local government agencies have their own charging policies. The Ministry of Justice guidelines describe how charges should be calculated and also list some of the factors which should be taken into account when deciding whether to reduce or waive a charge.

You can read our detailed guide to charging for official information here.

Can an agency ask me for more information or to change or clarify my request?

Yes. If an agency decides that it needs to do so, it can ask that you provide it with more information or to clarify or amend your request so that it is able to make a decision whether to grant or refuse it.

You are under no obligation to do so but, if you don't, the agency may need to extend the time limit to respond to your request, may have to impose a charge to cover administrative or other expenses, or may need to refuse the request altogether.

Clarification or amendment of your request can result in it being treated as a new request that replaces the original one, except if the agency sought your clarification more than 7 working days after receiving your original request.[32]

Can an agency consult others about my request?

An agency may decide to consult before it makes a decision on your request. Consultations may be with:

- you;
- the agency's in-house policy or legal team, external legal advisors, a particular staff member, the chief executive or relevant Minister for their comments on the proposed response;
- external third parties who supplied or are the subject of the requested information (to see if they have any concerns about disclosure, for example in relation to privacy issues, understandings of confidentiality or commercial sensitivities); and
- any other agency with an interest in the information.

[32] See s 15(1AA) and (1AB) OIA; s 13(7) and (8) LGOIMA.

If you have any concerns about disclosure of your identity to third parties during consultation, you should make this clear to the agency as soon as possible. You should be aware the agency may need to consider whether to disclose your identity, as this could be a relevant factor for a third party in identifying any concerns with release of the information.

Making a decision on your request

Can my request be refused?

The agency can refuse your request, but only if there is a reason to do so under the OIA or LGOIMA. Reasons for refusing a request fall into the following broad categories:

- administrative reasons;[33]
- conclusive reasons;[34]
- refusing to confirm or deny the existence or non-existence of information;[35] and
- good reasons.[36]

In some cases, before refusing a request, an agency must also consider whether there is a stronger public interest in favour of releasing the information which outweighs the need to withhold it. If so, the information must be made available.

Detailed guidance on the grounds for refusal of a request, in relation to particular sections of the OIA and specific subject areas, is available here.

Specific rules also exist for refusing requests for special categories of information, namely:

- internal rules or guidelines for decisions;[37]
- statements of reasons for decisions or recommendations;[38] and
- personal information requests by corporate entities.[39]

Sometimes, you may be given some, but not all, of the information you requested. For example, you may be provided with a copy of a document that has some information deleted. This amounts to a refusal of that part of your request.

---

[33] See s 18 OIA; s 17 LGOIMA.

[34] See ss 6 and 7 OIA; s 6 LGOIMA.

[35] See s 10 OIA; s 8 LGOIMA.

[36] See s 9 OIA; s 7 LGOIMA.

[37] See s 22 OIA; s 21 LGOIMA.

[38] See s 23 OIA; s 22 LGOIMA.

[39] See s 24 OIA; s 23 LGOIMA.

Reasons must be given for refusing requests

If your request for official information is refused, the agency must advise you of:

- the reason for the refusal;[40]
- if you ask, the grounds supporting that reason (unless doing so would itself harm an interest protected by the OIA or LGOIMA);[41] and
- your right to complain to an Ombudsman about the refusal.[42]

Releasing information

How will the information be provided?

There are a number of different ways an agency can make information available to you. These include:[43]

- giving you a reasonable opportunity to inspect the information;
- releasing a hard copy or electronic copy of the information;
- arranging for you to hear or view the information;
- providing you with a written transcript of the information;
- providing partial disclosure of the information—for example:
  - releasing a document with some information deleted ('redacted');
  - releasing a summary of the information;
  - releasing an excerpt, or particular passage, from a document; or
- providing you with an oral briefing.

The agency may also decide to:

- release the information subject to certain conditions, such as restricting you from disclosing the information to others;[44]

---

40 See s 19(a)(i) OIA; s 18(a)(i) LGOIMA.

41 See s 19(a)(ii) OIA; s 18(a)(ii) LGOIMA.

42 See s 19(b) OIA; s 18(b) LGOIMA.

43 See ss 16(1), 16(1A) and 17(1) OIA; ss 15(1), 15(1A) and 16(1) LGOIMA.

44 The imposition of conditions is allowed by s 28(1)(c) of the OIA (s 27(1)(c) of LGOIMA), which provides that an Ombudsman may investigate any condition imposed on the use, communication or publication of information released in response to a request.

- release the information with an additional statement to put it into context;
- release other relevant information in the public interest.

If you want the information to be provided in a particular way, you should say this in your request. Generally speaking, information should be released to you in the **way you prefer**.[45] If information is not provided in the way you would prefer, the agency must explain:

- the reasons why it decided not to give it to you in the way you wanted to receive it; and
- if you ask, the grounds supporting that reason (unless doing so would itself harm an interest protected by the OIA or LGOIMA).

Making information publicly available

An agency may, whether in response to your request or of its own accord, decide to publish information. For example, the agency may put the information on its website.

Public release of information by agencies promotes good administration, openness and transparency, and fosters public trust and confidence. It also has benefits for the agency including ease of handling or reduced requests for information that is readily accessible.

What can I do if I am unhappy with the response to my request?

If you are unhappy with the response to your request, you can complain to the Ombudsman. There is no charge for making a complaint.

The Ombudsman can consider most matters concerning an agency's decision making on an official information request.

Under the OIA and LGOIMA, an Ombudsman can investigate complaints about:

- a decision to refuse (or partially refuse) a request for information;
- delays in making a decision or in releasing information;
- a decision to extend any of the maximum time limits;
- a decision to charge for supplying information;
- the way in which information has been made available; and
- conditions imposed on the release of information.

[45] See s 16(2) OIA; s 15(2) LGOIMA.

An Ombudsman also has specific power to investigate, under the Ombudsmen Act 1975 (OA), complaints about requests:

- for internal rules or guidelines for decisions;
- for statements of reasons for a decision affecting you; or
- by corporate entities for their personal information.

In addition to these specific matters, an Ombudsman may also be able to consider complaints about the administrative conduct of an agency in responding to your request for information. Such complaints would be considered under the Ombudsman's general powers under the OA, provided the agency in question is subject to that Act.[46] This could include the processes followed by an agency during its consideration of your information request, such as transferring the request to another agency, or a decision not to grant urgency.

A complaint to the Ombudsman should be put in writing. The most straightforward way to make a complaint, and to ensure we have all the information we need from you, is to use the online complaint form.

You can also make a complaint by:

- email to info@ombudsman.parliament.nz;
- fax: (+64) 04 471 2254; or
- letter addressed to: Office of the Ombudsman, PO Box 10 152, Wellington 6143.

Your complaint should include the following information:

- your personal contact details, including your postal address;
- copies of your request and the agency's response (or full details if it is not possible to provide copies);
- the concerns you have; and
- the outcome you are seeking.

There is no obligation to tell the Ombudsman why you want the information, but it can be helpful in the overall consideration of your complaint.

If there are particular aspects of an agency's decision that you wish the Ombudsman to focus on, please say what these are. For example, if there are different parts to an agency's response, but you only want to complain about one part, or if you only need some of the information that has been refused rather than all of it, let us know. This may make it faster for us to deal with your complaint.

[46] See Schedule 1 of the OA. While an Ombudsman cannot investigate decisions by a Minister or at a meeting of the full council of a local authority under the OA, any advice provided to the Minister or full council by agency officials may be able to be investigated.

For more guidance on making a complaint visit www.ombudsman.parliament.nz. If you have any further queries, you can also telephone us on freephone 0800 802 602.

Appendix 1. Tips for making requests

- Make some general enquiries first—for example, a request for details of the work being done on a particular topic you are interested in may assist you to make a more specific, follow-up request for the exact information you are seeking.
- Be as clear and specific as possible about the information you are seeking:
    - If it is a particular document, name it or, if you are not sure of its name, describe it with reference to author, date, content and/or subject matter.
    - If it is information on a particular topic or subject, explain in detail the information you are seeking. You do not have to say why you want the information or what you intend to do with it, but sometimes providing this explanation may be helpful to the agency to identify all the relevant information that you would like to receive.
    - If you are seeking information held on a particular topic or subject that may span months or years, give a specific (and if possible limited) timeframe for the information you are seeking.
    - If you don't want to receive certain types of information (for example, internal emails, draft documents, or personal information about others) make that clear in your request so the agency doesn't waste time on these—or resources that you may be charged for.
    - If you are seeking reasons why a decision or recommendation was made about you, say so. You may be entitled to a statement of reasons created by the agency, even if it does not hold much documented information about the decision. In requesting a statement of reasons, it is helpful to refer to your specific right to seek reasons under section 23 of the OIA.
- If you are making multiple requests, prioritise the order in which you wish your requests to be answered or clearly state what is most important to you.
- If you need the information urgently say so, give the reasons why and the timeframe within which you hope to receive it.
- Tell the agency if you are happy to receive the information in an alternative form, for example, oral briefing, viewing or summary.
- Provide your contact details and, if you are happy to discuss your request with the agency, invite it to do so.
- Keep copies of any requests made in writing. If you make an oral request, make a note of when, how and who you made your request to.
- Consider following-up your request if you don't receive an acknowledgement within a reasonable period of time. While agencies are not required to acknowledge requests, many do. If no acknowledgement is received, it may mean your request has gone astray. Early follow-up can help ensure a more timely response is received.

Appendix 2. Template letter—request for official information

[Your full name]

[Your address]

[Phone number/email]

[Date]

[Name and address of the organisation]

Dear Sir or Madam

Official information request: [brief detail of the subject matter of the request]

Please supply the following information under the [Official Information Act (OIA) / Local Government Official Information and Meetings Act (LGOIMA)]:

[give specific details of the information you are seeking, such as a particular document or file, or information on a particular topic created within a stated time frame]

If you need any more information from me please let me know as soon as possible.

I understand that a decision on a request for information under the [OIA/LGOIMA] should be made within 20 working days of receiving that request.

If you do not normally deal with official information requests, or you need advice on dealing with this request, guidance is available from the Ombudsman at www.ombudsman.parliament.nz.

Yours faithfully

[Signature]

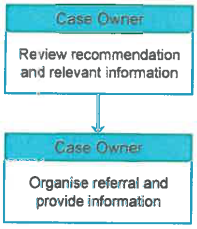
Making a referral to the Clinical Advisory Panel

The Clinical Advisory Panel (CAP) can provide medical advice regarding causation for complex cases, but only if referral to the CAP is recommended by a branch medical advisor (BMA), clinical advisor (CA), regional clinical leader (RCL) or senior medical advisor (SMA).

When a case owner receives a recommendation for referral to the CAP from a BMA, CA, RCL or SMA, they use this process to organise the referral and ensure it includes all the relevant information.

Contact [redacted] Last review 12 Oct 2016 Next review 12 Oct 2017

Click on a shaded box for instruction details



Show all instructions

Review recommendation and relevant information

Responsibility

Case owner

When to use

Use this instruction to check that the referral includes all the relevant medical information.

Instruction

Step 1

Review the recommendation.

Step 2

Ensure the recommendation and all relevant medical information has been uploaded to the claim.

Step 3

If the claim involves a hip labral tear, prepare a CD containing all the relevant imaging.

What happens next

Go to Organise the referral.

Back to process map ↑

Organise referral and provide information

Responsibility

Case owner

When to use

Use this instruction to arrange the referral after you've checked the request and the relevant information.

Instruction

Step 1

Create an 'Organise Internal Referral' parent task in Eos.

Step 2

Create a 'Complete Internal Referral' sub- task in Eos and:

- edit the 'Description' to ensure the first words are either "BMA Referral", "CA Referral" ,"RCL Referral" or "SMA Referral", as appropriate.
- ensure the 'Description' also includes:
  - the surgeon's name and surgery code, where appropriate
  - the specific questions the CAP needs to answer.

Step 3

Link the relevant documents to the 'Complete Internal Referral' sub-task.

Step 4

Transfer the 'Complete Internal Referral' sub-task to the 'Elective SC – Clinical Advisors' queue.

If the claim involves a hip labral tear, provide the CD with the relevant imaging to the Clinical Advisory Panel (CAP).

Step 5

Place the 'Organise Internal Referral' parent task on hold for 5 working days.

What happens next

If there is...	then...
enough information	• an administration officer – CAP will allocate the referral to the appropriate medical advisor – CAP • the medical advisor - CAP will review the referral and provide an opinion • the administration officer – CAP will upload the opinion to the relevant claim 'Documents' tab in Eos and close the 'Complete Internal Referral' sub-task • the 'Organise Internal Referral' parent task will come off hold and return to the case owner's active work list • this process ends

not enough information	• an administration officer – CAP will:
	  • review the 'Complete Internal Referral' sub-task and ask the case owner to provide any missing or additional information
	  • cancel the 'Complete Internal Referral' subtask
	• return to step 2

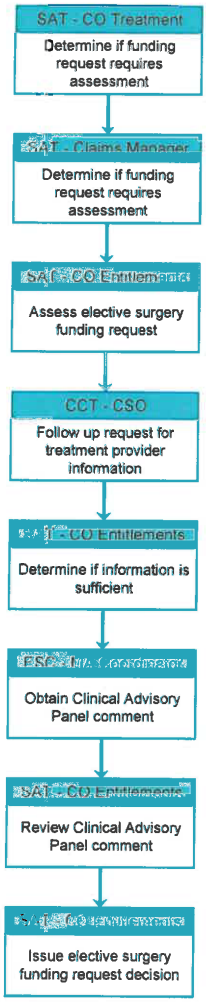
Back to process map ↑

Issuing an elective surgery funding decision

The Surgery Assessment team (SAT) use this process to gather the appropriate information and to make a decision when they receive an Assessment Report and Treatment Plan (ARTP) that includes a request for elective surgery funding.

Contact [redacted] Last review 01 Dec 2016 Next review 01 Dec 2017

Click on a shaded box for instruction details



Show all instructions

Determine if surgery funding request is acceptable

Responsibility

Surgery Assessment team – Claims Officer Treatment

When to use

Use this instruction when you receive an Assessment Report and Treatment Plan (ARTP) to determine if an elective surgery funding request is acceptable.

Instruction

Step 1

Review the ARTP and check that the details match those in Eos.

Step 2

If...	then...
the surgeon has indicated on the ARTP that either: • the condition is not accident related • cover has been declined • there is no registered injury	• create a purchase order (PO) • go to Issue elective surgery funding request decision to decline the request
the ARTP is incomplete	• create a PO • send the client an ELE02a – Elective surgery – missing information – client letter and copy to the lead provider and specialist • cancel the PO • go to step 3
cover is still "held"	• create a PO • send the client an ELE03a – Claim not accepted – cover pending – client letter and copy to the lead provider and specialist • cancel the PO • go to step 3
there is no registered claim	• send the client an ELE40 – Request received (party level) – no registered claim - client letter and copy to the lead provider and specialist • go to step 3
it is an accredited employer claim	• create a PO • send an email to the lead provider and specialist telling them that it's an accredited employer claim and they should send the ARTP directly to the employer • cancel the PO • go to step 3
the surgeon has established a causal link and there is appropriate cover	go to step 5

Step 3

Update the 'Determine Surgery Funding Eligibility' task by describing the action taken in step 2 above, and then close it.

Step 4

Put the claim into 'ESC – Actioned Cases'.

This process ends.

Step 5

Determine which office will manage the elective surgery funding request using the following table.

If...	then the surgery decision is made in...	and any resulting incapacity or assistance is managed in...
the request or another claim for the same client is open at branch	branch	branch
the client was in receipt of weekly compensation on this claim within the previous 12 months in STCC (and surgery will likely create reactivation and transfer to branch)	ESU Surgery Assessment Team (ESC & NSC)	branch
the request is for a dental procedure		STCC or branch

If...	then the surgery decision is made in...	and any resulting incapacity or assistance is managed in...
	Dental team (Hamilton or Dunedin)	
the request does not fit the above categories	ESU Surgery Assessment Team (ESC & NSC)	STCC or branch

Step 6

Create a PO under the correct managing site. If transferring to a branch issue the ELE10a - Referred to Branch letter.

Step 7

Transfer the 'Determine Surgery Funding Eligibility' task to the appropriate queue.

What happens next

Go to **Determine if funding request requires assessment.**

Back to process map ↑

Determine if funding request requires assessment

Responsibility

Surgery Assessment team – Claims Manager

When to use

Use this instruction to determine if a surgery funding request requires assessment when the 'Determine Surgery Funding Eligibility' task has been transferred to your work queue.

Instruction

Step 1

- Determine if the elective surgery funding request can be approved with the information provided or if it will require further assessment
- Refer to the Fast Track Assessment (FTA) consideration factors if applicable.

Step 2

If...	then...
there is sufficient information for approval	go to Issue elective surgery funding request decision to approve the funding request

the request requires further assessment	• update the 'Determine Surgery Funding Eligibility' task explaining why the request requires further assessment
	• transfer the task to the relevant Surgery Assessment queue for further investigation:
	  • NSC looks after all knee requests
	  • ESC looks after all other body sites that are not transferred to branch
	• go to Assess elective surgery funding request

Back to process map ↑

Assess elective surgery funding request

Responsibility

Surgery Assessment team – Claims Officer Entitlements

When to use

Use this instruction to assess an elective surgery funding request when the 'Determine Surgery Funding Eligibility' task has been transferred to your work queue.

Instruction

Step 1

Create an ACC5971 Elective surgery information summary and clinical comment (132K), complete the relevant fields and leave as incomplete.

Step 2

If...	then...

additional information is required	• create a PO for each additional information request (MEDR/COPY/DHBC)
	• create the appropriate letter and send to the treatment provider:
	  • ELE38a - Further info – request for info – GP
	  • ELE38b – Further info – request for info – Allied
	  • ACC2386 Clinical records request – DHB
	• send the client an ELE01a – acknowledge request – client letter and copy to the lead provider and specialist
	• go to step 3

no additional information is required	• send the client an ELE01a – acknowledge request – client letter and copy to the lead provider and specialist • go to Determine if information is sufficient

Step 3

Update the 'Determine Surgery Funding Eligibility' task with the notes that have been requested and who they have been requested from, and then place it on hold.

Step 4

Create the subtask 'Contact Treatment Providers for Information', and update the target date to nine network days.

Step 5

Transfer the task to the Customer Contact team for follow-up.

What happens next

Go to **Follow up request for treatment provider information.**

Back to process map ↑

Follow up request for treatment provider information

Responsibility

Customer Contact team – Customer Support Officer

When to use

Use this instruction to follow up a request for additional information from the treatment providers when the subtask 'Contact Treatment Providers for Information' has been transferred to your work queue.

Instruction

Step 1

Check the claim to see if the requested information has already been received.

If the information...	then...
has already been received	• close the 'Contact Treatment Providers for Information' subtask • update the 'Determine Surgery Funding Eligibility' task with "notes in" and take it off hold • go to Determine if information is sufficient
hasn't been received	• call the provider to ensure they received the initial request (via ELE38a, ELE38b or ACC2386) and re-send it if necessary • go to step 2

Step 2

Once the target date is reached, use the following table.

If the information...	then...
has been received	• close the 'Contact Treatment Providers for Information' subtask • update the 'Determine Surgery Funding Eligibility' task with "notes in" and take it off hold • go to Determine if information is sufficient
the required information is not received within the timeframe	• close the 'Contact Treatment Providers for Information' subtask • update the 'Determine surgery funding eligibility' task with "target date reached" and take it off hold • go to Determine if information is sufficient

Back to process map ↑

Determine if information is sufficient

Responsibility

Surgery Assessment team – Claims Officer Entitlements

When to use

Use this instruction to determine if the information available is sufficient or if clinical comment is also required for a decision to be made about the elective surgery funding request.

Instruction

Step 1

Review the information on hand to determine whether there is sufficient information to proceed.

Step 2

If...	then...
there is sufficient information to approve surgery without clinical comment	• save the ACC5971 Elective surgery information summary and clinical comment (132K) as complete • go to **Issue elective surgery funding request decision** to approve the funding request
there is sufficient information and clinical comment is required	• update the ACC5971 in Eos with any additional information that has been received and the questions for the Clinical Advisory Panel (CAP) • go to step 3
there is insufficient information	• send the client an ELE35 – Request to pay for surgery – further information required - client letter and copy to the lead provider and specialist • go to **Issue elective surgery funding request decision** to decline due to insufficient information

Step 3

Update the 'Determine Surgery Funding Eligibility' task with "referred to CAP" and place it on hold.

Step 4

Create a 'Request Clinical Advisor Comment' subtask, attach the relevant documents from the relevant claims and transfer it to the Elective Service Centre - Clinical Advisors queue.

What happens next

Go to **Obtain Clinical Advisory Panel comment.**

Back to process map ↑

Obtain Clinical Advisory Panel comment

Responsibility

Elective Service Centre – Medical Advisor Coordinator

When to use

Use this instruction to obtain Clinical Advisory Panel (CAP) comment on an elective surgery funding request when the 'Request Clinical Advisor Comment' subtask has been transferred to your department queue.

Instruction

Step 1

Create a 'Complete Internal Referral' subtask and transfer it to a CAP member for comment.

Step 2

When CAP comment is available, add it to the ACC5971 Elective surgery information summary and clinical comment (132K) in Eos and save the document as complete.

Step 3

If the CAP member...	then...
has requested that the file be discussed at a full CAP meeting	• update the 'Determine Surgery Funding Eligibility' task with "Full CAP" or "FTF (face to face) CAP" and the date of the meeting • leave the 'Request Clinical Advisor Comment' subtask open • go to **Review Clinical Advisory Panel comment**
has commented	• close the 'Request Clinical Advisor Comment' subtask and update the 'Determine Surgery Funding Eligibility' task with "comment uploaded" • go to **Review Clinical Advisory Panel comment**

Back to process map ↑

Review Clinical Advisory Panel comment

Responsibility

Surgery Assessment team – Claims Officer Entitlements

When to use

Use this instruction to review the Clinical Advisory Panel (CAP) comment when the 'Determine Surgery Funding Eligibility' task has been updated with "comment uploaded".

Instruction

Step 1

Review the CAP comment and determine if the surgery funding request can now be approved or declined, or if further information is required.

Step 2

If...	then...
CAP comment has been provided and the information is sufficient	go to **Issue elective surgery funding request decision**
CAP has requested further information or requested a second opinion	• confirm with the medical advisor coordinator that the case has been added to the list to be heard at the next CAP meeting – a second opinion cannot be requested without a full CAP comment • contact the client to advise of the delay in issuing a decision. If unable to contact by phone, send the client a delay in decision letter and copy to the lead provider and specialist • go to **Assess elective surgery funding request** and request the required information or second opinion • go to step 3

If...	then...
Senior Medical Advisor (SMA) opinion is required	• create a 'Complete Internal Referral' subtask and transfer to SMA using the Corporate Clinical Advice Queue. • update the 'Determine Surgery Funding Eligibility' task with "SMA comment requested" and place the task on hold • go to step 4
CAP has requested the surgery request be discussed at the next full CAP meeting (either teleconference or face to face)	• contact the client to advise of the delay in issuing a decision. If unable to contact by phone, send the client a delay in decision letter and copy to the lead provider and specialist • place the task on hold • go to step 3

Step 3

If...	then...
the required information or second opinion has been received	go to **Issue elective surgery funding request decision**
there is insufficient information to progress the surgery request and an ELE35 - No decision - further information required letter has already been sent	• suspend the assessment – decline on the basis that we have been unable to obtain sufficient information • go to **Issue elective surgery funding request decision** to issue the appropriate decline letter

Step 4

If...	
SMA has commented	go to **Issue elective surgery funding request decision**
SMA hasn't commented	• follow up with SMA to attain comment • once SMA has commented, go to **Issue elective surgery funding request decision**

Back to process map ↑

Issue elective surgery funding request decision

Responsibility

Surgery Assessment team – Claims Officer Entitlements

When to use

Use this instruction to approve or decline a request for elective surgery funding when sufficient information has been received.

Instruction

Step 1

Update the 'Determine Surgery Funding Eligibility' task with the decision and close the task.

Step 2

If appropriate, amend or update the injury codes on the medical tab.

Step 3

If the decision is to...	then...
approve	• authorise the PO

If the decision is to...	then...
	• go to step 4

decline due to surgery being required to treat a "condition" that ACC has not agreed to cover	• decline the PO
	• send the appropriate letter to the client and copy to the lead provider and specialist. Attach the ACC5971 Elective surgery information summary and clinical comment (132K) where necessary:
	  • ELE30b – Request to pay for surgery decline – client (46.5K)
	  • ELE39 – Request to pay for surgery decline (and amend cover) – client (45.5K)
	• create the 'Contact Party' task and send to the Customer Contact team to phone client to advise them of the surgery decline decision
	The Customer Contact team will close the task

decline due to insufficient information	• send the client an ELE37 – Request to pay for surgery decline (insufficient information) – client (40K) letter and copy to the lead provider and specialist • go to step 5
decline because the surgeon has indicated on the ARTP that surgery is not injury related	• send the client an ELE34 – Request to pay for surgery - decline (surgeon states no causal link) – client (42K) letter and copy to the lead provider and specialist • go to step 5
decline because there is no registered injury	• create a PO • call the client to advise of the decision and confirm that the decision letter can be sent to the lead provider and specialist, as it contains privacy information • once confirmed, send the client an ELE04a – no injury recorded – client (43K) letter and copy to the lead provider and specialist • decline the PO • go to step 5

Step 4

Create and send the appropriate letter.

Client:

- ELE20a - FF Surgery approval letter - client (40.5K)
- ELE21 - Elective surgery approve - part funded (regs) - client (98.5K)
- ELE22 - Elective surgery approve - part funded (non-core) - client (98K)
- ELE23 - Surgery approval (add cover for additional diagnosis) - client (44K)
- ELE24 - Surgery approval (and amend cover diagnosis) - client (45K)

Vendor:

- ELE20b - ESC FF Approval letter - vendor (45.5K)
- ELE21 - Elective surgery approve - part funded (regs) - vendor (48K)
- ELE22 - Elective surgery approve - part funded (non-core) - vendor (45K)

Step 5

Put the claim into 'Elective Service Centre – Actioned Cases'.

This process ends.

Back to process map ↑

Clinical advice standards

March 2015

Initial clinical advice must address all of the following standards.

Subsequent advice may only require a short response providing the initial advice is complete.

Eos is the primary tool for communication and is to be used to capture even verbal advice.

Standard	Description
1. The structure of clinical advice includes:	The clinical advisor includes their name, designation qualification/ area of specialty if relevant to a complex case.
• the issue is identified	Identified and relevant issues explained. Consideration of the clinical findings, investigations, and opinion of treating clinicians, along with any expert opinion and references. Review of the necessary material to provide an informed opinion. Look beyond what's being asked to ensure a full understanding of the claim and the right issues are being identified. Documentation of what is agreed/disagreed with.
• analysis	Evidence of appropriate analysis, material reviewed and weighing up of the available evidence.
• conclusion	An objective conclusion with consideration of the client's unique information. The way in which the advice is communicated should be clear and explicitly written in a way that is understandable by the case owner to support safe outcomes for the client.
• recommendations as appropriate	Explicit statement of recommendations if required for the case owner to action.
2. Factual and objective clinical advice	Review the claim information, weigh up the evidence, provide a rationale for the clinical opinion with the advice offered being independent, neutral and unbiased.
3. Based on relevant referenced literature where necessary and clinical opinion	Use appropriately cited documents where required.
4. Clinical advice is consistent with legislation and policy	Clinical advice demonstrates the application of awareness of ACC and other relevant legislation. Advice given is culturally appropriate.
5. Timely completion of clinical advice	Completed within 10 working days or less from the date taken from the task queue until completion of clinical advice. If not met an explanation is provided.
6. Clinical advice is completed for the client with respectful consideration of their circumstance	Respectfully written, readily understandable by the case owner and possibly a wider audience inside and outside ACC.

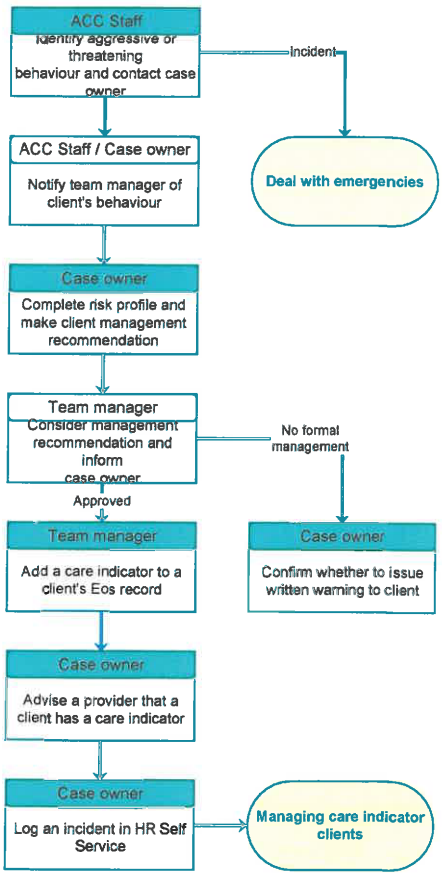
Assessing a client's risk level

ACC staff use this process when a client behaves in an aggressive and threatening manner and could pose a risk to providers or staff. The case owner (or staff member if there's no active claim) then works with their manager to decide if a Care Indicator is required on the client's record and makes a recommendation for how they are managed.

See also WorkSAFE: Dealing with aggressive/dangerous clients.

Contact [redacted] Last review 01 Jul 2016 Next review 01 Jul 2017

Click on a shaded box for instruction details



Show all instructions

Identify aggressive or threatening behaviour and contact case owner

Responsibility

ACC staff

When to use

Use this instruction to immediately raise a concern about a client's behaviour when you think they could be a risk to providers and other staff.

You may get information about their behaviour from any external source, eg a provider.

Before you begin

If you're not sure whether the behaviour requires escalating see Aggressive and threatening behaviour guidelines.

Instruction

Step 1

If you're...	then...
the client's case owner	• immediately let your team manager know of the incident • go to Complete risk profile and make client management recommendation
not the client's case owner	go to step 2

Step 2

Look up the client in Eos.

If the client...	then...
has an active claim	• contact the case owner and let them know the details of the incident and that they need to assess the client's risk level • go to Complete risk profile and make client management recommendation
doesn't have an active claim	go to step 3

Step 3

Look up the client's most recent closed claim.

If...	then...
you can locate the most recent closed claim	• contact the case owner/team manager and let them know the details of the incident and that they need to assess the client's risk level • go to Complete risk profile and make client management recommendation
there are too many claims to go through to find the most recent	go to step 4

Step 4

Contact the ACC branch closest to the client's address.

If the case owner/team manager at the site...	then...
can manage the client	• let them know the details of the incident and that they need to assess the client's risk level • go to Complete risk profile and make client management recommendation
can't manage the client	• escalate the situation to the branch manager or area leader • this process ends

Back to process map ↑

Complete risk profile and make client management recommendation

Responsibility

Case owner

When to use

Use this instruction to complete a risk profile for a client when they have behaved in an aggressive or threatening manner and make a recommendation to your team manager for how they are managed.

If your team manager is unavailable, escalate to your unit manager.

Before you begin

Ensure you've advised your team manager of the incident as soon as possible.

If necessary, the team manager can activate a Care Indicator on the relevant client straight away. See Add a care indicator to a client's Eos record.

Instruction

Step 1

Check the client's Eos record for active claims. If there are other staff members involved with the client, contact them and let them know about the situation.

Step 2

Open an ACC159 Client risk profile summary (108K) form and fill in as much detail as possible, including information from:

- Eos contacts and claimant care notes
- the client's general practitioner (GP), employer or provider
- any other source that is publicly available, such as a media report

Step 3

Summarise the level of risk the client poses and make a recommendation for how you think the client should be managed.

See Guidelines for making a client management recommendation.

Step 4

Discuss the risk profile summary with your team manager to confirm it's accurate, then give it to them as they will need it when developing the management plan.

If formal management is...	then go to...
not required	Confirm whether to issue written warning to client
required	Add a care indicator to a client's Eos record

Back to process map ↑

Confirm whether to issue written warning to client

Responsibility

Case owner

When to use

Use this instruction to confirm with your team manager whether it's necessary to issue a written warning to a client, and add a claimant care note to their Eos party record.

Instruction

Step 1

Speak with your team manager about the incident and use the following table to determine the appropriate action.

If...	then...
you've already warned the client on the phone and no further warning is required	go to step 4
a written warning is required	go to step 2

Step 2

Send the client a written warning outlining the incident and the reason they are being warned for their behaviour or comments.

Step 3

Upload the letter under the documents tab in Eos.

Step 4

Add a client care note to the 'Contacts' tab of the client's Eos Party record detailing the incident and whether or not a phone call was made to discuss it.

What happens next

This process ends.

Back to process map ↑

Add a care indicator to a client's Eos record

Responsibility

Team manager

When to use

Use this instruction to add a care indicator to a client's Eos record when you approve the recommended management plan.

Before you begin

Ensure you have met the Criteria for activating the care indicator.

Instruction

Step 1

Open the client's Eos party record and add a care indicator.

Step 2

Inform the case owner that you've added the Care Indicator and that they can notify the relevant business units and/or providers. To notify a provider, go to Advise a provider that a client has a care indicator.

What happens next

If the client has made a threat or behaved aggressively to staff and/or a provider, go to Log an incident in HR Self Service.

The care indicated client is managed according to the Managing care indicated clients process.

Back to process map ↑

Advise a provider that a client has a care indicator

Responsibility

Case owner

When to use

Use this instruction to advise a provider that a client has an active care indicator.

Instruction

Step 1

Notify the provider in writing either by email or post to let them know the client has an active care indicator. Make sure you save this correspondence on the party file on the claim.

Note: It's important staff do not release details about a client's criminal history to providers or anyone else.

Step 2

If the provider asks for a security guard go to Ordering security for staff and provider safety.

What happens next

Go to Log an incident in HR Self Service.

Log an incident in HR Self Service

Responsibility

Case owner

When to use

Use this instruction to log an incident in HR Self Service if a client has either:

- made a personal threat against a staff member or service provider
- made an organisational threat against ACC

- used offensive or abusive language when talking to an ACC staff member
- behaved in a way that may have put staff or providers at risk of harm.

Instruction

Step 1

Log in to HR Self Service.

Step 2

Click 'Incident Reporting' in the 'Employee Self Service' box.

Step 3

Complete all the fields as appropriate, then click 'Submit'.

What happens next

The care indicated client is managed according to the Managing care indicated clients process.

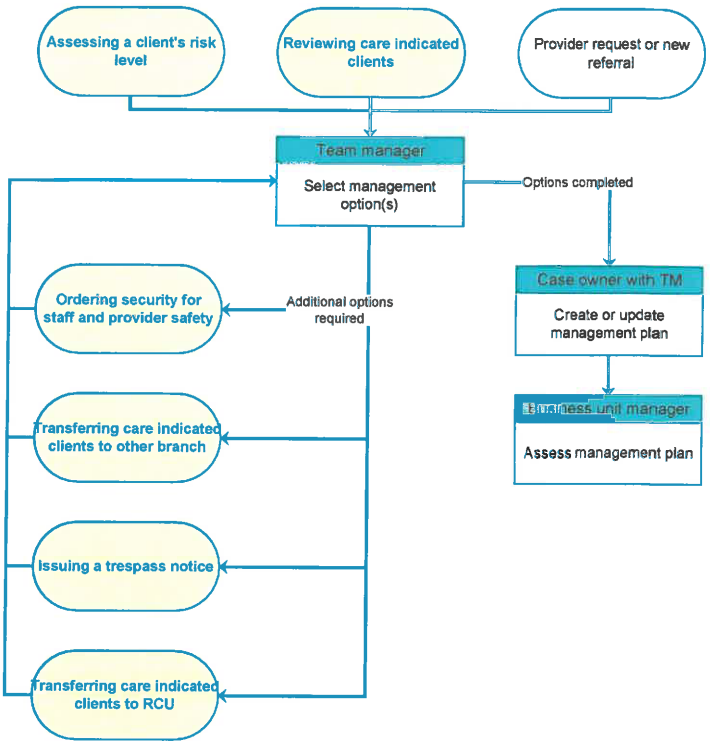
Back to process map ↑

Managing care indicated clients

Team managers and case owners use this process to implement the recommended management options for care indicated clients and to create or update their management plans in Eos.

Contact [redacted] Last review 01 Jul 2016 Next review 01 Jul 2017

Click on a shaded box for instruction details



Show all instructions

Select management option(s)

Responsibility

Team manager

When to use

Use this instruction to implement the approved management option(s) for a care indicated client.

Instruction

Step 1

If the management option involves...	then go to...
ordering security	Ordering security for staff and provider safety
transferring to another branch	Transferring care indicated clients to another branch
a trespass notice	Issuing a trespass notice
transferring to the RCU	Transferring care indicated clients to the RCU

What happens next

When all the management options have been actioned, go to Create or update management plan.

Back to process map ↑

Create or update management plan

Responsibility

Case owner with team manager

When to use

Use this instruction to create or update a client's management plan on their Eos party record when all required management options have been actioned.

Instruction

Step 1

The latest instructions for how to create or update a client's management plan can be found on the Sauce here: Activate, review and remove a client Care Indicator.

See Add an indicator.

Step 2

Notify your business unit manager that the management plan is completed.

What happens next

Go to Assess management plan.

Back to process map ↑

Assess management plan

Responsibility

Business unit manager

When to use

Use this instruction to assess a client's management plan to ensure it is complete and correct when a case owner notifies you that it has been completed.

Instruction

Step 1

The latest instructions for reviewing a client's management plan in Eos can be found on the Sauce here: Activate, review and remove a client Care Indicator.

Step 2

If the management plan is...	then...
complete and correct	• inform the case owner • this process ends
not approved	• liaise with the case owner to correct any errors or discuss the management of the client • restart this process

What happens next

The client and the way they are being managed will be reviewed as part of the Reviewing care indicator clients process.

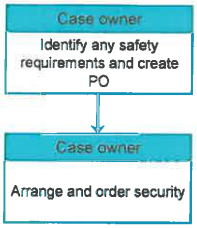
Ordering security for staff and provider safety

Case owners use this process to order security when we've arranged a meeting with an ACC client with a care indicator, or a provider requests security for a meeting.

If you require security for non-claim purposes, go to Order a security guard on The Sauce.

Contact [redacted] Last review 01 Jul 2016 Next review 01 Jul 2017

Click on a shaded box for instruction details



Show all instructions

Identify any safety requirements and create PO

Responsibility

Case owner

When to use

Use this instruction to confirm the dates and times of meetings that require security.

Where possible, arrange security guards to attend meetings during normal working hours.

Instruction

Step 1

If the meeting is...	then...
with a provider	go to step 2
at ACC	go to step 4

Step 2

Review the client's claim and risk status in Eos.

Step 3

Contact the provider to discuss the safety requirements, including:

- how many guards we need
- where we need the guard(s)
- whether the guards need to be male or female
- the dates and times we need the guard(s)
- whether we need the guards in uniform or plain clothes
- the urgency for security, eg within the next 45 minutes or not.

Note: If a provider doesn't want security for a care indicated client, add a contact on the claim noting the details.

Step 4

Update the 'Rehabilitation actions, Interventions and Entitlements' in the client's claim record in Eos. Use the following codes for entitlements.

Code	Description	Billing method
SG01	Standard security guard service	hourly

Code	Description	Billing method
SG02	After hours security guard services	hourly
SG03	Exceptional circumstances	hourly
SGTD	Travel distance > 50km	distance

Step 5

Create a purchase order for security on the client's claim record in Eos.

What happens next

Go to Arrange and order security.

Back to process map ↑

Arrange and order security

Responsibility

Case owner

When to use

Use this instruction to order security when you've confirmed the requirements and created a purchase order in Eos.

Instruction

Step 1

Open and complete the ACC7408 Security guard request for ACC or a provider form (171KB).

Note: Complete section three to order a guard for an ACC office. Complete section four to order a guard for a provider's office.

Step 2

Email it to armourguard.response@armourguard.co.nz.

Step 3

Save a copy of the form to the claim record in Eos.

Step 4

Contact the provider and:

- tell them we've ordered security for their client meeting
- ask if they have told the client that there will be security at the meeting. If they have not, contact the client to tell them
- record the conversation by adding a contact on the Eos claim.

Step 5

The security company confirms when they receive the order. If there is no confirmation within 24 hours, ring the security company to confirm.

Step 6

Record the security confirmation details as a client care note on the client's party record in Eos.

What happens next

If the security has been arranged well in advance, it is advised that you call the security company to confirm the booking closer to the date.

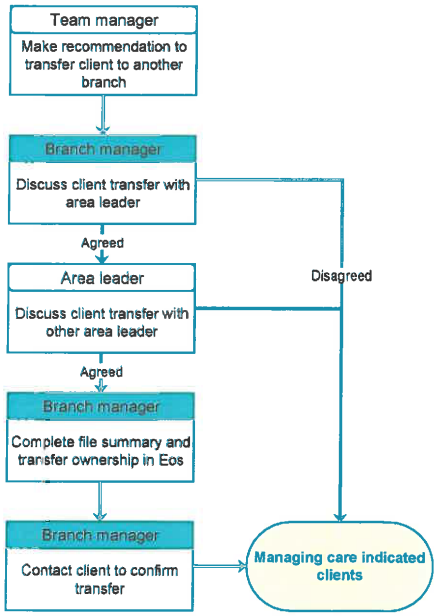
Back to process map ↑

Transferring care indicated clients to another branch

Branch managers use this process to initiate discussions with area leaders about potentially transferring a care indicated client to another branch. This client management option is often used when a care indicated client moves to another city and needs to be transferred to a branch closer to their new location, but can also be used when a client has behavioural issues dealing with specific branch staff.

Contact [redacted] Last review 01 Jul 2016 Next review 01 Jul 2017

Click on a shaded box for instruction details



Show all instructions

Discuss client transfer with area leader

Responsibility

Branch manager

When to use

Use this instruction to discuss transferring a care indicated client to another branch with your area leader.

See also Guidelines for making a client management recommendation.

Instruction

Step 1

Discuss the client transfer with your area leader. Useful information to discuss at this meeting includes:

- whether the client has moved and if so, their new location
- details of the events that led to the care indicator being put in place
- details of any events or actions that caused a strain in the client relationship
- historical information about the client
- the reason why the branch transfer is the best course of action.

What happens next

The area leader will discuss the transfer with the area leader of the new branch to confirm it is okay (if the other branch is in another area).

If the transfer is...	then...
agreed	• the area leaders will inform both branch managers that the transfer is progressing • go to Complete file summary and transfer ownership in Eos
not agreed	go back to the Managing care indicator clients process.

Back to process map ↑

Complete file summary and transfer ownership in Eos

Responsibility

Branch manager

When to use

Use this instruction to transfer ownership of a client to another branch when your area leader confirms the transfer has been agreed.

Instruction

Step 1

Complete an ACC29 File summary and overview form and save it to the client's Eos record.

Step 2

Open the client's active claim and click the 'To Department' magnifying glass icon.

Step 3

Navigate to and click on the name of the other branch in the 'Department' list.

Step 4

Click the 'Reason' drop-down menu and select 'Requested from Branch/CC'

Step 5

Add any other applicable information to the 'Description' field and click 'OK'

Note: Repeat steps 2-5 for each of the client's active claims.

Step 6

Send the client's physical case file to the other branch, if required.

Step 7

Contact the other branch at the same time Eos is updated to confirm that the ownership has been transferred correctly.

What happens next

Go to Contact client to confirm transfer.

Back to process map ↑

Contact client to confirm transfer

Responsibility

Case owner

When to use

Use this instruction to confirm the transfer of ownership with the client when you have received all of their files.

Instruction

Step 1

Check the client's management plan in Eos to see how you are able to contact them.

If you...	then...
can contact the client by phone	• phone them to introduce yourself and explain the situation • record the details of the conversation in the client's management plan • go to step 2
cannot contact the client by phone	go to step 2

Step 2

If there is an appropriate standard letter for introducing yourself as the new case owner, send this to the client.

Otherwise follow your branch's standard procedure for notifying the client.

What happens next

Return to the Managing care indicator clients process.

Back to process map ↑

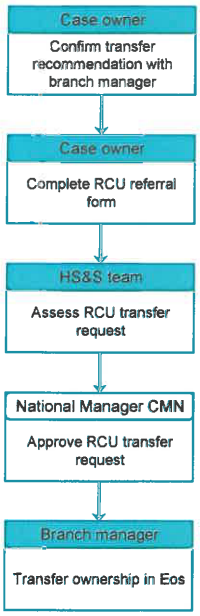
Transferring care indicated clients to the RCU

Case owners, branch managers and area leaders use this process to transfer a care indicated client to the Remote Claims Unit (RCU).

If the transfer is approved, the branch manager arranges the transfer. If the transfer is not approved, we continue to manage the client in line with their individual management plan.

Contact [redacted] Last review 01 Jul 2016 Next review 01 Jul 2017

Click on a shaded box for instruction details



Show all instructions

Confirm transfer recommendation with branch manager

Responsibility

Case owner

When to use

Use this instruction to confirm a Remote Claims Unit (RCU) transfer recommendation with the branch manager.

Instruction

Step 1

Discuss the client transfer to the RCU with your branch manager, focusing on the specific threats made to ACC staff or providers. Useful information to discuss includes:

- details of the events that led to the care indicator being put in place
- details of any events or actions that demonstrate that the client could pose a direct risk to the safety of staff
- historical information about the client
- the reason why the RCU transfer is the best course of action.

What happens next

The branch manager will discuss the RCU application with the Health, Safety and Security Team.

If the transfer is...	then...
agreed	go to Complete RCU referral form

If the transfer is...	then...
not agreed	• discuss an alternative solution with the branch manager • go back to the Managing care indicated clients process

Back to process map ↑

Complete RCU referral form

Responsibility

Case owner

When to use

Use this instruction to complete a Remote Claims Unit (RCU) referral form to apply for a client to be transferred to the RCU.

Instruction

Step 1

Complete an ACC2222 Remote Claims Unit referral form and get it endorsed by your branch manager.

Step 2

Email the completed form to the Security Advisor.

What happens next

Go to Assess RCU transfer request.

Back to process map ↑

Assess RCU transfer request

Responsibility

Health, Safety and Security team

When to use

Use this instruction to review a request to transfer a care indicated client to the Remote Claims Unit (RCU).

Instruction

Step 1

Review the party record in Eos, the client file and the ACC2222 Remote Claims Unit referral form.

Contact the branch manager to discuss if required.

Step 2

Consider whether all management options have been exhausted before deciding whether the client meets the criteria for the RCU. Contact the RCU manager with a recommendation as to whether the client should be transferred or not.

Step 3

Use the following table when the RCU manager, in consultation with the National Manager, Claims Management Network, reaches a decision.

If the decision is...	then...
to transfer the client	go to step 4
not to transfer the client	• refer the matter back to the branch manager with suggestions for the client's management plan • go back to the Managing care indicator clients process

Step 4

Inform the branch manager of the decision.

What happens next

The RCU staff complete the transfer process to the RCU

Go to Transfer ownership in Eos

Back to process map ↑

Transfer ownership in Eos

Responsibility

Branch manager

When to use

Use this instruction when the National Manager approves a request to transfer a client to the Remote Claims Unit (RCU).

Instruction

Step 1

Complete (or get the case owner to complete) an ACC29 File summary and overview form and upload it to the claim file along with all other relevant information.

Note: If the client has a physical file, send this to the RCU also. Or see Preparing, scanning and filing documents for VCF if you'd like to do it electronically.

Step 2

Open the client's active claim and click the 'To Department' magnifying glass icon.

Step 3

Navigate to and click on the 'Remote Claims Unit' department (page 2).

Step 4

Click the 'Reason' drop-down menu and select 'Requested from Branch/CC'

Step 5

Add any other applicable information to the 'Description' field and click 'OK'

What happens next

Repeat steps 2-5 for each of the client's active claims.

This process ends.

Back to process map ↑

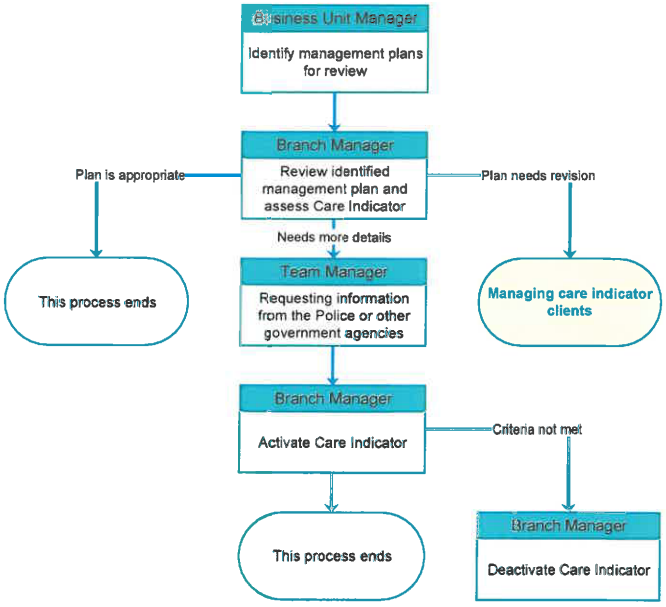
Reviewing care indicated clients

Branch managers use this process on the six month anniversary of when a care indicator was activated and every six months from the last review date. They update the client's management plan as appropriate and assess whether the care indicator is still required.

This process is also used when a management plan needs updating based on another incident involving the client.

Contact [redacted] Last review 01 Jul 2016 Next review 01 Jul 2017

Click on a shaded box for instruction details



Show all instructions

Identify management plans for review

Responsibility

Business Unit Manager

When to use

Use this instruction when you need to review the Care Indicator report for your office.

Instruction

Step 1

Log in to InFact and go to your Dashboard.

Step 2

Select 'Network' then 'Office Toolkit'.

Step 3

Click the 'Care Indicator Claims' tab then select your claim management office to generate the Care Indicator report for your office.

Step 4

Review the 'Update Overdue' column to find out which Care Indicator clients need their management plans reviewed.

What happens next

Go to Review identified management plan and assess Care Indicator.

Back to process map ↑

Review identified management plan and assess Care Indicator

Responsibility

Branch Manager

When to use

Use this instruction to review a management plan identified in the Care Indicator report, and assess whether the care indicator is still required on the client's profile.

Instruction

Step 1

For each identified client management plan, open the client's Eos record and:

- review the management plan entries, details of any contacts and any care notes
- note the details of each relevant party associated with the client's management.

Step 2

Contact each relevant party and have a discussion about the client's current management, whether it's still appropriate and whether it's still necessary.

Step 3

Update the client's management plan with details about each conversation you had.

The latest instructions for how to update a client's management plan can be found on the Sauce here: Activate, review and remove a client Care Indicator.

See also Add an indicator

Step 4

If the client's current management plan...	then...
is appropriate	• in the management plan, update the 'Management Plan Updated Date' and 'Management Plan Update By' fields • click 'OK' • this process ends
requires more information	• go to Request information from the police or other government agency
is no longer required as the client doesn't meet the care indicator criteria	go to Remove care indicator
needs revision	• discuss the required revisions with your team manager • go to Managing care indicator clients
needs revision and the client is VULNERABLE	• discuss the required revisions with your team manager and make the appropriate changes • in the management plan, update the 'Management Plan Updated Date' and 'Management Plan Update By' fields • click 'OK' • this process ends

Back to process map ↑

Requesting information from the Police or other government agencies

Responsibility

Team Manager

When to use

Use this to request background information on a client from the Police or other government organisations.

Step 1

Complete the Request for Information form and send it to the Health, Safety and Security team,

Step 2

When you receive the information back from the Health, Safety and Security team, review and assess it to see if the criteria has been met for activating the Care Indicator.

Step 3

Make recommendations to the Branch Manager as to whether to activate or deactivate the Care Indicator.

What happens next

Go to Activate Care Indicator

Activate Care Indicator

Responsibility

Branch Manager

When to use

Use this instruction to activate the Care Indicator.

Step 1

If the criteria is...	then...
met	make a decision within 48 hours to activate the Care Indicator or update the management plan in Eos go to step 2
not met	• remove Care Indicator as the client doesn't meet the Care Indicator criteria • go to Deactivate Care Indicator

Step 2

After a decision has been made, delete and destroy all information and correspondence received from the Police or other government agencies.

What happens next

This process ends

Deactivate Care Indicator

Responsibility

Branch Manager

When to use

Use this instruction to remove a Care Indicator from a client's profile when you've decided the client no longer presents a risk to staff.

Before you begin

Ensure you have met the Criteria for removing the Care Indicator.

See also Guidelines for when to remove a care indicator.

Step 1

Navigate to the Indicator tab on the client's party record and click 'Edit'.

Step 2

Click the 'Care Status' drop-down menu and select 'Inactive'.

Step 3

Click 'Management Plan'.

Step 4

Click the 'Management Plan Update Type' drop-down menu and select 'Discharge'.

Step 5

Type the reason why the Care Indicator is being removed into the relevant field and click 'OK'.

What happens next

The General screen of the party record will now display the Care Indicator icon as being 'greyed out'. This will notify staff that the client has had an active Care Indicator but does not currently present as a risk.

All previous information of the client being a risk still remains in 'Indicators' in the Eos record.

This process ends.

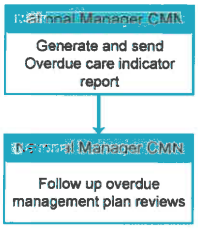
Back to process map ↑

Ensuring overdue management plan reviews are completed

The National Manager, Claims Management Network uses this process to ensure all overdue management plan reviews are identified and completed.

Contact [redacted] Last review 01 Jul 2016 Next review 01 Jul 2017

Click on a shaded box for instruction details



Show all instructions

Generate and send Overdue care indicator report

Responsibility

National Manager, Claims Management Network

When to use

Use this instruction in April and October to generate the 'Overdue care indicator report', which identifies clients with management plans that still need reviewing.

Instruction

Step 1

Contact BIAR and ask them to run the 'Overdue care indicator report' and send you the results.

Step 2

Using the report, note how many care indicated client management plans need reviews completed.

Step 3

Email the report and a notification of how many reviews are required to the relevant area leaders.

What happens next

The National Manager Claims Management Network will distribute tasks to the appropriate offices for actioning.

Go to Follow up overdue management plan reviews.

Back to process map ↑

Follow up overdue management plan reviews

Responsibility

National Manager, Claims Management Network

When to use

Use this instruction one month after the first 'Overdue care indicator report' was generated to check if any management plans still require review.

Instruction

Step 1

One month after the original 'Overdue care indicator report' was generated, request BIAR to run the report again. This will show any care indicator clients that have not had their management plans reviewed.

Step 2

Using the report, note how many care indicator client management plans still need reviews completed.

Step 3

Email the report and a notification of how many reviews are required to the appropriate area leaders.

What happens next

Liaise with the area leaders to ensure that all care indicator client management plans are reviewed and up to date.

This process ends.

Back to process map ↑

Guidelines for making a client management recommendation

Contact [redacted] Last review 01 Jul 2016 Next review 01 Jul 2017

Introduction

These guidelines clarify the management options available for clients who have behaved inappropriately and aim to help staff when completing an ACC159 Client risk profile summary (108K).

When to use

Use these guidelines to help you make a recommendation to your team manager for how a client who has behaved inappropriately is managed.

Note: If your team manager is unavailable, escalate to your branch manager.

Management options summary

There are six options to recommend for the management of a client who has behaved inappropriately, shown in the diagram below:

[insert finalised pic]

Warning

The following behaviors can warrant a client being warned:

- made racist, sexist, or other offensive or obscene comments
- enters the office and is clearly under the influence of alcohol, drugs, or solvents
- client contacts you outside of work hours.

Notes:

- If the behavior persists over time it may warrant activation of the care indicator on the client's profile.
- Scenarios that don't warrant a warning should still be noted on the client's profile as a claimant care note. For example:
  - associations with gangs or dangerous people,
  - current, active, or pending criminal charges

Activate care indicator

A care indicator is used on a client's record to signal to all staff that they need to be careful when dealing with the client, and should look up their management plan before proceeding. Care indicators are always part of the recommendation when further management options are required.

In the following scenarios you might recommend to your team manager that a care indicator is activated on the client's profile:

- the actions we're taking on their claim are known to have caused, or are expected to cause a significantly negative response from the client, eg cessation of weekly compensation
- they have a history of violence or aggressive behaviour
- they've made threats previously against ACC, ACC staff or agents acting on ACC's behalf
- they send abusive, threatening or offensive material in the mail
- they have threatened to harm themselves or others
- they've been abusive or verbally threatening
- they've been arrested, convicted or had court orders relating to violent behaviour
- they contact you outside of work hours.

Order security

If the client demonstrates behaviour which presents a serious risk to either ACC staff or providers, you might recommend to your Team manager that security is arranged for their meetings.

Clients who may require security would demonstrate behaviours such as physical violence or threats of violence against ACC staff, providers, or themselves.

Transfer to another branch

If a client has continued to demonstrate intimidating and/or offensive behaviour that is not significant enough to warrant a trespass order or transfer to the Remote Claims Unit (RCU), you might recommend to your Team manager that the client is transferred to another branch.

Branch transfers are often used when clients have a personal problem with their current case manager or branch reception.

Issue a trespass notice

- If a client displays any of the following behaviours you might recommend to your Team manager that the client is trespassed from your office (and other ACC or provider locations if necessary):
- they've been asked to leave the premises but are not doing so
- they've intimidated a staff member to the extent that they felt unsafe. This could be over the phone or face-to-face through written abuse or verbal abuse
- they deface or destroy property
- they've sexually harassed a staff member
- they're physically violent towards ACC staff, providers or suppliers

Transfer to the Remote Claims Unit (RCU)

If the client is demonstrating behaviour which creates genuine concern for the safety of ACC staff or providers, you might recommend to your Team manager that the client should be transferred to the Remote Claims Unit (RCU).

The following criteria must be met before a client is considered for transfer to the RCU.

Scenario 1:

All of the following have occurred:

- a trespass order is in place
- the client has demonstrated behaviour either in person, by mail or on the phone that threatens staff safety to the extent that genuine concerns are held as determined by management, including the National Manager, Health and Safety or Security Advisor
- all other reasonable options have been considered including the management of the client by another branch.

Scenario 2:

Information has been received from a reliable source, eg the Police or their doctor, to the effect that genuine concerns are held as determined by management, including the National Manager, Health and Safety or Security Advisor and all other reasonable options have been considered including the management of the client by another branch.

Scenario 3:

An incident has occurred or information has been received of such concern that the National Manager of Claims Management has immediately approved the client being transferred to the RCU.

Guidelines for when to remove a care indicator

Contact [redacted] Last review 01 Jul 2016 Next review 01 Jul 2017

Introduction

These guidelines aim to help with the decision whether to remove a care indicator from a client's profile when they are no longer a risk to staff or providers.

See also: WorkSAFE: Dealing with aggressive/dangerous clients.

When to use

Use these guidelines when you are reviewing a care indicator client and are unsure whether they should still have a care indicator on their profile.

Who can remove a care indicator

The decision to remove a client's care indicator rests with the branch/centre manager in consultation with their team manager and the Security Advisor.

Criteria for deactivating a care indicator

In making the decision to remove the indicator, the Branch/Centre manager must consider the following:

- Is the client still receiving support from ACC?
- How many times has the client visited the office since their care indicator was activated?

Note: If the client has not visited the office, it is not possible to state they are no longer a threat (or a potential threat) to the safety of ACC employees, unless there are some other mitigating factors.

- How have they behaved when they have visited the office?
- How does staff feel about interviewing the client?
- Has the action that was being undertaken on their claim (that may have caused a negative response) been completed? ie. Fraud Investigation, Prosecution, Cessation of Weekly Compensation, etc.
- Is there any factor why this client should (or should not) have an active Care Indicator?

Other issues to consider

- Has the client continued to demonstrate the unacceptable behaviour that led to the activation of the Care Indicator?
- What changes and/or improvements have there been to the client's behaviour?
- Is ACC's continued use of the Care Indicator fair and reasonable now? When evaluating what is 'fair and reasonable' staff should look at the client's current circumstances in an objective manner.
- Given that there has been a six month period since the last date of evaluation, is there a new strategy that could improve the relationship with the client?
    - Eg if the Care Indicator is a result of a higher then expected level of contact from the client, a communication strategy may improve the relationship. This can include limiting contact to emails and phone calls only, diarised contact from ACC to the client and vice versa, or the client could be asked to attend all meetings with a nominated support person, and so forth.

Activate, review and remove a Client Care Indicator

The Care Indicator is noted on a client's Eos profile, to let staff know that the client poses a potential threat to safety.

Contact [redacted] Last review 04 Oct 2016 Next review 04 Oct 2017

Activating the Client Care Indicator

Any member of staff can activate the Indicator, but they need to follow the below process.

Each time a client with an active Care Indicator does anything which has the potential to cause harm to ACC staff, the client's Care Indicator must be updated.

Criteria to activate

If two or more of these criteria are met

Clients who meet more than one of the following criteria are considered to pose a potential risk to staff safety, and therefore must have their Care Indicator activated:

- Have continued to demonstrate intimidating and/or offensive behaviour, ie body language and verbal dialogue has made staff feel unsafe.
- Been abusive, verbally or in writing.
- Made racist or sexist comments.
- The current actions being undertaken on their claim by ACC are known to have caused, or are expected to cause a significantly negative response from the client. For example, prosecution, fraud investigation, cessation of weekly compensation.

Note:
The extent that the client's behaviour or action was triggered by the behaviour, action or reaction of an ACC staff member, must be considered.

If one of these criteria are met

Clients who meet any one of the following more serious criteria are also considered a potential risk to staff safety and must have their Care Indicator activated:

- Have been, or are, physically violent (this unacceptable behaviour may not have occurred directly towards ACC staff).
- Have a history of violence or aggressive behaviour, have known convictions for violence.
- Made threats previously against ACC, ACC staff or agents acting on ACC's behalf.
- Intimidated a staff member to the extent that they felt unsafe through written abuse or verbal abuse (face-to-face or over the telephone).
- Exhibited homicidal ideation.

Individual roles when the Care indicator is activated

Staff member (the person who activates the Indicator)

If a staff member thinks a client's behaviour warrants having the Care Indicator activated on their Eos record, they should:

1. Discuss the specific client and the incident(s) that caused the concern, with their team manager. Base any request on the criteria to activate the Indicator.
2. Provide the team manager with all supporting evidence. (If the Care Indicator is activated, this evidence needs to be entered in Eos as a contact - to do this, select 'claimant care notes' from the contact drop-down list.)

Team manager

Team managers must use the criteria to activate the Indicator, when making a preliminary decision about whether or not to activate the Care Indicator on the client's Eos record.

If the preliminary decision is...	then...
yes	• ensure there is evidence within the client's claim to support the decision, ie the information must be current and the rationale for activating the Care Indicator must be reasonable and fair • ensure the Care Indicator box is activated in the client's Eos record. • within 24 hours, recommend the Branch/Centre Manager confirms the Care Indicator is activated.
no	• within 24 hours, recommend the Branch/Centre Manager does not activate the Care Indicator.

Branch/Centre Manager

- Ensure there is up-to-date evidence within the client's claim, that supports the decision.
- Within 24 hours, confirm or reject the team manager's preliminary decision.
- Email the Safety Partner [redacted] to advise that the client's care indicator has been activated.
- Ask the team manager to update the file.

Security Advisor

- Upon receiving notification from the Branch/Centre manager, check the claim to ensure:
  - the above process has been correctly followed
  - there is sufficient evidence to support the decision is documented.

How to activate the Indicator on Eos

If the Team manager needs to activate the Care Indicator box on a client's Eos file:

1. Navigate to the **Indicator** tab on the View Party Record screen.
2. Click **Add**.
3. Select the 'Care Indicator' from the dropdown list. Click **Yes**.
4. Select **Active** from the drop down list.
5. Enter the details of the incident resulting in the client being placed on the register.
6. Select the Care Category from the drop down list:
   - **Other** – (Category Three)
7. Click the **Management Plan** button.
8. Select **Initial** from the drop down list to update the Management Plan. Fill out all fields with the relevant information.
9. Click **OK.**

   The red flashing icon will now be displayed on the front general screen, and the client now has an active Care Indicator!

Reviewing the Client Care Indicator

Who reviews Care Indicators and why

Branch/Centre Managers must review the Care Indicators of their clients every six months – in April and October.

To help guide the review, they can run a Care Claimant Report for clients at their Branch.

They must discuss any findings with their team manager, the case manager, and the Security Advisor if necessary. For example, whether the client's behaviour has improved enough to warrant removing the Care Indicator.

Any decisions made should be recorded in Eos, and there is a process for removing a Care Indicator, as discussed below.

Keeping clients' information up to date, is a requirement of Principle 9 of the Privacy Act 1993.

How to do the review

Go into Eos, then:

1. Go to **Indicators**
2. Click **Edit**
3. Click on **Management Plan**
4. Select **Review** from the drop down list in the Management Plan Update Type

5. Fill out all relevant fields in Eos
6. Click **OK** when completed.

Transferring a client with a Care Indicator

The files of clients with active Care Indicators can only be transferred to another Branch with the approval of both:

- The Branch/Centre Manager of the branch receiving the file
- The Network Area Manager.

Removing a Client Care Indicator

Who removes it

As discussed above, the decision to remove a client's Care Indicator rests with the Branch/Centre Manager in consultation with their team manager and the Health, Safety and Security team's Safety Partner [redacted]

Deciding whether to remove

Branch/Centre Managers' decisions on whether to remove a client's Care Indicator, must be guided by the below criteria and issues.

Criteria to apply when looking to remove a Client Care Indicator

- Is the client still receiving support from ACC?
- How many times has the client visited the office since their Care Indicator was activated?

  Note:
  If the client has not visited the office, it is not possible to state they are no longer a threat (or a potential threat) to the safety of ACC employees, unless there are some other mitigating factors.
- How have they behaved when they have visited the office?
- How do staff feel about interviewing the client?
- Has the action that was being undertaken on their claim (that may have caused a negative response) been completed? Ie fraud Investigation, prosecution, cessation of weekly compensation, etc
- Is there any factor why this client should (or should not) have an active Care Indicator?

Other issues to consider

- Has the client continued to demonstrate the unacceptable behaviours that led to the activation of the Care Indicator?
- What changes and/or improvements have there been to the client's behaviour?
- Is ACC's continued use of the Care Indicator fair and reasonable now? When evaluating what is 'fair and reasonable' staff should look at the client's current circumstances in an objective manner.
- Given that there has been a six month period since the last date of evaluation, is there a new strategy that could improve the relationship with the client?
  - Eg if the Care Indicator is a result of a higher then expected level of contact from the client, a communication strategy may improve the relationship. This can include limiting contact to emails and phone calls only, diarised contact from ACC to the client and vice versa, or the client could be asked to attend all meetings with a nominated support person, and so forth.

How to remove the Indicator

Clients that are deemed to no longer pose a risk to staff safety must have their Care Indicator removed. This needs the permission of the Unit Manager.

To remove the Care Indicator, in Eos the Branch/Centre Manager must:

1. Navigate to Party Record then Indicator tab
2. Click **Edit**
3. Select **Inactive** for the Care Status
4. Click on **Management Plan**
5. From the Management Plan Update Type select **Discharge**
6. Enter all details
7. Click **OK**.

The General screen of the Party Record will now display the Care Indicator icon as being 'greyed out'. This will notify staff that the client has had an active Care Indicator but does not currently present as a risk.

All previous information of the client being a risk still remains in Indicators in the Eos record.

Managing Care Indicators

The purpose of the Care Indicator is to ensure that staff are notified through the Eos system that a client they are about to interview or meet with has been identified as exhibiting behaviours or actions that ACC considers pose a potential threat to the safety of ACC employees and/or service providers. The care indicator has been designed to be used as a notice for staff to ensure they fully assess the situation before proceeding to engage with the client. For example, if a client has an active care indicator they can only be met by appointment, in an interview room with CCTV and must have a colleague, service provider or security guard present.

Criteria for activating the Care Indicator

It is important that staff adhere to ACC's policy and only activate the Care Indicator in limited circumstances. That is, to ensure that the Care Indicator is only used in situations where there is sufficient and current evidence to consider a real and imminent risk to staff safety exists.

Note: The Health and Safety at Work Act 2015 defines the term 'hazard' as *'includes a person's behaviour where that behaviour has the potential to cause death, injury, or illness to a person (whether or not that behaviour results from physical or mental fatigue, drugs, alcohol, traumatic shock, or another temporary condition that affects a person's behaviour)*

Criteria:

Clients who meet **more than one** of the following criteria are considered to pose a potential risk to staff safety, and must have their Care Indicator activated:

- Have continued to demonstrate intimidating and/or offensive behaviour (e.g. body language and verbal dialogue has made staff feel unsafe).
- Been abusive, verbally or in writing
- Made racist or sexist comments
- The current actions being undertaken on their claim by ACC are known to have caused, or are expected to cause a significantly negative response from the client. For example, Prosecution, Fraud Investigation, cessation of Weekly Compensation, etc.

Note: The extent that the client's behaviour or action was triggered by the behaviour, action or reaction of an ACC staff member, must be considered.

Clients who meet **any one** of the following more **serious criteria** are also considered a hazard and must also have their Care Indicator activated:

- Have been or are physically violent (this unacceptable behaviour may not have occurred directly towards ACC staff)
- Have a history of violence or aggressive behaviour, have known convictions for violence
- Made threats previously against ACC, ACC staff or agents acting on ACC's behalf
- Intimidated a staff member to the extent that they felt unsafe through written abuse or verbal abuse (face-to-face or over the telephone)
- Exhibited homicidal ideation

Making the decision to activate the Care Indicator

Activating a client's Care Indicator and complying with the ACC Safety Rules are steps that must be taken by ACC employees in order to minimise the potential for this hazard to cause harm.

Any ACC staff member can identify any client as meeting the criteria for activating the Care Indicator in their Eos Record. However, that staff member must then take the following actions:

1) Discuss the specific client, and the incident (s) that caused the concern with their Team Manager. The staff member must have a clear rationale for why they consider the clietnt meets the criteria for having the Care Indicatior activated in their Eos record.
2) Provide the Team Manager with all supporting evidence. If the decision is to activate the Care Indicator, this information will be entered in the claim as a contact (select the reason from the contact drop down list as 'Claimant Care Notes').
3) Team Managers have the delegated authority to make a preliminary decision concerning the appropriateness of activating the Care Indicator. ***The decision must then be confirmed by the Branch/Centre Manager.***

Team Manager's Role

Make a preliminary decision concerning the appropriateness of activating the Care Indicator on the client's Eos Record;

If the preliminary decision is yes:

- Ensure there is evidence within the client's claim to support the decision (i.e. the information must be current and the rationale for activating the Care Indicator must be reasonable and fair).
- Ensure the Care Indicator Box is activated in the client's Eos record.
- Within 24 hours recommend to the Branch/Centre Manager that the decision be confirmed.

If the preliminary decision is no:

- Within 24 hours recommend to the Branch/Centre Manager that the decision is that the client's Care Indicator is **not** activated.

Branch/Centre Manager's Role

- Ensure there is current evidence within the client's claim to support the decision
- Within 24 hours, the Branch/Centre Manager must confirm the Team Manager's preliminary decision.
- Email the Security Advisor to advise that the client's care indicator has been activated.

Security Advisor's Role

- Upon receiving the notification from the Branch/Centre manager, check the claim to ensure the above process has been correctly followed and sufficient evidence to support the decision is documented.

How to Activate The Care Indicator

To activate the Care Indicator box the Team Manager must:

1. Navigate to the **Indicator** tab on the **View Party Record** screen.
2. Click **Add**.
   Result: The 'Select Indicator' pop-up box appears.
3. Select the 'Care Indicator' from the dropdown list. Click **Yes**.
   Result: The **Add Care Indicator** screen displays.
4. Select **Active** from the drop down list.
5. Enter the details of the incident resulting in the client being placed on the register.
6. Select the Care Category from the drop down list:
   a. Other – (Category Three)
7. Click the **Management Plan** button.
   (Result: The **Add Management Plan** screen displays.)
8. Select **Initial** from the drop down list for the Management Plan Update Type

(i) Management Plan Update Comments:

Enter all relevant details in regards to the client in here. This should include:

- Any issues that staff should be aware of if they were to be contacted by the client either by phone or at a branch.
- Any safety issues pertaining to the client.
- Any other information that may be useful for any staff member or external provider when meeting or communicating with the client.

(ii) Management Plan Updated Date

- Enter in the date it was updated

(iii) Management Plan Update By

- Enter the name of the person who updated it

(iv) Tick the appropriate boxes to indicate how the client can communicate with staff

- **Allow Communication by Phone**
- **Allow Communication by Mail**
- **Allow Communication in Person**
- **Allow Communication by Email**

(v) Communication Comments

- Detail who the client can communicate with eg: *ISC please advise client that he can only communicate with RCU staff and to ring on 0800 158 931 and then close the call*

(vi) People to Communicate With

- Detail the people who the client can communicate with eg: *Can only communicate with the team manager from the Masterton branch*

(vii) Trespass Notice

- Select the 'Yes' radio button next to **Trespass Notice** field, if applicable
- An additional Trespass Notice field displays on the **Add Management Plan** screen.

(viii) Trespass Notice Start Date

- Enter the date the trespass notice was served on the client

(ix) Trespass Notice Finish Date

- Enter the date for 2 years after the date the trespass notice was served, this is the finish date

(x) Trespass Notice Comments

- Enter the branch(es) where the client is trespassed from and where the original endorsed copy is held

(xi) Click "OK"

- The red flashing icon will now be displayed on the front general screen.

The client now has an Active Care Indicator

Updating the Care Indicator

Each time a client with an active care indicator threatens ACC staff or does anything which has the potential to cause harm to ACC staff, the client's Care Indicator must be updated. This can be completed by most ACC network staff.

To update the Care Indicator:

1. Go to **Indicators** in the Party File
2. Click **Edit**
3. In the "Details" box enter all relevant information of the latest incident, this should include any changes in behaviour and safety issues staff and providers should be aware of.
4. Click **OK**

The client's Care Indicator has now been updated to include the latest incident.

This incident can also be entered as a contact by using 'Claimant Care Notes' on the contacts tab

Click on **History** if you wish to view all incidents relating to that client.

Reviewing the Care Claimant Report

The Care Indicator policy requires ACC to check every six months whether a client still warrants the application of the care indicator. In addition the Branch/Centre Manager is accountable for reviewing the details of clients in their branch with active Care Indicators every six months – March and September.

Clients must have their Care Indicator removed when it is believed that the client no longer poses a risk to staff safety and the Unit Manager gives their approval for the client to have the care indicator de-activated..

Below is the pathway to the dashboard reports in In Fact

- Sensitive Claims: In Fact > SCU > BIAR Development > Care Ind Claims
- Network: In Fact > Network > Office Toolkit > Care Indicator Claims
- CPSS: In Fact > CPSS > Care Indicator Claims

The review must:

- Fully assess the need for the continuation of ACC's use of the Care Indicator for each client. This evaluation must include discussions with the current Case Manager, Team Manager, and a full review of the client's current circumstances. Questions that must be asked and answered reasonably include;
    - Has this client continued to demonstrate the unacceptable behaviours that led to the activation of the Care Indicator?
    - What changes and/or improvements have there been to the client's behaviour?
    - Given that there has been a six month period since the last date of evaluation, what other strategies can be implemented by ACC that may improve/enhance this relationship? E.g. if the Care Indicator is a result of a higher then expected level of contact from the client, a communication strategy may improve the relationship. This can include limiting contact to emails and phone calls only, diarised contact from ACC to the client and vice versa, or the client could be asked to attend all meetings with a nominated support person, and so forth.
    - Is ACC's continued use of the Care Indicator fair and reasonable now? When evaluating what is "fair and reasonable" staff should look at the client's current circumstances in an objective manner.
- Confirm in the Health and Safety Audit that the review has been completed (on the Health and Safety Quarterly Report).

How to review the Care Indicator

To review a client the Care Indicator:

1. Go to **Indicators**
2. Click **Edit**
3. Click on **Management Plan**
4. Select **Review** from the drop down list in the Management Plan Update Type
5. Follow the steps from "**To activate the Care Indicator box the Team Manager must:**" from 8 (i) – (xi) in the Management Plan Update Comments start with *'Six monthly review……'*
6. Click **OK** when completed.

Note: Reviewing a client's Care Indicator is a requirement of Principle 9 of the Privacy Act 1993. Specifically, ACC must ensure that its client information is always up to date and accurate. For instance, continuing to approve the use of a client's Care Indicator based on an incident from five years ago, without any recurrences since, is breaching ACC's obligations under the Privacy Act.

Criteria for Inactivating the Care Indicator

The delegation for removing a client's care indicator rests with the Branch/Centre Manager in consultation with the Team Manager and if necessary, the Security Advisor.

The criteria for removing a client's Care Indicator are that they no longer justify having the Care Indicator activated in their Eos Record.

In making that decision the Branch/Centre Manager must consider the following factors:

- Is the client still receiving support from ACC?
- How many times has the client visited the office since their Care Indicator was activated?

Note: If the client has not visited the office, it is not possible to state they are no longer a threat (or a potential threat) to the safety of ACC employees, unless there are some other mitigating factors.

- How have they behaved when they have visited the office?
- How do staff feel about interviewing the client?
- Has the action that was being undertaken on their claim (that may have caused a negative response) been completed? i.e., Fraud Investigation, Prosecution, Cessation of Weekly Compensation, etc
- Is there any factor why this client should (or should not) have an active Care Indicator?

How to remove the Care Indicator

Inactivating the Care Indicator on a client's Eos record removes the client from the Care Claimant Report. The delegation for inactivating the Care Indicator rests with the Branch/Centre Manager in consultation with the Team Manager and then approval from the Health, Safety and Security Team.

To inactivate the Care Indicator the Branch/Centre Manager must discuss with the Team Manager and Case Manager if necessary why they consider the client no longer meets the criteria defined in above and, if possible, provide any supporting evidence.

The Branch/Centre Manager must:

Navigate to the Indicator tab on the Party Record

1. Click Edit
2. Select Inactive for the Care Status
3. Click on Management Plan
4. From the Management Plan Update Type select Discharge
5. Enter all details
6. Click OK

The **General** screen of the **Party Record** will now display the Care Indicator icon as being 'greyed out'. This will notify staff that the client has had an active Care Indicator but does not currently present as a risk.

All previous information of the client being a risk still remains in Indicators in the Eos record.

Transferring a Care Indicated Client between Branches

The files of clients with an active Care Indicator are not to be transferred to another branch to be case managed without the agreement of:

1. The Branch/Centre Manager of the branch receiving the file; and
2. The Network Area Manager.

Privacy and Documentation

Privacy Act

Clients who have the potential to threaten the safety of ACC employees and/or service providers are considered to be a significant hazard, in terms of the Health and Safety in Employment Act 1992.

The ability to activate a client's Care Indicator is subject to the provisions of the Privacy Act 1993. It is personal information about a client collected for the lawful purpose of minimising the potential for an identified hazard to cause harm.

The application of the Privacy Act to Care Indicators is discussed below:

The provisions of *Principle 3* of the Privacy Act mean:

- If it is possible to do so without escalating the situation or without endangering the safety of any ACC employee, the client is to be advised that their behaviour is unacceptable and that the incident will be recorded on their claim file. This advice can be in writing or by telephone, and must clearly outline the reasons why ACC is taking the action. It is important to inform the client about any consequences that may occur, should the inappropriate behaviour continue (e.g. the Police will be called, a trespass order may be issued and so forth), and that ACC will evaluate the situation in six months time to consider if the situation has improved.

The provisions of *Principle 5* of the Privacy Act mean:

- ACC staff should take demonstrably reasonable steps to safeguard information against loss and access, use, modification or disclosure except as specifically authorised by ACC.

You must not disclose the names of clients with active Care Indicators to any person or organisation external to the ACC Group of Companies without the prior approval of the National Manager Health and Safety
The only exception being that:

Service Providers are to be advised prior to their initial contact with a client of:

- any threatening or aggressive behaviour that ACC has observed that client exhibit; and/or
- any diagnosed mental condition the client has which is likely to make them aggressive or violent

The provisions of *Principle 6* of the Privacy Act mean:

- Any and all readily retrievable personal information that ACC holds on a client is to be disclosed to that client, upon request.

  You must disclose information on the client's file if they request it, including information concerning any threatening or aggressive incident. However there may be a basis not to disclose to a client that the Care Indicator has been activated if ACC considers that releasing this information may result in some one being harmed. Guidance should be sought from the ACC Privacy Group if it is intended to withhold this information.

The provisions of *Principle 7* of the Privacy Act mean:

- The client can request to have the information concerning the incident corrected, this must be done in accordance and consistent with ACC's correction policy. ACC can consider whether or not this is appropriate. Where ACC decides that a correction is not warranted (i.e. the incident record is deemed to be a correct representation) the client may instead provide a "statement of correction". This is an opportunity for them to outline their view of the incident. The statement of correction must be attached to the document that the client has raised a concern about so that it can be read in conjunction with ACC's view.

  Below is the link to CHIPS which further explains the correction process:

  http://thesauce/team-spaces/chips/clients/privacy--client-rights/process/managing-a-client-s-request-to-change-personal-information/index.htm

The provisions of *Principle 8* of the Privacy Act mean:

- ACC must ensure that the retention of the client's name on the Care Claimant Report is justifiable by the latest information on that client. i.e. the information must be accurate, up to date, complete, relevant and not misleading.

  Client names can only be added to the list if the client meets the criteria and there is current evidence within their claim to support and /or justify their addition to the list.

  The Care Claimant Report must be reviewed at least every six months by the Branch/Centre Manager who must re-evaluate the client's circumstances, and record that they have done so.

The provisions of *Principle 9* of the Privacy Act mean:

- ACC must not keep information about the "potential risk" of a client on the Care Claimant Report for longer than required for purposes of making the necessary decisions to protect staff.

The Care Claimant Report must be reviewed at least every six months by the Branch/Centre Manager who must record that they have done so.

The provisions of *Principle 10 & 11* of the Privacy Act mean:

- Staff must not disclose to any person or organisation the existence of the Care Claimant Report or the clients named on it other than for purposes of maximising the safety of ACC staff.

  Disclosure within the ACC group of companies must be limited to those people who may interact with the client or need to know within the context of their job. **Note:** The Police may request client information if an offence has been committed against ACC staff or property. All liaisons with the police will be through the National Manager, Health and Safety. Evidence of the incident that lead to the Care Indicator being activated must be on the client file.