19 January 2015

Lee M
fyi-request-3423-f9d6405e@requests.fyi.org.nz

Dear Lee M

Official Information Act Request

In an email dated 27 November 2015 to Hon Nikki Kaye you asked a number of questions under the Official Information Act 1982 (the Act) about ACC files and the ACC filing system. Hon Kaye's office forwarded this request to ACC for a response. Your questions and ACC's corresponding responses are set out below.

1. *How many different claimant file/record naming options are there in the ACC's EOS computer system in which information about individual claimants can be stored, including but not limited to personal, health and employment history, individual claims history, communications between the ACC and the individual claimants (regardless of method), communications between the ACC and its internal staff, communications with the ACC's legal team and external legal organisations, communications with treatment providers, communications with vendors, etc?*

There are two *places* where information and communications records can be created, stored and managed in Eos; these are at **party** and/or **claim** level:

- **Party** is the term for a person (e.g. claimant), group of people or an organisation associated to a claim. These records provide relevant information in regards to the party and general interactions with them. Party records are named after the individual, group or organisation they pertain to.

- **Claim** records provide a single view of the information for a claim and how ACC is managing it. Copies of all communications sent and received about a claim are stored, or accessed from the Virtual Claim Folder, within Eos. Claim records are named after the ACC-generated number of the claim they pertain to. Information contained in the claim record includes:
    - general details such as cover status, claim type, case ownership
    - the individual plan, entitlements and supporting activities
    - details of the accident and injury caused
    - medical diagnosis
    - employment details
    - any special indicators
    - payments made on the claim
    - any contact with the client and/or associated parties including documents issued or received.

Documents and Contacts can be stored at just a party level or both claim and party level. In most cases, the document would relate specifically to the claim so it would be created and stored on the claim record.

We note that some historical claim records will have a physical file that has been archived rather than virtualised (i.e. electronically uploaded).

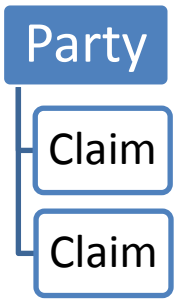
2. *I am aware that two names given by the ACC to files/records that are created and stored in its EOS computer system are "claim file" and "party status (or level) file", however, I am wanting to know the names, hierarchy [sic] and architecture of the many other file name options that the ACC uses to create files for individual claimants and their individual claims. (Possibly a diagram can also be provided).*

As noted above, Claim and Party level are not names given to files or records stored in Eos. They are the two distinct areas within in Eos where an individual client, provider or employer's information is filed. The file name options that ACC uses to create files for individual clients and their individual claims are therefore either:

a. the individual's full name, and/or

b. the number that ACC allocates to each new claim.

Every claim is associated to the individual claimant (party) record that the claim relates to as shown in the following diagram:



3. *Is a "party status (or level) file" stored in the ACC's EOS computer system accessible by any external organisation including Fairway Resolution Limited?*

Third Party Administrators (TPAs) who are participating in a service for external management of claims have very limited access to Eos. They can only view and access claims they manage, and this access is enabled by ACC using strict criteria. They also have very limited access to view party information. These TPAs are unable to search other claims related to the individual they are managing, or any other persons.

FairWay Resolution Services Limited (FairWay) does not have access to ACC's Eos system, or access to claim or party records. FairWay is an independent company that has its own software applications to create and view its records. FairWay also confirmed this in an email dated 16 October 2015 when they stated that: "FairWay does not have electronic access or connectivity to any of ACC's electronic records, such as the Eos print claim file".

4. *Why do ACC claimants have difficulties – in some cases this is publicly reported to have taken great persistence over long periods of time – in getting the ACC to simply provide copies of "party status (or level) files"?*

The information provided by ACC is directly related to an individual's request. Most clients request information about their current managed claim. As mentioned above, documents relating specifically to a claim are allocated to the Claim record so only this is provided. If clients request party level files, these will be provided.

5. *Why does the ACC not publish the file/record naming options to assist claimants when they want to make Privacy Act or Official Information Act requests? (If such a list was available, the claimant could then specify which file/record they would like a copy of).*

Thank you for your suggestion but there is no such list to make available. Clients generally ask for information related to their claim and will specify the associated claim number. Alternatively they ask for personal information that ACC holds about them, or official information about a specified ACC policy or procedure, or data that ACC holds.

6. *When claimants request "all" information that the ACC holds about them and their claims, why does the ACC only provide copies of the records held in the ACC's "claim file" stored in its EOS computer system? (In other words, why does an ACC claimant need to make specific and sometimes even separate requests for "all" files held by the ACC, and name those individual files, when most of the file/record names are not known to claimants)?*

The information a client is provided will depend on the request that they make. Eos has been ACC's repository for claim information since 2007, therefore if a client requests information ACC holds about their current or recent claim or claims, this will generally come from Eos.

There are some exceptions. For example, historic claim information may not have all been scanned into Eos. This means that these physical files will be sourced from archives before responding to a request. In addition, payment transactions are managed through separate systems and Eos accesses a sample of the information for internal use. Ultimately however, the source of the information provided is directly related to the individual's request. ACC will clarify any details with the requestor if their request is unclear.

7. *Why does the ACC need to have so many different file/record names, and create and store information about individual claimants and their individual claims in so many differently named files/records?*

As set out above, ACC stores information about clients under their name and under the claim number of each claim lodged. A client will have one party record, but may have many different claim records. ACC receives approximately 1.84 million claims a year, so it is practical to name and store each file according to the claim number allocated to it, and against the individual related to the claim.

8. *Do ACC claimants have a legislated right to access "all" information that the ACC holds about them irrespective of the file/record name assigned to that information and the name of the file/record that the information is stored under? If not, what information is not considered relevant and important and what is considered irrelevant and trivial, and what are the reasons for this?*

Principle 6 of the Privacy Act 1993 states where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled to obtain from the agency confirmation of whether or not the agency holds such personal information, and to have access to that information.

The application of this principle is subject to the provisions of Parts 4 (good reasons for refusing access to personal information) and 5 (procedural provisions relating to access to and correction of personal information) of the Privacy Act.

Accordingly, clients do have a right to access all information that ACC holds about them, subject to the reasons set out in sections 27-29 of the Privacy Act that enable information to be withheld from release. Redactions to personal information are only made in accordance with these sections of the legislation and the reasoning must be explained to the requestor. An assessment with regard to redaction is done on a case by case basis when reviewing the information relevant to the request.

9. *Please provide me with a copy of ACC's policies and procedures, or guidelines, in relation to Privacy Act and Official Information requests.*

The documents listed below are enclosed with this request:

a. Access policy
b. Requests for personal information
c. Differences between personal and health information
d. Requests for full client copy files
e. Requests for call recordings
f. Requests for client emails
g. When to withhold personal information
h. Examples of declining personal information requests
i. Preparing client information in a CIT
j. Official information requests policy
k. Official information requests
l. When to withhold information
m. Timeframes for responding to official information requests
n. Examples of declining official information requests
o. Manage requests for personal information from insurers
p. Responding to a request for official or personal information.

Please note that the staff 'contact' name on each of these policies has been redacted pursuant to section 9(2)(a) of the Act to protect the privacy of these staff.

There are also policies on ACC's website which relate to this request but are not enclosed as they are publicly available (as per section 18(d) of the Act). You can access these policies at the following web addresses:

- ACC's privacy policy: http://www.acc.co.nz/privacy/privacy-notice/WPC120319
- Request access to your personal and health information: http://www.acc.co.nz/privacy/privacy-notice/WPC120331
- Requesting official information: http://www.acc.co.nz/publications/index.htm?ssBrowseSubCategory=Requesting official information.

Invitation

We note that your questions seem to indicate confusion about the layout and compilation of ACC files in Eos. As suggested to you previously, you are welcome to arrange a visit with your local ACC branch to view Eos in operation (as per section 16(c) of the Act). This should help to alleviate any misconceptions you have about ACC's filing systems. Please talk to your case manager to arrange this.

ACC is happy to answer your questions

If you have any questions about the information provided, ACC will be happy to work with you to answer these. You can contact us at GovernmentServices@acc.co.nz or in writing to *Government Services, PO Box 242, Wellington 6140.*

You have the right to complain to the Office of the Ombudsman about our reply to your request. You can call them on 0800 802 602, 9am-5pm on weekdays, or write to *The Office of the Ombudsman, PO Box 10152, Wellington 6143*.

Yours sincerely

Government Services

Government Services

Enc. 16 x ACC policy documents

Access policy

People have the right to access their personal information and personal health information (personal and health information), and also to correct that information.

Personal information is about an identifiable individual; health information is information about the health of an individual.

The right of access to personal and health information is central to giving the individual control over their information.

Contact [redacted] Last review 30 Nov 2015 Next review 30 Nov 2016

Principles for clients' access to personal or health information

To ensure we are fulfilling our obligations on access, we need to follow the principles below:

- We need to know clients' rights to access their own personal and health information, and be able to distinguish these requests from requests for official information.
- We need to be considerate and helpful when responding to clients' requests for personal and health information.
- We need to know the timeframes and processes for responding to access requests, and the criteria for determining whether a client's request needs to be transferred to another agency.
- We need to know the grounds for refusing access to personal and health information.
- We need to ensure that clients do not gain access to other clients' personal and health information.
- We need to understand the link between clients' rights to access their personal and health information, their right to correct that information, and the requirement for ACC to advise a requestor about this right when given access to personal and health information.

The legislative framework

ACC's access policies are bound by three key pieces of legislation:

- the Privacy Act 1993
- the Health Information Privacy Code 1994
- the Accident Compensation Act 2001, including the Code of ACC Claimants' Rights. Right 7 of the Code provides for a claimant's right to privacy, which includes obligations for ACC to comply with all relevant legislation relating to privacy and for ACC to give access to ACC claimants (in keeping with legislation).

ACC collects two types of information – personal information and personal health information.There are differences between personal and health information and slightly different rules govern their collection, use, and disclosure.

The Privacy Act 1993 and the Health Information Privacy Code 1994 list 12 principles that must be followed for effective privacy management. Information Privacy Principle (IPP) 6 and Health Information Privacy Rule (HIPR) 6 relate to accessing personal and health information.

Back to top

Requirements when access to personal information is requested

Under IPP 6, where an agency holds personal information that can be readily retrieved, the individual has a right to:

- obtain confirmation whether the agency holds information about them
- obtain access to that information.

When access is given, the individual must be advised that correction of the information, under IPP 7, may be requested.

However, the right to access personal or health information is subject to the agency's rights to refuse access as stated in Part 4 of the Privacy Act (sections 27 to 29). The agency is also subject to the provisions of Part 5 of the Privacy Act (sections 33 to 45), which set out time requirements and other process requirements.

Key points for responding to requests for personal and health information

- Under the Privacy Act, there is a **presumption of access**. Unless there is a good legal reason not to, individuals must be given access to their personal and health information.

- **If we fail to respond to an access request, with no proper basis for that failure, we will be found to have interfered with a person's privacy** – so we must be on the alert for access requests and respond in a timely way.
- When exercising their right to access, **a person does not need to make their request using a particular format**. A request might be part of a letter of complaint. All communications from clients – including phone conversations/call recordings, letters and emails – must be carefully assessed for whether the client is requesting access.
- **Identification:** We need to be sure about the identity of the person making the request and that any personal and health information to which we give access is received only by that person or their authorised representative.
- **Representatives:** Under the Health Information Privacy Code, there are specific policies for access in relation to a deceased person's representative, parents and guardians of children and young persons under the age of 16, and where a person is unable to give consent or authorise a representative.
- **Children and young people have rights to access their personal or health information**, but where an individual is under the age of 16 there may be reasons for refusing access. Requests for access to children's or young persons' personal and health information also need to be considered under IPP 11/HIPR 11 – Disclosure – especially where a parent or guardian is making the request.
- A request for personal and health information (eg, information about the assessment of a person's levy obligations, or their medical certificates) can be made at the same time as a request for official information (eg, ACC's policies and procedures that led to an entitlement decision). **Official information requests must be treated as separate requests** and follow the operational policies set out for requests under the Official Information Act 1982.
- We must comply with the statutory response times for access. ACC must decide whether a request should be granted **as soon as reasonably practicable** and no more than **20 working days** from when the request was received. This response time includes the time for providing the information.
- **Extension of response time:** If a reply cannot be given within the 20 working days, we must notify the requestor of a need for an extension, setting out the reasons for the extension and of the person's right to complain to the Office of the Privacy Commissioner.
- **Urgent requests:** Where a person asks that their request be treated as urgent and gives reasons for the urgency, we must help them to get their information urgently.
- **Requests can be transferred:** If ACC does not hold the information, but knows it is held by another agency, we may transfer the request to that other agency **within 10 working days**.
- **Requests for access can be declined,** but only for reasons specified in the Privacy Act and Health Information Privacy Code. Some of these reasons include protecting another individual's rights to privacy or safety, preserving legal professional privilege, or not prejudicing the physical or mental health of the individual requesting access.
- **If ACC refuses to give an individual access to their information, or deletes information from documents, the individual must be given the reasons why.** They must also be advised of their right to ask the Office of the Privacy Commissioner to investigate and review the decision – as with any decision we make about privacy.
- **Access can be provided in different forms.** We should make the information available in the form requested by the person unless there is good reason for providing the information in some other way. A client might also be interested in inspecting their information at an ACC office, or having a summary of the contents, or having oral information.
- **ACC cannot charge for providing personal information.**
- When access is given, **we must also advise that under IPP 7/HIPR 7, that person may request correction of their information.**
- **We must help clients, especially when their requests are not clear, and always communicate in a timely and helpful way.**

Back to top

Requests for personal information

Contact [redacted] Last review 30 Jan 2015 Next review 30 Jan 2016

Introduction

The Privacy Act 1993 (Privacy Act) and the Health Information Privacy Code 1994 (Health Information Privacy Code) provide legislation for protecting individual privacy and managing personal and health information.

- The Privacy Act contains 12 Information Privacy Principles for collecting, accessing and releasing personal information
- The Health Information Privacy Code 1994 (2.08M) contains 12 Health Information Privacy Rules for collecting, accessing and releasing an individual's health information.

We must all understand these principles and rules when handling requests for the release of personal and health information. For more information see Differences between personal and health information.

Rules

Office of the Privacy Commissioner

The Office of the Privacy Commissioner is responsible for investigating complaints about the withholding or disclosure of personal information. Our Privacy team manages ACC's liaison with the Office of the Privacy Commissioner.

Who can request personal information?

Under the Privacy Act, only the client or a person with authority to act on their behalf may request information that we hold about a client.

Under the Official Information Act 1982 (OIA) the following parties may request information that we hold about a client:

- a third party administrator
- an insurance company assessing a related claim
- any other person or organisation.

If the request for personal information is from...	then treat it as a request under the ...
the individual concerned or their authorised representative	Privacy Act 1993
another individual	Official Information Act 1982
an organisation or government agency	

Requests from members of Parliament

We frequently receive enquiries from members of Parliament (MPs), or their electorate office staff, advising that they're acting on behalf of an ACC client or premium payer.

We don't normally require formal confirmation of the MP's advocacy role. If you're concerned about disclosing or releasing the information, contact the client to confirm the MP is acting on their behalf.

Requests from members of the New Zealand Police

We occasionally receive requests from the Police for information about clients. These should be referred to the Privacy Team who will respond direct to the Police.

If you receive a written request, please email it to the Privacy Team on privacy.officer@acc.co.nz.

If you receive a verbal request, advise the Police that they must make their request in writing (email or letter) and send it to The Privacy Officer, ACC, PO Box 242, Wellington 6140 or privacy.officer@acc.co.nz.

Under no circumstances should you disclose any information about the client. If you have any questions, please contact the Privacy Team.

Requests from insurance companies for client information

If you receive a request from an insurance company for a copy of a client's file(s), See Manage requests for client information from insurers.

Photocopying client files

You must complete the ACC6173 Information disclosure checklist (168K) if you photocopy any part of an ACC client file. See also Privacy check before disclosing information.

Charging for information

ACC cannot charge for providing personal information.

Response time

Under the Privacy Act, Section 40 we must make a decision on a request for personal information:

- as soon as reasonably practicable
- within a maximum of 20 working days after receiving the request.

Extension of response time

Sometimes you may need a time extension to respond to a request for personal information. Extensions are allowed where:

- large quantities of information are involved
- searching through large quantities of information will unreasonably interfere with ACC's operations
- you need to consult.

You may only make one request for an extension so you must be able to complete the response within the extended timeframe.

Formal notification of extension

You must formally notify the requestor about an extension of time within the 20 working days limit and include the:

- extension period required
- reason(s) for the extension
- advice that the requestor has the right to lodge a complaint about the extension with the Office of the Privacy Commissioner.

Transferring a personal information request

If we don't hold the requested personal information, but know another government agency that does, we can transfer the request to the other agency under the Privacy Act, Section 39. The transfer must be arranged within 10 working days of the date of receiving the request.

Releasing personal information

We must release requested personal information unless we have good reasons to withhold it. See the Privacy Act, Section 27 and Section 29.

Withholding personal information

If we have good reasons to withhold the information we may consider declining the request. See Examples of declining personal information requests.

Releasing only part of the requested personal information

Sometimes it's appropriate to release only part of the personal information requested, eg when the information identifies multiple individuals. The Privacy Act, Section 43 permits us to delete the part (s) of the document containing this information before releasing it. We must provide reasons for withholding any parts of the information.

The recipient must not be able to read any of the information that has been deleted.

We might also only provide part of the personal information requested if:

- we're satisfied, after consulting with the requestor's medical practitioner, that disclosure would be likely to affect the requestor's physical or mental health
- the request is frivolous or vexatious, or the information requested is trivial.

You must consult the Privacy team about any decision to decline a request based on it being frivolous, vexatious or trivial.

Differences between personal and health information

Contact [redacted] Last review 03 Aug 2015 Next review 02 Aug 2016

Introduction

The information we hold about individuals falls into two categories, **personal** and **health**. You must be able to distinguish between personal and health information as the content determines which legislation governs its release.

- Personal information is governed by the Privacy Act 1993
- Health information is governed by the Health Information Privacy Code 1994.

Rules

Privacy Act 1993

All ACC staff must be aware of and comply with the Privacy Act. The Act includes 12 Information Privacy Principles that cover the collection, management and release of **personal** information.

The Privacy Act applies to both public and private sector organisations and provides a legislated structure for:

- collecting personal information
- managing personal information
- handling requests for personal information.

We must ensure that we provide all reasonable assistance to anyone who wishes to request personal information about themselves.

Examples of requests made under the Privacy Act:

- A person asks for details about the assessment of their levy obligations for the last two years
- A dependent asks for details about the payments that ACC has made to them for the last year

Health Information Privacy Code 1994

The Health Information Privacy Code (the Code) includes 12 Health Information Privacy Rules (2.8M) that health agencies must follow to protect individual privacy. These rules cover the collection, management and release of **personal health** information.

The Code applies to all agencies providing health or disability services. ACC and accredited employers are defined as health agencies and are subject to the Code.

When referring to the **health** information of identifiable individuals used by a health agency, the Code works in conjunction with the Privacy Act.

Examples of requests made under the Health Information Privacy Code:

- A client requests a copy of the independence allowance assessment
- A client asks when their latest medical certificate expires

Requests for full client copy files

Contact [redacted] Last review 04 Aug 2015 Next review 04 Aug 2016

Introduction

A request for a full client copy file may result from one of the following processes:

- Responding to a request for official or personal information
- Receiving a review application
- Managing an appeal.

A centralised Client Information team (CIT) in the Dunedin or Hamilton Service Centre will prepare the full client copy file, if the request meets the CIT criteria below. In rare cases, a request for a full client copy file may require an email sweep.

Rules

The CIT is responsible for collating, printing and privacy checking the copy file.

Privacy checks

Always use an ACC6173 Information disclosure checklist (166K) when privacy checking the file.

If needed, a team leader or manager may request a second privacy check.

You may reuse an existing full client copy file for a new request. You only need to privacy check the documents added to the file since the last release.

Securing documents

Once a copy file request has been sent to CIT, case owners and review owners are responsible for advising CIT if there are any documents that they feel should be secured before CIT releases the file eg legally privileged documents or on rare occasions, documents that should not be disclosed to protect client safety.

CIT will send a general task at the beginning of their process requeting a 'Complete disclosure validation'. Any details about documents which the case owner/review owner feels should be secured or not released to protect client safety should be detailed in an email to the claims officer in CIT who is processing the request. CIT will review and secure any documents which are legally privileged before releasing the file, referring to the instructions found in securing documents in Eos [link] and will discuss with the case owner/review owner any other concerns raised.

See Information requests and legal professional privilege and Requests for personal information.

CIT criteria

A request **may** meet CIT criteria if it's for a **full copy of a claim file** (may include multiple claims) needed for either:

- a personal information request from the client or their authorised representative or advocate
- a formal review lodged by the Review Unit
- a statutory appeal lodged by ACC Legal Services.

A request does not meet CIT criteria if it's:

- to support assessment processes
- for a provider
- from an outside insurer
- for a partial client copy file or specific individual documents only

The following tables show which copy files are in or out of CIT scope.

Personal information requests

In scope	Out of scope
• Claims Management (CM) branches • Recover Independence Service (RIS) • National Serious Injury Service (NSIS) • Sensitive Claims Unit (SCU) • Treatment Injury Centre (TIC) • Hamilton Service Centre (HSC) • Dunedin Service Centre (DSC)	Remote Claims Unit

In scope	Out of scope
• Northern Service Centre (NSC) • Short Term Claims Centres (STCC) • Registration, Assessment and Weekly Compensation Centre (RAWC)	

Reviews

In scope	Out of scope
• CM branches • Recover Independence Service (RIS) • National Serious Injury Service (NSIS) • Sensitive Claims Unit (SCU) • Short Term Claims Centres (STCC) • Treatment Injury Centre (TIC) • Dunedin Service Centre • Hamilton Services Centre • Northern Service Centre • Elective Service Centre	reviews lodged by: • Remote Claims Unit • Office of the Complaints Investigator (OCI) • Overpayment Decisions Unit

Appeals

Remote Claims Unit appeals files are out of scope. All other appeals files are in scope.

Preparing copy files for personal information requests

A request for a client's full copy file must be from an authorised person but does **not** need to be in writing.

All SCU files must have a second privacy check.

Timeframes

The CIT has 20 working days to prepare the copy file. If an extension is needed the CIT must:

- send an extension letter to the requestor to let them know the number of days extended
- let the requesting business unit know.

For more information see Requests for personal information.

Providing the copy file

We prefer to provide a full client copy file to a client or their advocate on a password protected computer disk. The requestor may collect the disk from their nearest ACC office if they wish.

If the requestor wants a printed copy of their file we prefer them or their advocate to collect it from their local ACC branch or office.

If the requestor wants us to courier the information to them, you must let them know the risks and reconfirm the request by reading them the ACC6181 Receiving personal information by courier (127K) information sheet.

See also:

- FAQs about delivering personal information
- Privacy check before disclosing information.

Questions following release

The case owner (managed cases), or other appropriate person if the case has been actioned, is responsible for answering questions from the client or advocate about the content of personal information that we provide.

Preparing copy files for reviews

Timeframes

The CIT has **15** working days to prepare the copy file for a review.

Review owner responsibilities

The review owner is responsible for:

- advising CIT if there are any documents that they feel should be secured before CIT releases the file, eg legally privileged documents, or any documents they feel should potentially not be disclosed to protect client safety

- CIT will send a general task at the beginning of their process requesting a 'Complete disclosure validation'.
- any details about documents that the review owner feels should be secured or not released to protect client safety should be detailed in an email to the claims officer in CIT who will process the request.
- CIT will review and secure any documents that are legally privileged before releasing the file, referring to the instructions found in securing documents in Eos and will discuss with the review owner any other concerns raised
- printing and preparing a copy of the file for the reviewer and tagging relevant documents. Please note CIT does not check any documents for relevance, this is the responsibility of the review owner.
- providing the full client copy file to the reviewer, usually Fairway Resolution Ltd, within 20 working days of receiving the review application. See Timeframes for reviews
- providing the full client copy file to the client or their advocate, if requested.

CIT will enquire, with the validation disclosure task whether the full copy file on a password protected CD is required for the review owner to provide to the client or advocate. CIT will provide the CD to the review owner but the review owner must double-check the contents are for the correct client/claim before releasing it. Note that this is not a full privacy check, but a content check.

Communicating with review applicants

The CIT must **not** communicate with the review applicant. The relationship with the review applicant is between the review owner and the applicant.

Preparing copy files for appeals

We're **not** required to provide a full client copy file to the appellant, unless they request one.

Appeal files do **not** require an ACC252 Relevant documents schedule (115K). However, if re-using a review file for the appeal, you must **not** remove the schedule.

The case owner or manager is responsible for:

- telling CIT if there are any documents that should be secured before CIT releases the file, e.g. legally privileged documents, or any documents they should potentially not be disclosed to protect client safety.
- CIT then send a general task at the beginning of their process requesting a 'Complete disclosure validation'.
- any details about documents which the case owner/manager feels should be secured or not released to protect client safety should be detailed in an email to claims officer in CIT who is processing the request.
- CIT will review and secure any documents which are legally privileged before releasing the file, referring to the instructions found in securing documents in Eos and will discuss with the case owner/manager any other concerns raised.

Timeframes

The CIT should try to prepare the copy file within 15 working days of receiving the request. If they need more time, eg if a file is over 4000 pages, the CIT must notify Legal Services as soon as possible.

Other units must complete their tasks within five working days, eg preparing the Judge and ACC Counsel copies of the appeal file.

Judge and ACC Counsel files

We must provide **two** copies of the full client copy file for the appeal, one for the Judge and one for ACC's Counsel. The pdf file prepared by the CIT forms the base file for the Judge and Counsel copies.

The business unit is responsible for printing the base file and preparing the copies for the Judge and Counsel.

You must print and privacy check documents that have been secured in Eos and add these to the base file, as appropriate. The two files must be identical, except for legally privileged documents.

- The Judge's file must **not** include any legally privileged documents
- The Counsel file must include **all** documents, including legally privileged.

Providing the copy file

Legal Services is responsible for couriering the Judge's files to the Court. The CIT or relevant business unit must **not** send files directly to the Court.

Requests for call recordings

Contact [redacted] Last review 03 Aug 2015 Next review 02 Aug 2016

Introduction

ACC's Business Service Centre (BSC) and Inquiry Service Centre (ISC) record some phone conversations between ACC staff members and external parties. We do this for training purposes. All recordings are held for a short time in a system called NICE. We refer to these as call recordings.

Rules

Call recordings contain personal information and may be requested by the caller under the Privacy Act 1993. If requested, under Section 42 of the Privacy Act we'll either provide the requestor with:

- a copy, or an opportunity to come to the office and listen to the recording. See Section 42 (1) (c)
- a transcript of the recording as it relates to them. See Section 42 (1) (d)
- an excerpt or a summary of the contents. See Section 42 (1) (e).

Use Responding to a request for official or personal information when responding to requests for call recordings.

Before releasing a call recording you must ensure you've identified the correct requested call(s) and completed a privacy check and an ACC6176 Checklist for releasing telephone recordings (139K).

How to provide a call recording

If we provide the call recording we'll usually provide the full recording as a password protected sound file on a computer disk. If needed we may provide an unprotected sound file on an audio CD, or by email if requested.

Where we can't provide the full call recording, eg because it includes information about other people or information that we can't disclose, we'll supply a written, edited transcript. If the call recording is difficult to transcribe we may provide a written summary. In some cases, it may be possible to extract a copy of the relevant segment of a call recording.

Unprotected call recordings

An unprotected call recording is similar to a printed copy of someone's personal information. If you're asked to supply an unprotected file you must let the requestor know the risks of sending unprotected information by courier or email. See the ACC6181 Receiving information by courier (127K) information sheet and Risks associated with email communication.

Requests for client emails

Contact [redacted] Last review 02 Oct 2015 Next review 01 Oct 2016

Introduction

As all client emails should already be on the client's claim file, when a client asks for a copy of all the emails we hold about them we'll provide them with a full client copy file. In rare cases we may need to check other systems to verify that all emails about the client have been uploaded correctly to their file. This check is called an email sweep or an IT sweep.

Rules

A request for client emails is a request for personal information under the Privacy Act 1993 and the same rules and timeframes apply when you respond to these requests.

A request for client emails must be initiated by the client, their representative or advocate. It does **not** need to be in writing. You must consider each request on a case-by-case basis.

The Hamilton Service Centre Client Information team (HSC CIT) is responsible for running email sweeps for client emails, including requests from their provider if appropriate. Only the Centre Administration team leader and team manager are authorised to run a client email sweep.

The HSC CIT will **not** run sweeps for emails that aren't claim related, eg emails relating to ACC staff, client complaints, investigations, levies.

Criteria for email sweeps

Since January 2011 it has been policy to upload all client emails to Eos. For this reason, we only run email sweeps for emails sent or recieved between 1 January 2007 and 31 December 2010.

The client must have a specific reason for requesting the emails, eg they must specify that we haven't provided all the emails they think we should hold about them or ask us for specific emails that we haven't provided.

The request must also meet other CIT criteria.

What we'll provide

In response to a request for a copy of a client's emails we will:

- provide a copy of either:
  - a full client copy file, which includes the relevant emails
  - a full client copy file and the email sweep results
  - email sweep results only, if a full client copy file has recently been provided.
- only provide email sweep results that meet the agreed search parameters
- provide the information either on a password protected computer disk or as a printed file. For delivery options, see Privacy check before disclosing information
- only consider restoring archived emails from backup tapes if specifically requested.

Attachments

We won't release attachments found in email sweep search results as all claim related information and documents should be on the claim or party record.

However, if an attachment is obviously missing from the record the HSC CIT team leader must follow up with the case owner or relevant business unit.

Privacy checks

You must print and privacy check the relevant emails before providing a copy to the client. See Privacy check before disclosing information. The CIT is responsible for:

- ensuring that all the emails we provide relate to the correct client and claim
- identifying and removing emails that aren't relevant to the request
- removing details about other clients or information that is subject to legal privilege or can't be disclosed for other reasons. See Information requests and legal professional privilege and Requests for personal information.

Always use an ACC6173 Information disclosure checklist (166K) when doing the privacy check.

If needed, a team leader or manager may request a second privacy check.

If you identify any potential issues in the emails, we must still provide the information to the requestor but we may need an extension of time.

Email sweep results

You must load email sweep results onto the client file as a single pdf document. Do **not** upload emails individually.

When to withhold personal information

Contact [redacted] Last review 03 Dec 2015 Next review 02 Dec 2016

Introduction

We can only refuse someone's request to access information about themselves if:

- it's appropriate to withhold it under sections 27-29 of the Privacy Act 1993
- another Act states that ACC does not have to provide access to the information.

The following rules apply to requests for personal information from the person themselves, eg a client or their representative or guardian.

Rules

We must let the requestor know our reasons for withholding the information.

If you need to photocopy any part of a client's file, you must complete an ACC6173 Information disclosure checklist (166K). See Privacy check before disclosing information.

Grounds for withholding personal information

The following are the most relevant grounds under sections 27-29 of the Privacy Act for withholding personal information when a person requests information about themselves. For further guidance and examples, click on the relevant link.

We can withhold information under the Privacy Act when:

- releasing the information would:
  - prevent detection and investigation of criminal offences and the right to a fair trial - s27(1)(c)
  - endanger a person's safety - 27(1)(d) and 29(1)(c)
  - involve an unwarranted breach of someone else's privacy - 29(1)(a)
  - breach confidence where the information has been collected only for reasons to do with the individual's employment or to decide whether to insure the individual - 29(1)(b)
  - be contrary to the interests of a person under 16 years old - 29(1)(d)
  - breach legal professional privilege - 29(1)(f)
- the request is frivolous or vexatious or the requested information is trivial - 29(1)(j).

Releasing part of the information

Sometimes it's appropriate to release only part of the information requested, either by deleting it from a document, or by blacking it out so that it can't be read. This is called redaction.

Examples:

- When information identifies multiple individuals it may be appropriate to delete information about other people from the document before we release it
- When a client's medical practitioner advises that disclosing particular information would be likely to affect the client's physical or mental health.

The recipient must not be able to read any of the information that we remove.

Not sure what to do?

If you're still unsure after referring to the individual pages above, discuss the request with your team manager or contact a member of the Privacy group.

Examples of declining personal information requests

Contact [redacted] Last review 12 Aug 2015 Next review 11 Aug 2016

Introduction

We can decline a request for personal information in certain circumstances, eg to protect an individual's privacy and safety or to preserve legal professional privilege and the public interest. For more information see Requests for personal information and Responding to a request for official or personal information.

Examples

The following table shows reasons and examples of when we may decline a personal information request. If you're unsure whether to decline a request for personal information, seek advice from Government Services.

Reason for declining request	Example
The release would prejudice the maintenance of law, including the prevention, investigation, and detection of offences, and the right to a fair trial	A person seeks details of an investigation ACC is undertaking into their claims for home help. The examining officer withholds the information to ensure that the ongoing investigation is not compromised.
The release is likely to endanger the safety of an individual	An ACC client seeks a copy of their investigation file. The file contains information provided to ACC by an informant. There are good grounds for believing harm could come to the informant, and consequently we decide to withhold the information.
The release would cause unwarranted disclosure of the affairs of another person, or a deceased person	A person requests a copy of a provider invoice from their claim file. We decline to release a full copy of the invoice because it contains details for other clients as well as those of the requestor
The applicant is under the age of 16 years, and disclosure would be contrary to his or her interest	ACC receives a report on a child who is being treated for a sensitive claim. We decline to release the report as it includes comments regarding the client's unrealistic expectations for a timely recovery.
Disclosure would breach legal professional privilege	A solicitor, acting on behalf of an ACC client, requests a copy of a legal opinion that the branch office obtained from Legal Services regarding their claim. We decide to claim legal professional privilege on the opinion and therefore decline to release the legal opinion.
The information does not exist, or cannot be found	A person wants a copy of an old claim. We're unable to locate the claim file in our archives or in any branch office. After making all reasonable attempts to locate the claim, we decline the request because the information does not exist or cannot be found
The information is not held by ACC, and it is not known if any other government agency holds the information	A client has asked ACC what their blood type is. This information is not stored on their claim file, and we're not aware if any agency holds it. We decline the request

Preparing client information in a CIT

Latest changes 30/11/15: *Major updates to process, including dispatching steps split into a separate process and email sweep instruction delete and steps redistributed to other instructions.*

The Client Information team (CIT) uses this process to prepare a copy of a client's file in response to a request for personal information, or an application for a review or appeal hearing. Requests must meet CIT criteria and in rare cases, may include an email sweep.

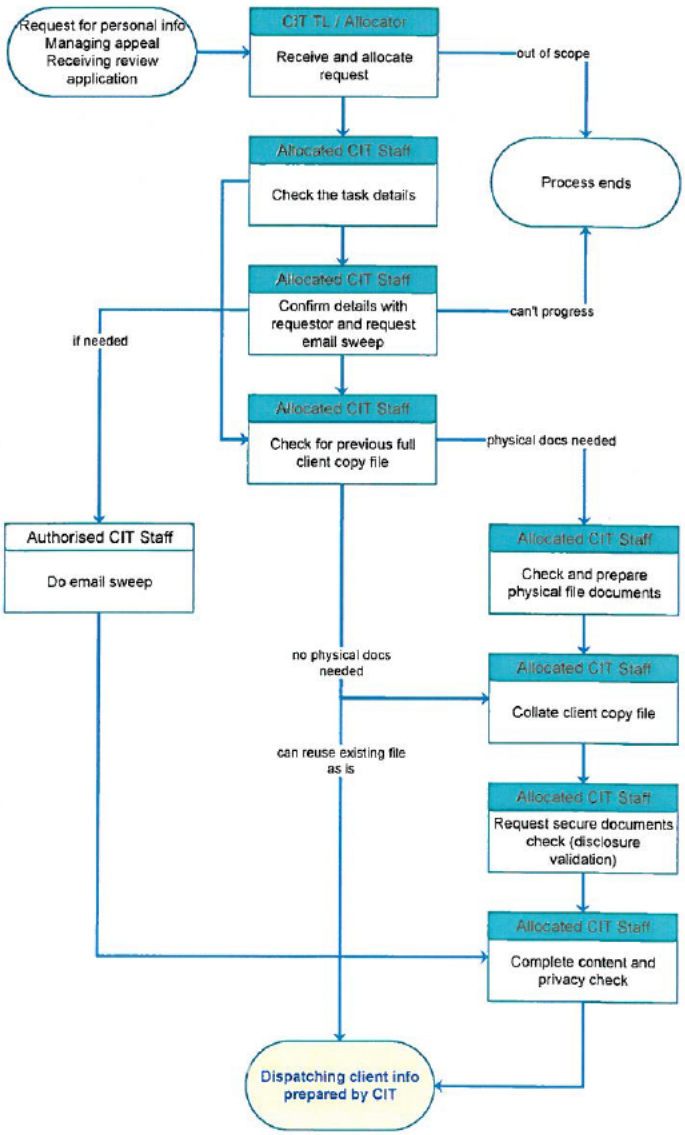
When the information has been compiled and the necessary content and privacy checks completed, the CIT will Dispatch the information.

See also:

- *Requests for personal information*
- *Requests for full client copy files*
- *Requests for client emails.*

Contact [redacted] Last review 30 Nov 2015 Next review 30 Nov 2016

Click on a shaded box for instruction details



Show all instructions

Receive and allocate request

Responsibility

CIT Team leader or allocator

When to use

Use this instruction when you receive one of the following tasks in the Client Information team (CIT) 'Client Information Request' queue:

- 'Complete Request for Copy of Client's Information'
- ' PRC REV: Complete Review Copy File'
- 'PRC APP: Prepare File for Hearing'.

Before you begin

See Requests for full client copy files and Requests for client emails.

Instruction

Step 1

Check the request task, and the email sweep request details if needed.

Step 2

Make sure the request is in CIT scope and meets CIT criteria.

If the request...	then...
is in scope	go to step 3
is out of scope	• add the appropriate description, eg "PIR/Review/Appeal file/email sweep request outside of CIT Scope" • create a 'General' task and insert the task description: "Information Request outside of CIT Scope, please action" • confirm where to send the request and forward it to the appropriate individual or business unit • if appropriate, call the requestor and let them know who is going to provide the information, eg the Investigation Unit • close the 'Complete request for copy of client information' task • this process ends
was out of scope and has been sent back to CIT following their agreement	go to step 3

Step 3

Use the following table to transfer the task. If your team manager or leader advises a second privacy check is needed, create a subtask and send it to the second checker.

If the request is for...	then...
a full client copy file for a review or appeal personal information and requires a full client copy file only	• transfer the task to the appropriate CIT team member(s) • note in the description that an email sweep is **not** needed if not requested

personal information and requires both a full client copy file and an email sweep	• transfer the task(s) to the appropriate CIT team member(s)
	• note the following in the description:
	  • an email sweep has also been requested
	  • they'll need to send a subtask to an authorised CIT team member to do an email sweep

personal information and: • only requires an email sweep	go back to step 2 and treat the request as "out of scope"

If the request is for...	then...
• it's the initial request	

What happens next

Go to Check the task details.

Back to process map ↑

Check the task details

Responsibility

Allocated CIT team member

When to use

Use this instruction to confirm the copy file request details when you receive one of the following tasks in your individual queue:

- 'Complete Request for Copy of Client's Information'
- 'Create PRC REV: Complete Review Copy File'
- 'PRC APP: Prepare File for Hearing'.

Before you begin

See Advocates and holders of authority to act, Pre-alert information and guidelines (54K) and FAQs about delivering personal information.

Instruction

Step 1

Open the request task from your individual queue and print an ACC6173 Information disclosure checklist (166K) to complete as you work through the process.

If the task is...	then...
'Complete Request for Copy of Client's Information'	go to step 2
'PRC REV: Complete Review Copy File'	• get more information from Legal Services, FairWay Resolution Limited or the ACC business unit if needed • go to Check for previous full client copy file
'PRC APP: Prepare File for Hearing'	

Step 2

Search for the party in Eos and make sure the request is recorded against the correct party and that there are no duplicate party records.

If...	then...
the request is on the wrong party record	• move the request and the request task to the correct party record • go to step 3
you find a duplicate party record	• open the request task • create an 'Action Client Duplicate' subtask with "CIT" in the description field • go to step 3

Step 3

Use the following table to review the request task.

If the request relates to...	then...

If the request relates to...	then...

an actively managed sensitive claim	• if the request came:
	  • from the client and the task came directly from the Sensitive Claims Unit (SCU), make sure the task confirms the client is aware CIT will be handling the request and contacting the client about it
	  • via the Inquiry Service Centre (ISC), contact the SCU case owner and ensure they advise the client that CIT will be contacting them about the request
	• once you've confirmed the client is aware CIT will be contacting them, go to step 4

any other type of claim	• confirm whether the request is from the client, their advocate or their authorised representative • make sure the task includes enough information for you to clearly identify the client and the information being requested. If needed, seek further details from the case owner or task creator • when you have all the information you need, go to step 4

Step 4

Use the following table to check the requestor has the right to request the information.

If...	then...
the client is not a minor and the request is from either the client, their advocate or their authorised representative	• check that you have the requestor's name, correct address and contact phone number • if the client isn't the requestor, make sure the requestor is authorised to request the information on the client's behalf and there is an ACC5937 Authority to Act (133K) signed by the client on file, or an alternative accepted authority. If needed, check with the client or their authorised representative • go to step 5

the client is a minor and the request is not from them	• check Eos for evidence that the requestor has a right to request the information:
	  • if unsure, consult with the case owner and/or the Privacy team
	  • then if appropriate and if needed, check with the client
	• go to step 5

Step 5

If:

- the task includes an email sweep request, check the email sweep details
- the request was forwarded by the case owner and the details are not clear, contact the case owner to clarify and update the task with any additional details provided.

What happens next

Go to Confirm details with requestor and request email sweep.

Confirm details with requestor and request email sweep

Responsibility

Allocated CIT team member

When to use

Use this instruction to confirm the request details with the requestor after you've checked the task details and, if needed, request an email sweep.

Step 1

Within two working days, call the requestor to confirm the details of their request and explain the options.

If/when...	then...
you contact them	go to step 2

If/when...	then...

you're unable to contact them within 2 working days	prepare and send a CM03 Blank letter to claimant (58K) asking them to contact us to confirm the details of their request within 7 days
	• if they respond within 7 days, go to step 2
	• if they don't respond within 7 days, prepare and send another CM03 letter, this time advising we'll be unable to complete their request until we hear from them
	  • if they respond to the second letter within 7 days, go to step 2
	  • if they don't respond within 7 days:
	  • close the 'Complete request for copy of client information' task
	  • this process ends

Step 2

When you get hold of the requestor:

- confirm the details of their request
- let them know:
  - we're working on it and will provide them with the relevant information that we hold
  - if we think the request will take longer than 20 working days, we'll send them a letter to let them know when we can provide the information
  - if we find that we don't hold some of the information, we'll transfer part of the request to another agency
- ask them if they'd like a paper copy or an electronic copy
- if the request requires an email sweep:
  - clarify the details if needed and update the task
  - let them know that we'll only provide emails within a specific date range. Explain that since January 2011 it has been policy to upload all client emails to Eos. For this reason, we only run email sweeps for emails sent or received between 1 January 2007 and 31 December 2010
  - discuss any other specific search parameters that you need to fulfil the request, eg 'have you ever been known by any other names' / 'is there anything specific you are looking for'?
- stay on the line and go to step 3 to explain the delivery options.

Step 3

Use the following table to discuss and agree on the most appropriate option for providing the information.

If the requestor...	then...
wants an electronic copy	• explain that we'll send them a password protected computer disk by post and a letter telling them the phone number to call for the password • end the call • add a 'Contact' on the claim recording the conversation and their instructions • go to step 6

wants a printed copy	explain that it's safer for them to either collect the file from their nearest ACC branch or office, or nominate someone to collect it on their behalf
	• if they ask you to deliver the information by courier, keep them on the line and go to step 4
	• if they agree to collect it, then:
	  • confirm which ACC office they can collect it from
	  • if they want someone else to collect it for them, get that person's details and explain that that person will need to bring suitable identification with them, eg driver licence, passport or other photo identification
	  • end the call
	  • add a 'Contact' on the claim recording the conversation and their instructions
	  • go to step 6

Step 4

Open an ACC6181 Receiving personal information by courier (126K) information sheet, read it to the requestor and ask them to confirm whether they still want to receive their information by courier or use another option.

If they...	then...
want to read the information sheet themselves before deciding	• arrange to send them a copy • end the call and go to step 5
still want us to send it by courier and it's to a rural address or the request includes copy of a sensitive claim file	• explain that we'll call them back to arrange the delivery once we've collated the information • end the call and go to step 5
still want us to send it by courier and it's not a rural address or a sensitive claim'	end the call and go to step 5
change their minds and choose another option	you need to explain the other options to them - go back to step 3

Step 5

Add a 'Contact' on the claim, noting:

- you've read the requestor the ACC6181 to advise them of the risks of sending unprotected information by courier
- either the confirmed delivery instructions or that you've sent them a copy of the ACC6181 and you're awaiting their decision. When you receive their confirmed decision, record it as a new 'Contact'.

Step 6

Confirm you have enough details for the request to progress.

If...	then...
you're able to progress and the request doesn't include an email sweep	go to Check for previous full client copy file
you're able to progress and the request includes an email sweep	go to step 7

you're unable to progress	• discuss with the CIT management team and the Privacy Team
	• call the requestor and:
	  • explain why we're declining their request
	  • let them know we'll send them a letter to confirm our reasons
	  • discuss any other options available to them
	• send the requestor an INP07 Personal info request – decline request (64K) letter
	• close the 'Complete request for copy of client information' task
	• this process ends

the request should be completed by another ACC unit	• create a 'General' task and insert the task description: "Information Request outside of CIT Scope, please action" • confirm where to send the request and forward it to the appropriate individual or business unit • if appropriate, call the requestor and let them know who is going to provide the information, eg the Investigation Unit • close the 'Complete request for copy of client information' task • this process ends
the request should be transferred to another government agency	• send the requestor an INP03 Personal info request transfer – requestor (54K) letter

If...	then...
	• send the government agency an INP04 Personal info request transfer – govt agency (51K) letter • this process ends

Step 7

If needed, request an email sweep by an authorised CIT team member:

- check that the request has been loaded on the local CIT work register
- create a subtask with a task type 'General task' and send it to an authorised CIT staff member responsible for running and compiling email sweeps for client emails
- make sure the subtask includes the:
  - client's full name
  - date range required. (The date range must be within the specified timeframe. See Requests for client emails.)
  - any additional parameters gathered in step 2.

What happens next

The authorised CIT team member will:

- locate and compile the relevant emails using the email sweep instructions for your team
- save the email files in the restricted access folder:
  - 'I:_public_client information team_email searches' with the naming convention: "Claim#_FirstName Surname_Emails.pdf", eg 10011712914_Mickey Mouse_Emails.pdf
- return the subtask to you when they're all ready.

When you receive the subtask back, go to Complete content and privacy check.

If you also need to prepare a copy file, go to Check for previous full client copy file and do this while you wait for the email sweep to be completed.

Back to process map ↑

Check for previous full client copy file

Responsibility

Allocated CIT team member

When to use

Use this instruction after confirming the request details, to determine whether you:

- can reuse an existing full client copy file or need to prepare a new copy file
- need to add new documents if you're reusing an existing file
- need a physical file.

Instruction

Step 1

Check the local Client Information team (CIT) work register and Eos to see if the CIT has previously produced a full client copy file.

If there is...	then...
an existing full client copy file	go to step 2
no existing full client copy file	go to step 3

Step 2

Determine whether it's appropriate to reuse the existing full client copy file for this request. Consider things like, the length of time since the last request, who is requesting file and the amount of new information since the last request.

If you think it's...	then...
	go to step 3

If you think it's...	then...
not appropriate to reuse the existing file	

appropriate to reuse the existing file	• make sure it's the most recently provided file
	• check the date of the last document on the file and determine whether there are any new documents to add to it. If:
	  • there are no new documents to add:
	  • go to Dispatching client information prepared in a CIT
	  • this process ends
	  • you need to add new documents, go to step 3

Step 3

Determine whether you can still meet the timeframes. See Requests for full client copy files, Timeframes for reviews or Requests for personal information.

If the file is for...	and...	then...
a personal information request	you can meet the 20 day timeframe	go to step 4
	you can't meet the timeframe	• generate and send the requestor an INP02 Personal info request - Advise time extension (60K) letter • go to step 4
a review	you think you need an extension	• contact FairWay Resolution Limited to request an extension of time • when approved, email the review owner to let them know • go to step 4
an appeal	you think you need longer than 15 days	• let Legal Services know • go to step 4

Step 4

Whether you're preparing a new copy file or adding documents to an existing copy file, check Eos to determine whether physical file documents are required. If:

- yes, go to Check and prepare physical file documents
- no, go to Collate client copy file.

Back to process map ↑

Check and prepare physical file documents

Responsibility

Allocated CIT team member

When to use

Use this instruction when you're preparing a new copy file or adding documents to an existing copy file, to request and prepare the physical documents.

Before you begin

- Determine whether you can still meet the timeframes. See Requests for full client copy files, Timeframes for reviews or Requests for personal information
- If you're preparing the file for a review and you receive a 'General' task to let you know the review application has been formally withdrawn, contact the review owner to confirm whether to stop or continue this process. See Requests for full client copy files.

Instruction

Step 1

Check the location of the physical files.

If the physical file(s) are...	then...
archived and the claim is in the Dunedin or Hamilton Service Centre 'Actioned Cases' queue	on the same day and in this order: • transfer the claim to the department name then into your name, noting the reason as "Requested from branch/CC" • set the Eos 'Indicators' tab to 'requested' • go to step 2
archived and the claim is in 'actioned cases' in another unit	• send a 'General' task to the appropriate administrative queue or case owner with the task description: "URGENT- please transfer physical file to DSC/HSC CIT attn:*name*" • once the claim has been transferred to the CIT department queue, update the 'user' to your name and check the physical file indicator has been updated to 'requested'. If not, then change it to 'requested' • go to step 2
in open filing and shows as 'exists' with our storage provider	• send a 'General' task to the appropriate administration queue requesting the file from our storage provider • go to step 2

Step 2

Edit the original request task and add the task description: "Physical file(s) requested from *unit/branch* on *date*".

Step 3

When you receive the physical file(s):

- make sure you retain them in the order they were received
- tape any small documents to an A4 sheet, eg deposit slips and receipts
- put aside any documents that may need to be scanned individually, eg legally privileged documents, documents assessed as documents, documents assessed as potentially harmful to the client, fraud-related documents
- check each document to make sure it's about the right client. If unsure, note on your redaction spreadsheet that the item needs to be reviewed during the content and privacy check
- load each volume of the physical file separately into Eos using the code: "Back Scanned Physical File" and the description: "Documents from file to *date*".

Step 4

Arrange for the files to be backscanned into Eos. See Preparing, scanning and filing documents for VCF.

Step 5

Edit the original request task with the date you sent the documents for scanning, using the description: "Physical file documents sent for scanning on *date*".

What happens next

When the documents are viewable in Eos, go to Collate client copy file.

Back to process map ↑

Collate client copy file

Responsibility

Allocated CIT team member

When to use

Use this instruction to collate the client copy file from the ACC 'Print claim file' and Eos.

Before you begin

- Only work on one client's information at a time.
- Determine whether you can still meet the timeframes. See Requests for full client copy files, Timeframes for reviews or Requests for personal information
- If you're preparing the file for a review and you receive a 'General' task to let you know the review application has been formally withdrawn, contact the review owner to confirm whether to stop or continue this process. See Requests for full client copy files.

Instruction

Step 1

Check the claim for any incomplete documents and liaise with the case or review owner to determine whether they should be changed to 'complete' and included in the copy file bulk print.

Step 2

Use the 'print all' function on each relevant claim to generate the bulk print of the documents in Eos for the client copy file. If it's appropriate to reuse an existing client copy file and additional documents are needed, then only generate a bulk print containing the additional documents.

Step 3

Run the 'Print Claim File Report':

- Open In Fact and go to section 'Print Claim File Report'
- Run the report for each claim required and save each report in the appropriate folder on your team's local drive, using the naming convention: "Claim#_FirstName Surname_Source (Eos or RP), eg 10011712914_Mickey Mouse_PCF.pdf".

Step 4

Check for sensitive claims.

If...	then...

there is a sensitive claim and it has entered an ISSC interval	• run the 'ISSC PCF Addendum':
	  • open In Fact
	  • select 'Dashboards' from the Header menu
	  • select and expand the CIT menu
	  • select the 'ISSC PCF Addendum'
	  • run the report for each sensitive claim required and save each report in the appropriate folder on your team's local drive, using the following naming convention: "Claim#_FirstName Surname_SC Addendum, eg 10011712914_ Mickey Mouse_SC Addendum.pdf
	• go to Request secure documents check (disclosure validation)

there is no sensitive claim	go to Request secure documents check (disclosure validation)

Request secure documents check (disclosure validation)

Responsibility

Allocated CIT team member

When to use

Use this instruction to ask a case or review owner to identify any documents that:

- are secure or may need to be secured, eg legally privileged information
- may not be suitable to release to the requestor, eg could to be harmful to the client.

Before you begin

- See Limits on using and disclosing information and Requests for personal information.
- If you're reusing an existing full client copy file, then only documents added to the file since the date of the last document validation need to be reviewed
- If you're preparing a copy file for a review and the case owner lets you know the review application has been formally withdrawn, and this is confirmed in writing on the claim, then you can discuss whether to stop or continue this process with the case owner and your manager. See Requests for full client copy files.

Instruction

Step 1

If the file is for...	then...
a personal information request	• send a 'General' task with a same day target date to the appropriate administration or department queue for each claim • enter the following description: "CIT - Please review attached 'bulk print' and complete disclosure validation as per Privacy Act requirements. Please return task to sender once completed"

If the file is for...	then...
	• link the bulk print you've created to the task • if reusing a previously provided client copy file, note this in the task and provide the date range for documents included in the bulk print • go to step 2
a review	• send a 'General' task with a same day target date to the appropriate administration or department queue for allocation to the review owner • enter the following description: "CIT - Please review attached 'bulk print' and complete disclosure validation as per Privacy Act requirements. Please return task to sender once completed. If you require this file on CD, please confirm the number of CDs when you return this task" • link the bulk print you've created to the task • if reusing a previously provided client copy file, note this in the task and provide the date range for documents included in the bulk print • go to step 2
an appeal	• send a 'General' task with a time of same day target date to the appropriate administration or department queue • enter the following description: "CIT - Please review attached 'bulk print' and complete disclosure validation as per Privacy Act requirements. Please return task to sender once completed" • link the bulk print you've created to the task • if reusing a previously provided client copy file, note this in the task and provide the date range for documents included in the bulk print • go to step 2

Step 2

Update the original request task with the task description: "Sent for document validation*date*".

What happens next

If the file is for...	then...
a personal information request	• the case owner or allocated staff member will review the documents in Eos when they receive the task and let you know via a separate email which documents need to be secured, which may not be suitable for release and why. See Responding to a request for information • when you receive the task back, go to Complete content and privacy check
a review	• the review owner will review the documents in Eos when they receive the task and let you know via a separate email which documents need to be secured, which may not be suitable for release and why. See Receiving a review application. • when you receive the task back, go to Complete content and privacy check
an appeal	• the case owner will review the documents in Eos when they receive the task and let you know via a separate email which documents need to be secured, which may not be suitable for release and why. See Managing an appeal • when you receive the task back, go to Complete content and privacy check

Back to process map ↑

Complete content and privacy check

Responsibility

Allocated CIT team member

When to use

Use this instruction to privacy check the prepared information and complete section 4 of the ACC6173 Information disclosure checklist. If the request includes both a copy file and an email sweep, check both the copy file and the email sweep results when each is ready.

Before you begin

- You must complete a separate ACC6173 for each completed request, ie if the request includes a copy file and an email sweep, complete one form
- If you're reusing an existing client copy file, you only need to privacy check documents not included in the previously released file
- If you're preparing a copy file for a review and the case owner lets you know the review application has been formally withdrawn, and this is confirmed in writing on the claim, then you can discuss whether to stop or continue this process with the case owner and your manager. See Requests for full client copy files
- See Privacy check before disclosing information and Limits on using and disclosing information, Requests for personal information and Information requests and legal professional privilege.

Instruction

Step 1

Edit the original request task with the description: "Privacy check in progress".

Step 2

Print all the prepared documents securely.

Step 3

Read through each document **very carefully** to ensure we're only providing the appropriate requested information. Use the following table to ensure you do a thorough check. If needed, do both boxes in this table.

If the request includes...	then...

copy file documents	• make sure:
	  • you check both sides of every page
	  • the information we're providing only relates to the client whose information is requested and does not include:
	  • information about any other people that should not be there
	  • legally privileged information
	  • documents that should have been secured earlier, eg documents legitimately on file that refer to other parties, such as in accidental death cases
	• if needed, get advice from other parties, eg case owner, Legal Services
	• either go to step 4 or complete the box below if the request includes an email sweep

an email sweep	• make sure the information we're providing:
	  • only relates to the client whose information is requested
	  • does not include:
	  • information about any other people that should not be there
	  • legally privileged information
	• if needed, get advice from other parties, eg case owner, Legal Services, People Services
	• go to step 4

Step 4

If you feel there are any issues or content that is a risk to ACC, discuss with your team manager. See also Requests for client emails.

If the team manager decides...	then...
to escalate the issue(s), eg to Corporate Communications Media team, the Legal team, the Privacy team or Executive Services, and there's likely to be a delay in providing the response	• generate and send an JNP02 Personal info request – advise time extension (71K) letter to the requestor • go to step 5
to escalate the issue(s), but no delay is expected	go to step 5

If the team manager decides...	then...
not to escalate the issue(s)	

Step 5

If you...	then...
don't need to exclude content	go to step 6
need to exclude content, eg details or documents that we can't disclose	• block out (redact) or remove the information from the CIT copy file • secure the documents in Eos if needed • if the deleted information should not be retained on the file, create an amended version, upload it to Eos and request removal of the original document. If needed, consult with your team leader and/or team manager • update your team's 'Near Miss Register' and redaction spreadsheet • go to step 6

Step 6

If requested by your team leader or manager, or if needed for another reason, eg it's a sensitive claim file, check the subtask to confirm that there has been a second privacy check. If yes:

- meet with the second checker and relevant team leader/manager to compare what you found
- make sure they sign Section 7 of the ACC6173 Information disclosure checklist.

Ensure the secure documents check task (validation) has been returned and any appropriate resulting action completed.

Step 7

Create a pdf of the final copy file and/or email sweep file and upload it to Eos using:

- the document type 'Client Copy Information Request' (or 'SC VCF004 -Miscellaneous Outgoing Document' for Sensitive Claims)
- the appropriate document description shown in the following table.

If the request is for...	then...
a copy file	Part *X* of *X* Documentation requested for copy file *date requested*
a review file	Part *X* of *X* Documentation requested for review file *date requested*
an appeal file	Part *X* of *X* Documentation requested for appeal file *date requested*

Note:

- If you're reusing an existing copy file, **do not delete the existing file from Eos**
- If you've done an email sweep, **do not upload any of the emails individually into Eos**.

Step 8

Double check that what you've uploaded is correct and all the requested information that we can disclose has been uploaded.

What happens next

Go to Dispatching client information prepared in a CIT.

Back to process map ↑

Official information requests policy

Contact [redacted] Last review 28 Jan 2015 Next review 28 Jan 2016

Objective

ACC holds information about itself, its governing legislation, and the processes it uses to carry out its functions and duties. This type of information is known as Official Information.

ACC must effectively manage this information, ensuring it is made available in appropriate circumstances in accordance with our obligations under the Official Information Act 1982.

Scope

This policy applies to all ACC employees or contractors working on behalf of ACC.

Standards

- ACC must assist a person with their request for official information.

  Note: It is not necessary for a request to be submitted in writing, or to specifically name the legislation. All requests are automatically deemed to come under the relevant legislation.
- Requests for official information must be acknowledged within five working days and responded to as soon as possible, and always within 20 working days of the request being received.

  See: Timeframes for responding to official information requests.
- Official information requests can be transferred, in part or in full, to another agency if ACC does not hold the relevant information. Transfers must be arranged no later than 10 working days from the date of receiving the request.

  See: Timeframes for responding to official information requests.
- ACC is required to release official information when it is requested, unless there are grounds under the Act not to. These grounds are specified in sections, 6, 9 and 18 of the Official Information Act 1982 (external link).

  See: When to withhold information.
- If a requested document contains some information that cannot be released, it is appropriate to delete part of the document before releasing it.

  See: When to withhold information.
- Some Government agencies (including ACC) have a statutory authority to access personal information from individuals or organisations. If such an authority exists in the agency's legislation, ACC is required to release information if it is requested. These requests must be actioned within 3 working days.

  See: Official information requests.
- ACC never charges for personal information, but in some cases it is appropriate to charge for official information.

  See: Official information requests.

Dual requests

A client may request both personal information (eg, copy of their claim file) and official information (eg, asking for a copy of ACC's policies and procedures that led to an entitlement decision) at the same time.

When responding to these dual requests, ACC should release the personal information separately from the official information. Each release must quote the relevant sections of the legislation guiding the disclosure, as well as the avenues of complaint that can be followed, where the requestor is unhappy with the information received.

Complaints under the Privacy Act and Health Information Privacy Code can be investigated by the Privacy Commissioner. Complaints about information released or withheld under the Official Information Act can be considered by the Office of the Ombudsmen.

Accountabilities

The Government Services Manager/Privacy Officer is responsible for ensuring organisational controls are in place in support of this policy.

Official information requests

Contact [redacted] Last review 30 Jan 2015 Next review 30 Jan 2016

Introduction

We gather and use a wide range of information in order to help our clients. This information may be either personal information or official information. Official information includes information held by ACC about our management, operation and business practices. It may also be information an ACC staff member receives in the course of their work.

The Official Information Act 1982 (the OIA) states that information held by government agencies must be made available to the public unless a good reason exists for withholding it.

Rules

Government Services

Government Services is responsible for:

- managing all requests needing consultation with the Minister's office
- responding to complaints lodged with the Office of the Ombudsman.

Our responsibilities

All ACC staff must be familiar with the OIA and the Privacy Act 1993 to reduce any breaches of privacy for our clients.

When we receive a request for information we must establish:

- whether the information exists
- if it can be released to the requestor.

If a request is for...	then we manage the request under the...
official information	Official Information Act 1982
personal information about an individual **from another individual or from an organisation**, ie someone wants information about another person	Official Information Act 1982
personal information **from the individual concerned**, ie someone wants information about themselves	Privacy Act 1993. See xRequests for personal information

Privacy Officer

It is a statutory requirement under the Privacy Act 1993 that we appoint a Privacy Officer.

The Privacy Officer:

- must ensure that ACC complies with the Privacy Act 1993 and the Health Information Privacy Code 1994.
- oversees investigations into complaints lodged with the Privacy Commissioner.

Who can make an official information request?

Section 12 of the OIA states that requests can be made by:

- a New Zealand citizen
- a permanent resident of New Zealand
- a person who is in New Zealand
- an organisation that is incorporated in New Zealand
- an organisation that is incorporated outside New Zealand, but has a place of business in New Zealand

Unnecessary to specify that request is formal

The requestor does not need to specify that they're making a formal request or name the legislation they're making the request under. All requests are automatically considered to come under the relevant legislation.

Requests may be written or verbal.

Due particularity

Section 12(2) of the OIA states that requests must be made with due particularity. This means the request must:

- clearly identify the information needed
- indicate how the requestor wants the information provided
- provide reasons for urgency, if necessary
- include the requestor's name, address and daytime phone number.

You must contact the requestor if you're not sure what they're asking for, or if their request is so wide that it's impossible to answer.

Requests from media organisations, journalists etc

ACC's media team handles all requests from media organisations and journalists.

Requests from government agencies

If requested, we're required to release personal information to other government agencies that also have legal authority to access personal information from individuals or organisations.

Most of these requests will be from:

- Work and Income, quoting the Social Security Act 1964, Section 11
- Inland Revenue, quoting the Tax Administration Act 1994, Section 17
- the New Zealand Police.

The agency making the request must:

- provide us with details of their legal authority
- make the request in writing.

Requests from members of the New Zealand Police

We occasionally receive requests from the Police for information about clients. These should be referred to the Privacy Team who will respond direct to the Police.

If you receive a written request, please email it to the Privacy Team on privacy.officer@acc.co.nz.
If you receive a verbal request, advise the Police that they must make their request in writing (email or letter) and send it to The Privacy Officer, ACC, PO Box 242, Wellington 6140 or privacy.officer@acc.co.nz.

Under no circumstances should you disclose any information about the client. If you have any questions, please contact the Privacy Team.

Requests for information from outside New Zealand

The OIA does not govern our response to a request for official information from an individual or organisation that does not reside or have a place of business in New Zealand. However, we still need to provide assistance in a timely manner and make every effort to comply with the request.

You must **not** supply any personal information in response to such a request.

Charging for information

Section 15 of the OIA allows us to charge for providing official information. However, we usually only charge when a large amount of documentation is requested or we have to undertake a significant amount of work to fulfil the request.

We do **not** charge for providing personal information.

- You must consult with Government Services before deciding to charge for information
- If you consider a charge should be imposed, you must advise the expected costs in writing and ask the requestor to confirm that they are prepared to meet those costs
- We may seek part or all of the expected costs prior to undertaking the work
- Other costs, eg courier fees, are paid at the actual cost incurred by ACC
- Clients have a right of review, through the Office of the Ombudsman, regarding any charges imposed by ACC for official information.

For up-to-date rates for staff time, photocopying, or other costs see the Ministry of Justice, Charging Guidelines for Official Information Act 1982 Requests.

When to withhold information

Contact [redacted] Last review 07 Jan 2015 Next review 07 Jan 2016

Introduction

The OIA states that information held by government agencies must be made available to the public unless a good reason exists for withholding it. Withholding information includes providing partial information while omitting some information, or declining a request outright. Reasons for withholding information are described in the Official Information Act 1982 (the OIA).

Rules

Releasing only part of the requested information

Sometimes it's appropriate to release only part of the information requested, eg when the information identifies multiple individuals. In such cases, it's appropriate to delete the part(s) of the document containing this information before releasing it. See Section 17 of the OIA.

Declining a request for information

Grounds for declining an official information request are specified in Sections 6, 9 and 18 of the OIA.

We must have regard to the public interest when deciding whether to decline a request. The grounds for declining to release information can be outweighed by the public interest. See Section 9 (1) of the OIA.

See also Declining official information requests – examples.

Timeframes for responding to official information requests

Contact [redacted] Last review 07 Jan 2015 Next review 07 Jan 2016

Introduction

We must comply with the legislated timeframes when responding to official information requests.

Rules

Response time

The Official Information Act 1982 (OIA), Section 15 states that we must make a decision on an official information request:

- as soon as reasonably practicable
- within 20 working days of receiving the request.

Extending the response time

Occasionally you may need to notify an extension of time to complete a response. Extensions are allowed when:

- large quantities of information are involved
- searching through large quantities of information will unreasonably interfere with ACC's operations
- you need to consult with others.

You can only notify an extension **once**. Make sure the extension is long enough for you to complete the response within the extended timeframe.

Formal notification

If you need a time extension you must formally notify the requestor within the 20 working days limit, and include:

- the extension period needed
- the reason(s) for the extension
- advice that the requestor has the right to lodge a complaint about the extension with the Office of the Ombudsman.

Timeframe for requests from government agencies

Requests from government agencies for personal information are handled under the Official Information Act 1982. You must try to action these within three working days, although this is not a legislative requirement.

Transferring an official information request

If we don't hold the requested official information, but we know that another government agency does, you can transfer the request to the other agency under the Section 14 of the OIA. You must arrange the transfer promptly, and no later than 10 working days from the date of receiving the request.

Examples of declining official information requests

Contact [redacted] Last review 07 Jan 2015 Next review 07 Jan 2016

Introduction

ACC can decline a request for official information in certain circumstances. These include the protection of an individual's privacy and safety, as well as preserving legal professional privilege and public interest. The following table shows the reasons, with examples, we may decline an official information request. See also When to withold information.

Reasons with examples

Reason for declining request	Example
The release would prejudice the maintenance of law, including the prevention, investigation, and detection of offences, and the right to a fair trial	A person seeks details of an investigation ACC is undertaking into the practices of a treatment provider. We decline the request for information to ensure that the investigation is not compromised
There is a need to protect the safety of any individual	A person seeks details of an informant who has given information to ACC. There are good grounds for believing harm could come to the informant, and consequently we decide to decline the request for information
There is a need to protect the privacy of persons, including that of deceased persons	A debt collection agency seeks the address or phone number of an ACC client. We decline to release the information as it would interfere with the client's privacy
The information is subject to an obligation of confidence where it is in the public interest to protect the future supply of similar information, or the source of such information	An insurance company seeks details of the advice ACC has received. We decline to release the information as it was given in confidence and it is in ACC's interests to protect the future source of information
There is a need to maintain effective conduct of public affairs through 'free and frank' discussions between Cabinet Ministers and officials and between officials when doing their job	A person has sought a copy of a note of a meeting held between ACC and the Minister for ACC regarding the progress of a legislative amendment. We decline to release the advice, as doing so would interfere with the 'free and frank' discussions
There is a need to protect legal professional privilege	A solicitor has requested a copy of a legal opinion that the branch office obtained from Legal Services. We decide to claim legal professional privilege on the opinion and decline to release the legal opinion
The information requested is, or soon will be, publicly available	A support group has sought details of ACC's future direction for the management of certain claims. The information is about to be released publicly, therefore we decline to release the information
The document alleged to contain the information does not exist, or cannot be found	A person has sought a copy of ACC's position on a specific medical condition. After conferring with the Chief Clinical Advisor, we decline the request because the information does not exist or cannot be found
The request is frivolous or vexatious, or the information requested is trivial	A person makes their sixth request in three weeks for a copy of ACC's policy regarding the Independence Allowance. Having supplied the information previously, we decline to provide a further copy, determining that the request is vexatious The decision to decline a request as being vexatious **must** be made in consultation with Government Services

Reason for declining request	Example
The information cannot be made available without substantial collation or research.	A person seeks details of the number of people who have undergone the vocational independence assessment process, who have not been found able to work 30 hours or more per week in work that is indicated as suitable in initial occupational and initial medical assessments, and how long they continue to receive weekly compensation. We decline to provide the information, as its compilation will require substantial collation or research It may be possible to help the requestor by refining the level of information required, or it may be possible to make this available subject to ACC imposing a charge

Manage requests for client information from insurers

Contac [redacted] Last review 08 Jun 2015 Next review 07 Jun 2016

Introduction

We receive requests for information about our clients from insurers to inform their decisions on insurance cover and services.

We must assess and provide the requested information in accordance with the Official Information Act 1982 (OIA) because they are requests from third parties. We must also comply with the Privacy Act 1993 (Privacy Act) and ACC processes. See Requests for personal information and Official information requests.

Rules

Requests from insurers for our clients' information

When a request is received from an insurer, you must:

- make sure the request is specific enough for you to identify what information is being asked for. If you're unsure and cannot identify what's required you must ask the insurer to refine their request
- make sure the insurer provides written 'authorisation to collect' what information they're asking for. Make sure the information complies with the Privacy Act and meets the requirements below. Alternatively, we can ask our client to authorise disclosure by ACC
- send copies of the information to the insurer.
  - The information must go directly to the insurer
  - Information must not be given to the client to pass on to the insurer
- only provide a copy of the released information to the client when requested. Preferably in a secure format, to mitigate any risk of breaching privacy.

It's the insurer's responsibility to make sure they do not collect more personal information than they need.

If our client is concerned about information the insurer has requested, do not release the information. If there are any issues about the requested information it must be resolved between the client and insurer.

Requirements for assessing insurers' authorisations

Before disclosing information you must be confident that the client is aware of:

- the information is being collected
- the purpose of the information being collected
- the intended recipient of the information
- the name and address of:
  - the health agency (in this case, the insurer) collecting the information, and
  - the health agency that will hold the information.

You must also consider:

- how old is the authorisation?
- will our client remember authorising the insurer to collect the information?
- will the client still agree to the collection?
- how sensitive is the client's information?
- does the scope of the insurer's request cause concern?

If an insurer's authorisation to collect information isnt adequate regarding the Privacy Act, we can't rely on our client's authorisation to disclose their information.

If you have any questions about whether an insurer's authorisation form is acceptable, please contact the Privacy Team.

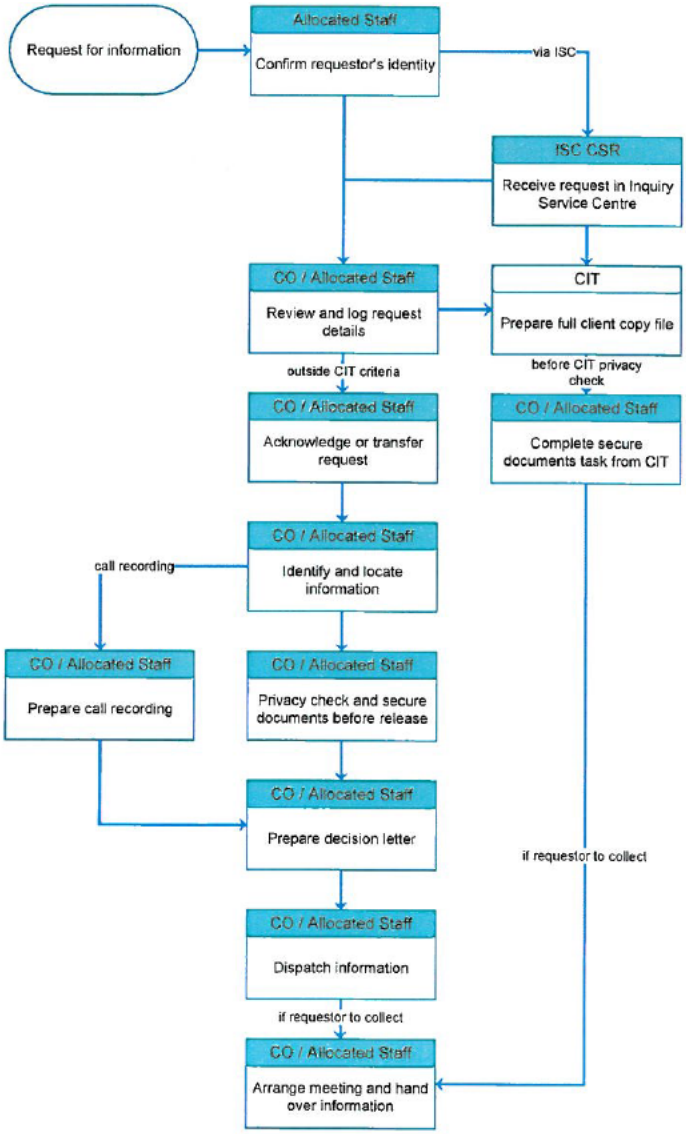
Responding to a request for official or personal information

Use this process when you receive a request for information from a client, client advocate or any external party. This process applies to all ACC staff, not just those who deal with claims. It includes confirming the requestor's identity, privacy checking the information and ensuring it is secure before it is released.

A request can be for personal information, such as client files, client related emails and call recordings, or for other information that we hold, eg official information. We'll try to provide the information within the required timeframes. If we don't hold the information we may transfer the request to another agency.

Contact [redacted] Last review 23 Jan 2015 Next review 23 Jan 2016

Click on a shaded box for instruction details



Show all instructions

Confirm requestor's identity

Responsibility

Allocated staff

When to use

Use this instruction when you receive a request for official or personal information to confirm the identity of the requestor.

Instruction

Step 1

In Eos, access the party record of the client whose information is being requested.

Step 2

If the request is made...	then...
by phone	go to step 4
via email	• in the client's Eos record, open the ACC5937 Authority to act (134K) form • check that the email address listed matches the email you have received • go to step 3

Step 3

If the email address...	then...
matches the one listed on the ACC5937 form and you are working in the Inquiry Service Centre (ISC)	go to Receive request in Inquiry Service Centre
matches the one listed on the ACC5937 form and you are not working in the ISC	go to Review and log request details
is not listed on the ACC5937 form or there is no ACC5937 form on the client's record	phone the requestor and go to step 4

Step 4

If the request is from...	then...
the client	go to step 5
the client's advocate	• in the client's Eos record, open the ACC5937 • go to step 5
a provider	go to step 5
a third party caller (none of the above)	• in the client's Eos record, click the 'Contacts' tab to ensure that the caller is listed • go to step 5

Step 5

Inform the caller that we need to complete a brief security check and ask them the standard Identity check questions.

Step 6

If the caller...	then...
correctly confirms the details and you are working in the ISC	go to Receive request in Inquiry Service Centre
correctly confirms the details and you are not working in the ISC	go to Review and log request details
cannot confirm the details	

If the caller...	then...
	• politely apologise that you are unable to proceed any further with the call • advise the caller that the client may need to add them as an authority and explain the Advocates and holders of authority to act process as necessary • this process ends

Back to process map ↑

Receive request in Inquiry Service Centre

Responsibility

Customer service representative, Inquiry Service Centre (ISC)

When to use

Use this instruction when you receive a request for information in the ISC from a client or other external party.

Before you begin

If you're **not** a customer service representative (CSR) in the ISC, start from **Review and log request details**.

Instruction

Step 1

If the request...	then...
relates to a Claims Management client or their claim	• identify the claim or primary claim that relates to the request • take the request details • go to step 2
does **not** relate to a Claims Management client or their claim	• transfer the call or the request details to the appropriate ACC team • this process ends for the CSR • go to **Review and log request details**

Step 2

If the requestor asks for a copy of a call recording only or as part of a larger request:

- get the details you need to identify the call recording
- let the requestor know that someone may need to contact them later to discuss the request further
- email the call recording request details to your team manager and ask them to **review and log the request details**.

Step 3

If the request...	then...
is for a call recording only	• this process ends for the CSR • go to **Review and log request details**
relates to a client's claim **and** includes a request for a call recording	go to step 4
does not include a call recording	

Step 4

Determine if the request meets CIT criteria

Step 5

If the request...	then...
relates to an actioned claim and meets CIT criteria	send a 'Complete Request for Copy of Client's Information' task to the 'Client Information Request' queue
relates to an actioned claim and does **not** meet CIT criteria	send a task to the administration queue of the last managing site
relates to a managed claim	transfer the call to the case owner or send them a task

What happens next?

If you sent the request to...	then...
the last managing site or the case owner	• the case owner or allocated staff member goes to **Review and log request details** • this process ends for the CSR

a Client Information team	• the CIT will prepare the client information:
	  • the case owner goes to **Complete secure documents task from CIT** when they receive the task
	  • the CIT completes the privacy check and either sends the information directly to the requestor or to an ACC branch or unit to be collected
	  • the branch or unit staff go to **Arrange meeting and hand over the information** when they receive it from the CIT
	• this process ends for the CSR

your team manager	• the team manager goes to **Review and log request details** • this process ends for the CSR

Back to process map ↑

Review and log request details

Responsibility

Case owner or allocated staff

When to use

Use this instruction if you're **not** a customer service representative (CSR) in the Inquiry Service Centre (ISC) and you receive a request for information from a client or other external party, either directly or via the ISC.

Before you begin

Print an ACC6173 Information disclosure checklist (166K) to complete as you work through this process. You should try to respond within the standard timeframe. See Requests for personal information and Timeframes for responding to official information requests.

Step 1

Review the request to confirm which Act applies, the Official Information Act 1982 (OIA) or the Privacy Act 1993. See Official information requests and Requests for personal information.

If the request for information is...	then...
about a Claims Management client or their claim	go to step 2

for personal information about any other person	• log the request as a 'personal information' request in the appropriate system, eg:
	  • Action Remedy System (ARS) (Corporate Office only)
	  • Oracle
	• go to step 4

If the request for information is...	then...

not for personal information	• log the request as an 'Official Information Act' request in the appropriate system, eg:
	  • Action Remedy System (ARS) (Corporate Office only)
	  • Oracle
	• go to step 4

Step 2

If the request is from...	then...
the client	• add a 'Contact' in Eos and log the request as a 'personal information' request • go to step 4
the client's advocate or authorised representative	• check that they have authority to request the information on the client's behalf. Make sure an ACC5937 Authority to Act (133K) signed by the client is on the client's file • go to step 3
either: • the client's parent or guardian • an organisation or third party who may not be entitled to the information, eg a third party administrator, insurance company, government agency, relative, friend	• check the client's file for evidence that they have a right to request the information, eg an authority to send information to the third party • go to step 3

Step 3

If the requestor...	then...
may request the information on the client's behalf	• add a 'Contact' in Eos and log the request as a 'personal information' request • update and initial the ACC6173 Information disclosure checklist, section 2 • go to step 4

may not request the information on the client's behalf	consider whether we can respond under the Official Information Act (OIA). See Requests for personal information.
	• if yes:
	  • add a 'Contact' in Eos and log the request as an Official Information Act request
	  • go to step 4
	• if no:
	  • generate and complete an INO08 Official info request – decline request (42K) letter
	  • send the letter to the requestor
	  • this process ends

Step 4

Review the request to see if it includes all the information needed to continue, eg:

- enough details to clearly identify the information, eg:
- specific document description(s) and/or title(s), such as a report from a doctor
- a full client copy file or a partial copy file. See Requests for full client copy files
- emails about a client covering a particular date range. See Requests for client emails
- a copy of a call recording
- details of how the requestor wants the information to be provided, eg printed or electronic, and their preferred method of delivery

- if the request is urgent, the reason why
- the requestor's name, address and contact phone number
- confirmation from the requestor of the intended recipient's name and address, if not the requestor.

Step 5

If...	then...
you have enough information to continue with the request	go to step 6
you need more information	• contact the requestor to get the details you need • go to step 6

Step 6

If a call recording ...	then...
is requested	• confirm the call recording details with the requestor • discuss whether releasing the recording is the best solution for them • if appropriate, discuss whether there may be other possible options such as referring them to the complaints process • go to step 7
is not requested	go to step 7

Step 7

If an email sweep ...	then...
is specifically requested by the client	• let them know that someone will contact them later to discuss the request further • confirm and agree the search parameters, eg client name, claim number and date of birth, details and/or date range of emails requested • go to step 8
is not requested	go to step 8

Step 8

Record the outcome of your discussion as a 'Contact' in Eos or other appropriate system and update and initial the ACC6173 Information disclosure checklist, section 3.

Step 9

Determine if the request meets CIT criteria.

If...	then...

yes	• send a 'Complete Request for Copy of Client's Information' task to the 'Client Information Request' queue:
	  • include email sweep request details, if needed
	  • if you identify a risk, eg the client says they want the file because they're going to the media, let the CIT know
	• set a task for 15 working days to check the progress of the request

no	go to **Acknowledge or transfer request**
a copy of a call recording only and they no longer want the call recording	this process ends

What happens next?

If the request meets CIT criteria the CIT will acknowledge the request and prepare the client information.

If the request requires...	then...
a copy file only a copy file **and** an email sweep	when you receive a 'General' task with a task time of 0 hours asking you to check and secure non-disclosure documents in Eos, go to **Complete secure documents task from CIT**
an email sweep only	either: • the CIT will send the information directly to the requestor. This process ends • the CIT will send the information to an ACC branch or unit to be collected. Go to **Arrange meeting and hand over the information**

Back to process map ↑

Acknowledge or transfer request

Responsibility

Case owner or allocated staff

When to use

Use this instruction to acknowledge a request for information or transfer it to another agency or business unit. Do **not** complete this instruction if a CIT is preparing the information.

Instruction

Step 1

If the request is...	then...
from a media organisation or journalist	• transfer to the request to the Corporate Communications Media team • this process ends
for **official** information that we **don't hold** but you know it's held by another government agency	within 10 days of receiving the request: • send the requestor an INO04 Official info request transfer – requestor (54K) letter • send the government agency an INO05 Official info request transfer – govt agency (49.5K) letter • this process ends
for **personal** information that we **don't hold** but you know it's held by another government agency	within 10 days of receiving the request: • send the requestor an NP03 Personal info request transfer – requestor (54K) letter • send the government agency an NP04 Personal info request transfer – govt agency (54K) • this process ends
for official **or** personal information that we **do** hold	go to step 2

Step 2

If the request is for...	then...
official information	• send the requestor: • an INO01 Official info request - acknowledge (85.5K) letter

If the request is for...	then...
	• an INOIS01 Requesting official information (93K) information sheet • go to step 3
personal information	• send the requestor: • an INP01 Personal info request - acknowledge (86K) letter • an INPIS02 Requesting personal information (99.5K) information sheet • add a 'Contact' in Eos, or note in another appropriate system, eg Oracle if a call recording • go to **Identify and locate the information**

Step 3

Decide whether we need to charge for the information. See Official information requests.

If...	then...
you think we need to charge for the information	• get approval from the Government Services team • contact the requestor to explain that we'll charge them for the information • go to step 4
there is no need to charge	go to **Identify and locate the information**

Step 4

If the requestor...	then...
still wants to proceed	send them an: • INO02 Official info request – advise costs (39K) letter providing an estimation of the cost and a request to agree to this cost • go to **Identify and locate information**
doesn't want to proceed	• note this in the appropriate system, eg Action Remedy System (ARS) (Corporate Office only) • this process ends

Back to process map ↑

Identify and locate information

Responsibility

Case owner or allocated staff

When to use

Use this instruction if you're preparing the information, to identify and locate the requested information and request an extension if needed. Do not complete this instruction if a Client Information team (CIT) is preparing the information. Go to **Complete secure documents task from CIT** when you receive the task from the CIT.

Before you begin

Read Timeframes for responding to official information requests and Requests for personal information.

Instruction

Step 1

Review the information request and confirm that the information can be released under the provisions of the:

- Official Information Act 1982, for official information. For more information visit www.ombudsmen.parliament.nz
- Privacy Act 1993, for personal information. For more information visit www.privacy.org.nz.

If the request is for...	then...
official information or information that we hold about a person who is **not** an ACC client	• identify and locate the requested information • go to step 3
a client's personal information	identify and locate the requested information in Eos. If physical files are: • required, go to step 2 • not required, go to step 3

a call recording	• send an email to the appropriate Telephony team:
	  • Inquiry Service Centre (ISC): ISC.TSA@acc.co.nz
	  • Business Service Centre (BSC): BSC.technicaladvisors@acc.co.nz
	• Include the following details in your request:
	• ask them to extract the call recordings
	• client Name & Eos Party Record ID (or ACC Account number etc)
	• for each call being requested, give
	  • date and time of call
	  • customer service representative's (or recorded staff members) Name
	  • phone Number the call was made from (if possible)
	• you will receive notification from the telephony team that the calls are available and this will include the location of where the calls are saved.
	• when you receive notification that the calls are available, go to Prepare call recording

Step 2

If the physical client file is...	then...
held at your own branch	• locate the file(s) • go to step 3
held at another branch and the client lives in that area	• send a task to that branch asking them to complete the request using this process • go to step 3
archived in the Dunedin or Hamilton Service Centre 'Actioned Cases' queue	• send a task to the DSC or HSC admin queue requesting the file(s) and make a note in the 'Inwards' book • set the Eos indicators tab to 'requested' • transfer the claim the claim to your department name • then transfer the claim into the your name • when the file arrives, add a Comment on the Eos 'Indicators' tab saying "file received in xxx branch on xxx date" • check the file status in Eos says "Exists" • go to step 3
held in another unit and is either open or closed	• send a 'General' task to the appropriate administrative queue or case owner with the task description "URGENT- please transfer physical file to *your branch* attn:*name*" • make a note in the 'Inwards' book • when the file arrives, add a Comment on the Eos 'Indicators' tab saying "file received in xxx branch on xxx date" • check the file status in Eos says "Exists" • go to step 3

If the physical client file is...	then...
in open filing with our storage provider	• send a 'General' task to the appropriate administration queue requesting the file from the storage provider • go to step 3

Step 3

Determine whether you can respond to the request within the standard timeframe, either:

- 3 working days (OIA requests from government agencies)
- 20 working days (all other requests).

Step 4

If you need an extension, advise the requestor of the expected timeframe using either:

- JNO03 Official info request – advise time extension (61K)
- JNP02 Personal info request – advise time extension (60K).

What happens next?

Go to **Privacy check and secure documents before release**.

Back to process map ↑

Privacy check and secure documents before release

Responsibility

Case owner or allocated staff

When to use

Use this instruction when you're preparing the information, to identify and withhold or remove information that we can't release because of legal professional privilege or to protect the client and/or their privacy. Do not complete this instruction if a Client Information team (CIT) is preparing the information. Go to **Complete secure documents task from CIT** when you receive the task from the CIT.

Before you begin

Clear your work area or go to a dedicated privacy desk. Read Privacy check before disclosing information.

Instruction

Step 1

If the request is for...	then...
official information	• identify any documents you need to withhold due to withholding provisions or legal professional privilege. See When to withhold information. If you're unsure, discuss with a team manager or Government Services • update the request details with the titles of any documents that you're withholding • go to step 2
personal information (not client information)	• identify any documents you need to withhold due to withholding provisions or legal professional privilege. See Requests for personal information. If you're unsure, discuss with a team manager or the Privacy team • update the request details with the titles of any documents that you're withholding • go to step 2
a client's personal information	go to step 3

Step 2

Photocopy the documents that you're planning to release and do a privacy check for personal information that is not relevant to the requestor.

- Put aside any documents that don't need amending and label these "for release"
- If you need to amend any documents:
  - use white correction tape to obscure any names or information that we should not disclose
  - photocopy the amended documents and make sure you can't read the obscured information
  - put the **checked** copies together with any other documents for release
  - securely destroy the copies that you amended
- Go to **Prepare decision letter**.

Step 3

Do a content check of the client's information to make sure no irrelevant information is included. If you have substantial or minor enclosures, refer to the guidelines in Privacy check before disclosing information.

If any of the relevant documents are...	**then...**
in Eos	• identify any documents that are covered by the withholding provisions in the Privacy Act. See Requests for personal information. If you're unsure, discuss with a team manager or the Privacy team • identify and secure any documents that you need to withhold due to legal privilege. Use the document type 'Legally privileged advice/documents'. See Information requests and legal professional privilege • identify and secure any documents that you need to withhold to protect the client's physical or mental health. See Requests for personal information • list all the document titles that you're withholding and the reasons why, eg appropriate legislation reference • print any remaining relevant documents securely • go to step 4

on a physical file	• identify and separate any documents that:
	  • are covered by the withholding provisions in the Privacy Act. See Requests for personal information. If you're unsure, discuss with a team manager or the Privacy team
	  • you need to withhold due to legal privilege. See Information requests and legal professional privilege
	  • you need to withhold to protect the client's physical or mental health. See Requests for personal information
	• copy any remaining relevant documents
	• go to step 4

Step 4

Privacy check the remaining documents to make sure they don't include any personal information that is not relevant to the client. If you have substantial or minor enclosures, refer to the guidelines in Privacy check before disclosing information.

If...	**then...**
no documents need amending	go to step 5

any documents need amending	• put aside any documents that **don't** need amending and label these "for release"
	• use white correction tape to obscure the irrelevant information in the remaining documents
	• make **two** copies of the **amended** documents and check these to make sure you can't read the obscured information
	  • put one set aside and label it "for scanning"
	  • either put aside the **second set** of amended documents and label them "for release", or put them with those you've already labelled "for release"
	• securely destroy the original amended documents
	• go to step 5

Step 5

If needed, ask a colleague to do a second content and privacy check of the copies that you've prepared for release. See Privacy check before disclosing information. When complete, update and initial the ACC6173 Information disclosure checklist, section 4.

Step 6

- Use Preparing, scanning and filing documents for VCF to arrange for all the amended copies to be scanned into Eos. When loading the barcodes, add a 'Comment' noting what has been removed, eg "removed other people's details for privacy reasons"
- Check Eos the next day to see if the documents have been scanned
- Attach all the privacy checked documents for release onto the Claim or Party (if multiple claims) record
- Make sure all the documents you're providing in response to the request have "privacy checked – client copy of requested document" in the 'Comments' field
- Add a 'Contact' in Eos with "All documents privacy checked and provided to the client" in the 'description' field.

Step 7

If you retrieved any physical file(s) from...	**then...**
our storage provider	• use Archiving physical claim files to send the file(s) back to storage (if file is closed) • if the file is open [process still being developed] • go to step 8
another branch or unit	• retain the file(s) at your branch • go to step 8

Step 8

If the requestor wants...	**then...**
a printed copy	• make sure the documents meet the required standards, are readable and numbered in chronological order • update and initial the ACC6173 Information disclosure checklist, section 5 • go to **Prepare decision letter**
an electronic copy	• save a pdf copy of all the prepared document(s) to a suitable location on your local or network drive • complete the Electronic claim file request form (31K) available in MS Outlook and attach the PDF documents to the email. Put your own name and branch contact details in the 'Delivery address' field, not the requestor's • check the attached documents to make sure they're correct • delete the PDF documents from your local or network drive

What happens next?

The claims officer will:

- combine the files into a single pdf document and burn this onto the password protected computer disk
- send you the disk via internal mail
- email you the password.

When you receive the disk, go to **Prepare decision letter**.

Back to process map ↑

Prepare call recording

Responsibility

Case owner or allocated staff

When to use

Use this instruction when you receive the requested call recording from the Inquiry Service Centre (ISC) or Business Service Centre (BSC) Telephony team.

Before you begin

We can provide a call recording as:

- a password protected.zip file on a computer disk (preferred secure option)
- an unprotected .wav file either by email or on an audio CD, if requested
- a written edited transcript or summary, if needed.

For guidance on passwords see Information security standards.

Instruction

Step 1

Generate an ACC6176 Checklist for releasing telephone recordings (117K) and complete this as you work through this instruction.

Step 2

Review the request and the files provided to identify the most likely call(s). If you:

- don't find the likely call(s), go to **Prepare decision letter**
- find the likely call(s), go to step 3.

Step 3

Listen to each call and make sure it's the correct requested call. Confirm the following details:

- the name(s) of the caller(s)
- the number they called from, if possible
- the name of the ACC staff member they spoke to
- the call date(s) and time(s).

Repeat this step until you're certain you've identified the correct call(s).

Step 4

Privacy check the call(s). Listen to each call again and make sure it does not include details about other people or information we should not disclose. See Requests for personal information and Information requests and legal professional privilege . If needed, consult with the relevant authority, eg technical claims manager (TCM) or unit manager.

If the recording...	then...
does not include any personal information about the requestor	• do not release the recording • go to **Prepare decision letter**
includes personal information about the requestor **and**: • does not include personal information about any other people • does not include information that we can't disclose	go to step 6

includes personal information about the requestor, **and either**:
• personal information about one or more other people
• information that we can't disclose
	• refer to Requests for call recordings and consider whether we can provide:
	  • a copy of the relevant segment of the recording
	  • a written edited transcript, or a summary if appropriate, eg if the recording is not clear
	• discuss with the Privacy Team if needed
	• go to step 5

Step 5

If...	then...
we **may** be able to provide a copy of the relevant segment of the call	send another email to the ISC or BSC telephone administrator requesting the relevant segment • if they provide it. go back to step 4 • if they can't provide it:

If...	then...
	• consider whether we can provide a written edited transcript or summary instead • discuss with the Privacy Team if needed • repeat step 5
we can provide a written edited transcript	• ask a team administrator or appropriate person to transcribe the relevant parts of the recording word for word into a Word document, using separate paragraphs to identify each speaker • when it's ready, save the transcript in the appropriate system, eg Eos client or claim record or the customer's Oracle account • go to step 7
we can provide a written summary	• ask the ACC staff member who took the call to complete a written summary of the relevant parts of the call • when it's ready, save the summary in the appropriate system, eg Eos client or claim record or the customer's Oracle account • go to step 7
we can't provide any of the above	go to **Prepare decision letter**

Step 6

If...	then...
the requestor wants the call on a password protected computer disk	• save the recording as a password protected .zip file in the same location as the original .wav file • name the .zip file using the client's surname and date of release • burn the .zip file onto a computer disk. If you can't do this, arrange for a technical expert to do it, eg ISC or BSC • double check that the right call recording(s) are on the disk • record the password with the request details in the appropriate system, eg Eos or Oracle • go to step 8
the requestor wants it on an audio CD	• burn the .wav file onto an audio CD. If you can't do this, arrange for a technical expert to do it, eg ISC • double check that the right call recording(s) are on the CD • go to step 8

Step 7

Complete a content and privacy check of the transcript or summary. Consult with the relevant authority as required, eg technical claims manager (TCM) or unit manager. If needed:

- remove any sections that refer to other people or contain information that we can't disclose
- clearly identify any sections where information has been removed
- check the edited transcript or summary against the call recording to make sure there are no discrepancies between what has been captured and what is on the call recording.

Step 8

Update the ACC6176 Checklist for releasing telephone recordings (117K).

What happens next?

Go to Prepare decision letter.

Back to process map ↑

Prepare decision letter

Responsibility

Case owner or allocated staff

When to use

Use this instruction to prepare the decision letter and double check the prepared information. Do not complete this instruction if a Client Information team (CIT) is preparing the information. Go to **Arrange meeting and hand over information** if and when you receive the file from the CIT.

Before you begin

All minor enclosures, including summaries or transcripts of call recordings, must be double checked by another staff member. See Privacy check before disclosing information.

Instruction

Step 1

If the request is for...	and you're releasing...	then ...
official information	all the information	• generate and complete an INO06 Official info request - provide info (48K) letter • go to step 2
	some of the information	• generate and complete an INO07 Official info request – provide some info (51K) letter • make sure you identify the right reasons for withholding some of the information. See When to withhold information • go to step 2
	none of the information	• generate and complete an INO08 Official info request – decline request (42K) letter • send the letter to the requestor • this process ends
personal information (includes call recordings)	all the information	• generate and complete an INP05 Personal info request - provide info (79K) letter go to step 2
	some of the information	• generate and complete an INP06 Personal info request – provide some info (79K) letter • make sure you identify the right reasons for withholding some of the information. See Requests for personal information • go to step 2
	none of the information	• generate and complete an INP07 Personal info request – decline request (64K) letter • send the letter to the requestor • this process ends

Step 2

Ask a colleague or manager to peer review the letter and the prepared information, and:

- check that the information we're supplying meets the requirements of the request and the relevant legislation
- if needed, double check that the information is correct and does not include any information that should be withheld or is on the wrong file.

When they've checked the information or if they don't have the equipment to check it, go to step 3.

Step 3

If it's ...	then...
a call recording	complete and sign the ACC6176 Checklist for releasing telephone recordings (117K) and load it in the appropriate system, eg Eos or Oracle
not a call recording	if the information was checked by a peer reviewer or manager, ask them to sign section 7 of the ACC6173 Information disclosure checklist

What happens next?

If the requested information...	then...
meets all the requirements	• the peer reviewer or manager will return the prepared information and letter to you • go to **Dispatch information**
does not meet all the requirements	• the peer reviewer or manager will ask the person who compiled the information to make the required changes • when it's ready, repeat from step 2

Back to process map ↑

Dispatch information

Responsibility

Case owner or allocated staff

When to use

Use this instruction to confirm the appropriate delivery method and dispatch the information either to the requestor or to an ACC office to be collected.

Before you begin

We'll only deliver by courier if specifically requested. See Privacy check before disclosing information. If a Client Information team (CIT) is preparing the information, they'll either release the information directly to the requestor on a computer disk, or send you the printed file to be collected. Go to **Arrange meeting and hand over information** when you receive the file from the CIT.

Instruction

Step 1

If the requestor is not the client, reconfirm their right to receive the information. Check that there is an ACC5937 Authority to Act (133K) signed by the client.

Step 2

Call the requestor to let them know the information is ready and confirm the delivery method. Use the following table for guidance. See also FAQs about delivering personal information.

If you're providing...	you can use...
information in response to a request under the Official Information Act	post
password protected information on a computer disk, eg substantial personal information or a call recording	post
substantial personal information in an unprotected format, eg: • a hard copy of a full client copy file or other substantial enclosures • a substantial written transcript or summary of a call recording	collect from an ACC office
a limited amount of personal information in an unprotected format, eg: • a minor enclosure • a short written transcript or summary of a call recording	either post or email. See Risks associated with email communication
a call recording in an unprotected format, eg a .wav file	• collect from an ACC office if it's an audio CD

Step 3

If...	then...

If...	then...
the requestor asks you to **courier** the information directly to them	• read the ACC6181 Receiving personal information by courier (127K) information sheet to the requestor to confirm whether they still want to receive their information by courier or prefer another option • if they ask for a copy of the sheet, tell them you'll send them a copy • end the call and if needed, send them an ACC6181 information sheet • go to step 4
the requestor or their representative agrees to **collect** the information	go to step 6
you can send the information by **email**	go to step 7
you can send the information by **post**	go to step 8

Step 4

Record the conversation in the appropriate system, eg Eos Claim or Party record, Oracle.

- Note that you've read the requestor the ACC6181 to advise them of the risks of sending unprotected information by courier
- Note the confirmed delivery method, or that you've sent them a copy of the ACC6181 and are awaiting their decision. Remember to update the 'Contact' or record when you receive their confirmed decision

When they've confirmed their decision, go to step 5.

Step 5

If they decided...	then...
not to use a courier	go back to step 3

they still want you to courier the information	• seal the information with the covering letter in a large envelope or suitable wrapping
	• check the delivery address details in Eos (or other system, eg BSC team) then print an address label, eg CLI05 Address label (32K) from Eos
	• stick a labelope to the front of the package and place the printed address label inside the labelope. Make sure only the name and address are visible
	• seal the package, mark it 'Private and Confidential' and place it inside a courier bag
	• print another address lable and place this in a labelope on the front of the courier bag. Make sure only the name and address are visible
	• seal the package then either:
	  • complete an ACC6174 Information required for courier forwarding (45K) form and clip this to the package
	  • complete the courier log book
	• place the package in the outgoing mail
	• update and initial the ACC6173 Information disclosure checklist section 6, sign section 8 then load the completed form in Eos
	• if you receive the ACC6174 form back with the tracking details added, save it to your local drive
	• go to step 9

Step 6

To prepare the information for collection:

- seal the information with the covering letter in a window envelope, bubble envelope or other suitable wrapping
- check the requestor's delivery address details in Eos then print an address label, eg CLI05 Address label (32K) from Eos
- stick a labelope to the front of the package and place the printed address label inside the labelope. Make sure only the name and address are visible
- mark the package 'Private and Confidential'

- generate an ACC6179 Acknowledge receipt of information form and complete **Part one**.

If the information will be collected from...	then...
your office	• attach the partially completed ACC6179 form to the prepared package and store the package safely to await collection • generate an JNP05 Personal info request - provide info (79K) letter, select **Option 1** and send it to the client • update and initial the ACC6173 Information disclosure checklist section 6, sign section 8 then load the completed form in Eos • go to **Arrange meeting and hand over the information**

another ACC office	• place the prepared package inside **another** envelope or wrapping, together with the partially completed ACC6179 Acknowledge receipt of information form
	• label the second package with the branch or unit name and type of content, eg "Wellington branch - client file to be collected"
	• place the double enveloped package inside a courier bag and stick a labelope to the front of the bag
	• print a branch address label and place this inside the labelope. Make sure the branch name and address are visible
	• seal the courier bag then either:
	  • complete an ACC6174 Information required for courier forwarding (45K) form and clip it to the courier bag
	  • complete the courier log book
	• place the bag in the outgoing mail
	• generate an JNP05 Personal info request - provide info (79K) letter, select **Option 1** and send it to the client
	• update and initial the ACC6173 Information disclosure checklist section 6, sign section 8 then load the completed form in Eos
	• if you receive the ACC6174 form back with the tracking details added, save it to your local drive
	• go to **Arrange meeting and hand over the information**

Step 7

To send the information by email, open the prepared documents or files and the covering letter in Eos, then:

- save the documents and letter on your business unit's network shared drive in a folder designated by your unit manager. Name the files using the client's surname and date of release
- send the requestor an email asking them to confirm their correct email address by replying to your email
- when they respond, create a reply to their confirmation email and:
  - attach the files and the covering letter
  - check the attachments and the address and Subject line then send the email
- delete the requested documents from your network drive
- update and initial the ACC6173 Information disclosure checklist section 6, sign section 8 then load the completed form in Eos
- this process ends.

Step 8

To send the information by post:

- seal the information with the covering letter in a window envelope, bubble envelope or other suitable wrapping
- place the package inside another envelope and stick a labelope to the front
- check the delivery address details in Eos or other system then print an address label, eg CLI05 Address label (32K) from Eos
- place the printed address label inside the labelope. Make sure only the name and address are visible
- seal the package and place it in the outward mail
- update and initial the ACC6173 Information disclosure checklist section 6, sign section 8 then load the completed form in Eos.

Step 9

If the information is...	then...
printed	this process ends

If the information is...	then...
on a password protected computer disk	when the requestor rings you for the password: • do the standard identification checks to confirm that they're the right person • if confirmed, tell them the password • add a 'Contact' in Eos • this process ends

Back to process map ↑

Complete secure documents task from CIT

Responsibility

Case owner or allocated staff

When to use

Use this instruction when the information is being prepared by a Client Information Team (CIT) and they send you a 'General' task with a task time of 0 hours asking you to secure documents in Eos that we can't disclose. Complete the task within **two** working days from when it was created.

Before you begin

See Limits on using and disclosing information, Information requests and legal professional privilege and Requests for personal information.

Instruction

Step 1

Open the 'General' task in Eos. If you think you can't complete the CIT task within the required timeframe:

- discuss with your team manager or team leader
- let the CIT know as soon as possible.

Step 2

Check the client information in Eos and make sure all information we can't disclose is secured.

- If legally privileged, use the document type 'Legally privileged advice/documents'
- Do **not** edit the task or remove any documents yourself
- Get advice from Customer Service Technical Support (CSTS) if needed.

If the file has...	then check...
previously been released	• documents added to the file since the date of the last document validation • already secured documents that we may now be able release, eg were previously withheld to protect the client
not previously been released	**all** the documents

Step 3

Send an email listing the document titles that you've secured to the CIT staff member responsible.

Step 4

Transfer the task back to the CIT within **two** working days of the date the task was created, stating that you've completed document validation.

Step 5

Discuss any further other actions needed with the CIT, eg if a document should be deleted.

What happens next?

The CIT will collate the client copy file, privacy check it and prepare the decision letter.

If the requestor wants...	then the CIT will...
a password protected computer disk	• post it directly to them • this process ends

If the requestor wants...	then the CIT will...
a printed copy by courier	• courier it directly to them • this process ends
to collect the printed copy	• send the printed information to the relevant ACC office for collection • go to **Arrange meeting and hand over the information**

Back to process map ↑

Arrange meeting and hand over information

Responsibility

Case owner or allocated staff

When to use

Use this instruction when you're ready to meet with the client or their representative to hand over information prepared by you, another branch or a Client Information team (CIT). Do this as soon as possible to ensure we meet the required timeframes for personal information requests.

Before you begin

- See WorkSAFE Managing aggressive/threatening situations (1.4MB) about having a safe meeting
- Make sure you store all copies of client information securely until it's collected, as you would for active physical files.

Instruction

Step 1

If...	then...
the information is being collected from your office	go to step 2
you've received the printed information by courier from another branch or a Client Information Team (CIT)	• open the courier bag • open the first envelope or wrapping inside the courier bag to access the ACC6179 Acknowledge receipt of information form • check the ACC6179 to find out who the information is for • go to step 2

Step 2

Contact the requestor and:

- confirm who will be collecting the information and note this as a 'Contact' in Eos
- if the client is collecting the information and has an active care indicator in Eos, tell them that another staff member or a security guard may need to be present
- ask them to make sure they or their representative bring personal identification with them, such as their driver licence, passport or other acceptable photo identification. If they don't have acceptable photo identification they may need to complete an ACC44 Statutory declaration (38K)
- tell them where they need to come to collect the information and arrange a suitable time to meet.

Step 3

If the client...	then ...
doesn't have an active care indicator	• you may arrange to meet with the client alone • go to step 4
has an active care indicator	• arrange for another staff member or a security guard to be present • go to step 4

Step 4

When they arrive to collect the information, use the following table to check their identification and authority to receive the information.

If the person is...	then...
the client	• check their identification • go to step 5
the client's advocate or lawyer	• check Eos to make sure they have an ACC5937 Authority to act (133K) form on file • check their identification • go to step 5
a representative from the client advocate or lawyer's office	• check Eos to make sure they are the person authorised by the advocate or lawyer to collect this information. If needed, contact the advocate or lawyer to get their authorisation • check their identification • go to step 5
a third party without authority to act, eg: • spouse • grandchild • friend • parent of a minor	• check Eos to make sure they are the person authorised to collect this information. If not, contact the client or their representative to get their authorisation • check their identification • go to step 5

Step 5

If you...	then...
confirm their identity	• give them the unopened envelope containing the information • make sure you both sign the ACC6179 Acknowledge receipt of information (126K) form • load the completed ACC6179 form in Eos
can't confirm their identity	• do not provide the information

What happens next

If the information is not collected when arranged, ring the requestor to determine whether there is an issue with collecting the information and discuss other options. See Frequently asked questions about providing information. If you're unable to resolve the issues, write to them asking them to collect the information within 10 days and record this as a 'Contact' in Eos.

- If not collected after 10 days, store the information securely onsite for a further 3 months
- If not collected after a further 3 months, destroy it securely, eg put it in a confidential shredding bin.

This process ends.

Back to process map ↑