



AFP

Better Practice Guide on Health File Access

Date of initial endorsement:	11 March 2016
Date of last review:	14 August 2020
Endorsed by:	SHIELD Coordinators Operational Forum
Owner:	Chief Medical Officer
Contact:	s 47E(d) afp.gov.au
Identifier:	MOH007
IPS status:	Full

Disclosure and classification: This document is classified OFFICIAL and is intended for internal AFP use. Disclosing any content must comply with Commonwealth law and the AFP National Guideline on information management.

Compliance: This instrument forms part of the AFP Governance Instrument Framework (GIF) as defined in the [AFP Commissioner's Order on governance \(CO1\)](#). The [AFP Commissioner's Order on professional standards \(CO2\)](#) and [AFP Commissioner's Order on security \(CO9\)](#) set the framework for the conduct expected of AFP appointees through obligations and best practice to help maintain the safety and security of AFP information, operations, assets and people. Inappropriate departures from the provisions outlined within AFP governance instruments may constitute a breach and be dealt with under Part V of the [Australian Federal Police Act 1979](#) (Cth).

1. Purpose

The purpose of this Better Practice Guide (BPG) is to address access to, and disclosure of health information collected and stored within OoCMO and SHIELD requested by business areas internal to the AFP.

This BPG applies to files held within OoCMO and SHIELD. Decisions about disclosure are made on a case-by-case basis following a review of the existing consents, the purpose for which the information is sought and the capacity to access and disclose under the:

- [Australian Federal Police Act 1979](#) (AFP Act)
- [Work Health and Safety Act 2011](#) (WHS Act)
- [Safety Rehabilitation and Compensation Act 1988](#) (SRC Act)
- [Privacy Act 1988](#) (Privacy Act).

2. Health files

The Australian Federal Police (AFP), as a Commonwealth agency is governed by the Privacy Act, which regulates the way personal information can be collected, used, stored and disclosed. The Privacy Act and the [Australian Privacy Principles \(APPs\)](#) set the minimum standards for handling of personal information by the Australian Government. All AFP personnel are required to comply with the APPs.

The Privacy Act regulates the use of health information in the AFP. Past or present AFP appointee's health information may be provided to relevant areas within the AFP if permitted under s.60A (secrecy) of the AFP Act.

OoCMO and SHIELD stores information pertaining to an AFP appointee's medical, psychological, rehabilitation and work health and safety status. This information is classified as Sensitive Personal information and OoCMO and SHIELD adheres to the Privacy standards of such information in accordance with the Privacy Act.

The personal information collected by OoCMO and SHIELD is unique to AFP appointees and applicants and is collected, stored and used for the purposes of:

- External recruitment
- internal recruitment
- deployment
- training
- general health maintenance
- Professional Standards investigations
- injury prevention

- Workplace injury management and rehabilitation.

OoCMO and SHIELD staff are AFP appointees and include registered Australian health practitioners under various professional streams who must meet legislated professional regulations around the management of health information,¹ in addition to their obligations under the AFP Act.

3. Purpose of access

OoCMO and SHIELD are lawfully permitted to divulge health information or other personal information without the express permission of the individual AFP appointee concerned to fulfil both internal and external requests, such as court or tribunal subpoena or summons and requests for information from AFP Professional Standards (PRS), AFP Security or AFP Legal. The health information that is made available for review is limited to that which is only relevant to the initial request.

In accordance with the requirements of the AFP Act and the Privacy Act, each OoCMO and SHIELD service area collects and stores personal information in a combination of hard copy file and electronic data formats. Those files are stored in a restricted-access compactus within their geographic location and on the AFP system in accordance with the [AFP National Guideline on information management](#).

Under the [AFP National Guideline on Information Security](#), information provided internally within the AFP is designated as 'use', not 'disclosure'. This information is unclassified, caveated with the Dissemination Limiting Marker of 'For Official Use Only' and 'Sensitive – Personal' material.

Access to and release of health information in these circumstances (where use is permissible rather than obligatory) requires OoCMO and SHIELD to be satisfied that the use of the information is reasonably necessary for the performance of the functions of the requesting person (in accordance with s. 60A (secrecy) of the AFP Act) and the terms of any consents provided.

Under the Australian Privacy Principles (APP), APP 6 outlines when an APP entity may use or disclose personal information. In summary, it states that:

- An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies
- the exceptions include where:
 - the individual has consented to a secondary use or disclosure
 - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose
 - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order
 - a permitted general situation exists in relation to the secondary use or disclosure
 - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure
 - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, or

¹ [Australian Health Practitioner Regulation Agency](#)

- the APP entity is an agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3.

It is also open to PRS to give a direction to OoCMO or SHIELD under section 40VE of the AFP Act. Compliance by OoCMO or SHIELD with such a direction is obligatory pursuant to subsection 40VE (3) of the AFP Act, and the provision of health information in response to such a legal requirement is therefore expressly permitted under APP 6.

Under paragraph 60A(2)(c) of the AFP Act, and APP 12.1, AFP appointees or former appointees can make direct request to OoCMO or SHIELD for a copy of their AFP Health file or part thereof. Under APP 12.4, OoCMO or SHIELD have 30 days to process these requests.

Under APP12, an agency is entitled to refuse access to personal information to an individual. If access is refused, or isn't delivered in the manner requested by the individual, the entity must give the individual a written notice that sets out:

- The reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so
- the mechanisms available to complain about the refusal
- any other matter prescribed by the regulations.

The request and proposed response must be checked with AFP Legal in the following circumstances:

- OoCMO or SHIELD are considering refusing to provide access in accordance with the request
- the request for health information of an AFP appointee comes from an external agency, with the exception of medical information held by Work Health Safety and Rehabilitation (WHSR).

The release of medical information for the purposes of injury prevention and rehabilitation under the WHS Act and the SRC Act is at the discretion of the Team Leader Injury Management or the delegated Rehabilitation Case Manager. Compliance by OoCMO and SHIELD with such a direction is obligatory pursuant to the relevant sections detailed within these Acts.

4. Health file access process

Requests for health information about AFP appointees should be progressed as per the flowchart at Attachment 1 of this BPG.

All queries for access to a health file must be in writing and must contain the context of the request. OoCMO or SHIELD personnel must be satisfied that the use of health information is consistent with the Commissioner's responsibilities under the Privacy Act and the AFP Act.

A medical summary will be provided (where considered appropriate by CMO or their clinical delegate) in the first instance, to ensure medical content is translated into suitable terminology. Where documents or detailed information is required, OoCMO or SHIELD will seek to provide the requested information to satisfy the context. Where there is material in the files which would not relate to the context, the requesting area will only be permitted to view material that is relevant, with areas not relevant redacted.

Requests must be processed using the attached 'AFP Health File Removal Authority Form' (Attachment 2) This request form will be kept in the appointee's health file for provenance and accountability reasons.

5. Resources

AFP Resources

[Australian Federal Police Act 1979 \(Cth\)](#)

[AFP Commissioner's Order on Governance \(CO1\)](#)

[AFP Commissioner's Order on Professional Standards \(CO2\)](#)

[AFP National Guideline on Information Security](#)

[AFP National Guideline on information management](#)

External Resources

[Privacy Act 1988](#)

[Australian Health Practitioner Regulation Agency](#)

[Australian Privacy Principles](#)

[Safety Rehabilitation and Compensation Act 1988](#)

[Work Health and Safety Act 2011](#)

Short Forms

AFP	Australian Federal Police
AFP Act	Australian Federal Police Act 1979
APP	Australian Privacy Principles
CMO	Chief Medical Officer
MS	Manager SHIELD
OoCMO	Office of the Chief Medical Officer
PRS	Professional Standards
SRC Act	Safety Rehabilitation and Compensation Act 1988
WHS Act	Work Health and Safety Act 2011
WHSR	Work Health Safety and Rehabilitation

Attachment 1 – Health File Access Flowchart

s 47E(d)

s 47E(d)

THIS DOCUMENT IS RELEASED BY
THE AUSTRALIAN FEDERAL POLICE UNDER THE
FREEDOM OF INFORMATION ACT 1982

Attachment 2 – AFP Health File Removal Authority Form



Date: __/__/__

[Name of requesting area] is requesting [nature of the request] on the basis of [reason that the use of the released information is legitimate].

The documents have been released to [Name of AFP Appointee] by [AFP OoCMO or AFP SHIELD] as required for the duration of [time frame]. These documents are authorised by law or for purposes within [60A \(secrecy\) of the AFP Act 1979](#) and the Ministerial Direction.

These documents will be stored in an appropriate manner to ensure the privacy of the AFP Appointee and compliance with AFP information handling and security requirements.

Document: [Description]

Provided To:

Print Name

.....

Sign

Function:

Estimated File Return Date:

Under the

Authority of:

Print Name

.....

Sign

Date: