13. MRS Online – Terms and Conditions

Part 1 — Preliminary

13.1. DAME Activities

13.1.1 In accordance with subregulation 67.180(2) of the CASR, DAMEs examine Applicants to assist CASA in determining the Applicants' suitability for medical certification. In performing this role, DAMEs will require access to MRS Online.

13.1.2 A DAME's functions under the CASR may also include:

a. extending a current medical certificate under subregulation 67.2220(1), and

b. issuing a new medical certificate under subregulation 67.225(3) where a medical certificate has expired.

13.1.3 Sections 2.4 and 11.1 provide further information about the role of DAMEs and the purpose of the medical examinations they perform.

13.2. Overview of MRS 2.0

13.2.1 From the Cutover Date, MRS Online is being upgraded to MRS 2.0. MRS 2.0 is a tool for processing applications for aviation medical certificates. It provides an online portal for Applicants to do the following:

a. apply for a medical certificate;

b. record medical information;

c. submit examinations;

d. make payments;

e. check the status of their application;

f. update their contact information.

13.2.2 MRS 2.0 also allows DAMEs, in real time within a secure online environment, to do the following:

a. carry out examinations and to submit examination findings;

b. identify an Applicant and receive alerts regarding the Applicant's medical history;

c. liaise with CASA.

13.2.3 MRS 2.0 retains all information entered so DAMEs can reuse it at future examinations. The information contained in MRS Online (**MRS Records**) comprises

Sensitive Information about Applicants and their physical/mental health or disabilities.

13.2.4 For the purpose of DAME Activities, CASA will provide DAMEs with access to MRS Online subject to these Terms and Conditions.

13.3. CASA's privacy obligations

13.3.1 CASA's ability to Use Personal Information contained in MRS Records is regulated by the Privacy Act and by the APPs established under that Act.

13.3.2 The APPs impose various duties on CASA to appropriately manage and protect the Personal Information it Holds, especially Sensitive Information. These duties include obligations to take reasonable steps to undertake the following:

a. implement practices, procedures and systems for ensuring compliance with the APPs (APP 1.2);

b. ensure the Personal Information it collects and Uses is up-to-date, complete and secure (APP 10);

c. protect the Personal Information it Holds from misuse and unauthorised disclosure (APP 11.1).

13.3.3 Aside from its legal obligations, CASA is accountable for ensuring that Individuals can trust it to appropriately handle and protect their Personal Information.

13.3.4 These Terms and Conditions have therefore been designed to ensure CASA can satisfy not only its obligations in this regard but community expectations as well.

13.4. Access rights to MRS 2.0

13.4.1 DAMEs can access MRS 2.0 for training or clinical purposes related to examinations. As appropriate, they can also Use MRS 2.0 to:

a. upload reports and information for CASA to consider in assessing an Applicant's suitability to hold, or continue to hold, an aviation medical certificate, and

b. in relation to Applicants they examine, email those Applicants (and only those Applicants) certain MRS Records relating to them.

13.4.2 CASA has configured the MRS 2.0 to grant DAMEs access rights to all MRS Records, other than CASA's internal records. However, those rights are subject to DAMEs complying with these Terms and Conditions, including the duty only to access records they require for a legitimate purpose. To enforce this requirement, CASA monitors and routinely audits access to MRS Online, as noted at subsection 13.5.2.

13.4.3 Where relevant to their duties, DAME Personnel will also be able to access MRS 2.0 as Authorised DAME Personnel, though their access rights will be restricted to

prevent them from accessing more information than they reasonably require to perform duties in support of DAME Activities.

13.4.4 DAMEs are liable for all –

a. actions logged under MRS Online log-ins assigned to them or to Authorised DAME Personnel; and

b. access to MRS Online by any DAME Personnel.

Part 2 — Guide to Terms and Conditions

13.5. Objectives

13.5.1 These Terms and Conditions set out various security measures DAMEs must adopt to protect MRS Records from misuse and unauthorised access/disclosure. These measures include ensuring the records are only accessed by those who are permitted to have them and who require them for a legitimate purpose.

13.5.2 CASA has taken certain security measures to protect MRS Records. These measures include ensuring that MRS Online is only accessible to DAMEs and Authorised DAME Personnel using individual logins. CASA conducts regular audits of system access and may contact DAMEs as a part of the audit process. CASA also has tools for detecting excessive or inappropriate use of MRS Online and will investigate any suspected instances of these sorts.

13.6. Overview of main Parts

13.6.1 The detailed requirements for DAMEs in using MRS Online are set out at Part 4 to Part 8. Part 9 and Part 10 relate to arrangements for administering MRS Online.

13.6.2 Part 4 requires DAMEs to establish a privacy management framework for handling and protecting MRS Records. This is principally to ensure compliance with APPs 1.2 and 1.3.

13.6.3 Part 5 sets out the circumstances in which DAMEs can Collect, Use and Disclose MRS Records. It prohibits DAMEs from doing these things otherwise. This is principally to ensure compliance with APP 11.1.

13.6.4 Part 6 describes requirements for DAMEs to do each of the following:

a. ensure the quality of Personal Information contained in MRS Records whenever they Collect, Use or Disclose this information;

b. not upload Material that is defamatory, misleading, inflammatory or offensive;

c. store MRS Records securely;

d. destroy or de-identify Personal Information in Disused Records, where authorised by CASA;

e. destroy or return MRS Records (other than Relevant Records) where demanded by CASA;

f. remove and, if required, replace a Relevant Record that CASA reasonably objects to.

13.6.5 These requirements are to satisfy APPs 10 and 11. They assist to ensure that, whenever a DAME uploads a Relevant Record, the Personal Information in those records is as accurate as possible and up-to-date at the time of uploading.

13.6.6 Part 7 describes requirements for DAMEs to correct or alter Personal Information in Relevant Records, but generally only where it has notified CASA first. These requirements are to ensure compliance with APP 13. They include a duty for DAMEs to upload corrected versions of Relevant Records that are found to contain incorrect, inaccurate or incomplete Personal Information.

13.6.7 Part 8 details security measures DAMEs must adopt to protect MRS Records. These are to ensure compliance with APP 11 and to protect CASA's reputation as a trusted holder of Sensitive Information.

13.6.8 Part 9 sets out arrangements for managing IP Rights. The purposes of these provisions are as follows:

a. enable Material to be uploaded to MRS Online and shared without breaching IP Rights or Moral Rights;

b. prohibit DAMEs from uploading Material if this would infringe another person's IP Rights or Moral Rights;

c. permit DAMEs to continue to own IP Rights in the Material they create and upload;

d. grant CASA rights to use Relevant Records, including a right to license it to others for DAME Activities.

13.6.9 Part 10 relates to the general terms and conditions such as:

a. the duty of DAMEs to cooperate in CASA's running of MRS Online, including a duty to assist in resolving an MRS Online inquiry, investigation or complaint; and

b. a disclaimer of CASA's liability for any loss resulting from errors in MRS Records.

13.6.10 Part 10 also sets out transitional arrangements for Existing DAMEs who require some time after the Cutover Date to establish a compliant privacy management framework or practices for managing Redundant Accounts or Compromised Accounts.

13.7. Relationship to codes of ethics

13.7.1 The obligations imposed on DAMEs through these Terms and Conditions parallel many of the ethical and privacy obligations of all medical practitioners to safeguard a patient's personal health record. These include the obligations of doctors under:

a. clause 1.1 of the AMA Code of Ethics to:

(i) maintain patient confidentiality; and

(ii) ensure patient information is stored, accessed and utilised securely;

b. the Medical Board of Australia's *Good medical practice: A code of conduct for doctors in Australia* to:

(i) protect patient privacy and confidentiality (clause 3.4); and

(ii) ensure medical records are held securely and protected against unauthorised access (clause 8.4.2);

c. The Royal Australasian College of Physicians' *Guidelines on ethics and professional conduct for occupational physicians* to:

(i) strictly control access to medical records by occupational health service employees (clause 2.1); and

(ii) employ appropriate security measures for storing or transmitting medical information (clause 2.2).

13.8. Breach of Terms and Conditions

13.8.1 In relation to DAMEs subject to Part 67 of the CASR, any DAME who breaches these Terms and Conditions will be regarded by CASA as having breached their conditions of appointment under regulation 67.060 or 67.080 of the CASR. This includes conditions under subregulations 67.060 (1) and 67.080 (1) that DAMEs observe the AMA Code of Ethics. Consequently any breach of these Terms and Conditions may result in CASA cancelling the DAME's appointment under paragraph 67.095(1)(c) of the CASR for failing to meet a requirement for holding their appointment.

13.8.2 COs are not subject to Part 67 of the CASR. Each CO is appointed by Optometry Australia to perform particular DAME Activities (i.e. aviation eye examinations) under an agreement made between them, CASA and Optometry Australia. This agreement includes the Credentialed Optometrist Rules (**CO Rules**). The CO Rules oblige COs to comply with:

a. the Optometry Board of Australia's *Code of Conduct for optometrists* (paragraph 3.1(d)); and

b. the DAME Handbook (paragraph 3.1(f)(viii)).[1]

[1] This paragraph currently refers to the DAME Handbook as the DAO Handbook.

13.8.3 Consequently any breach of these Terms and Conditions by a CO may result in Optometry Australia cancelling the CO's appointment under rule 3.4 of the CO Rules.

13.8.4 CASA may, in writing, cancel or suspend MRS Online access of any DAME or Authorised DAME Personnel if CASA is satisfied that any of the following has occurred:

a. the DAME or any DAME Personnel has breached these Terms and Conditions;

b. the cancellation or suspension is reasonably necessary to prevent a breach of these Terms and Conditions;

c. MRS Online's security or integrity has been, or may be, Compromised by the ICT System of their DAME Organisation;

d. the cancellation or suspension is otherwise appropriate, having regard to the need to protect MRS Online's security and integrity.

13.8.5 CASA may, in writing, suspend MRS access of any DAME or Authorised DAME Personnel while it investigates whether to take action under subsection 13.18.4 in relation to that person's access.

Part 3 — Terminology

13.9. Definitions

13.9.1 For chapter 13, the following terms and abbreviations have the following meanings:

Term/Abbreviation	Meaning
AMA Code of Ethics	is the Australian Medical Association's *Code of Ethics*.
AMA Privacy and Health Record Resource Handbook	means the Australian Medical Association's *Privacy and health record resource handbook*.
Applicant	means a pilot or air traffic controller who applies to CASA for an aviation medical certificate under Part 67 of the CASR.
Authorised DAME Personnel	means any DAME Personnel who needs access to MRS Online because of their duties in supporting DAME Activities. This includes a nurse or receptionist responsible for assisting an Applicant to book a medical examination with a DAME.
CISS	means the Royal Australian College of General Practice's *Computer and information security standards*.
CO Rules	has the meaning given at subsection 13.8.2.

Term/Abbreviation	Meaning
Collects	includes, in relation to the collection of Personal Information or an MRS Record, gathers, acquires or obtains from any source (including from an Individual) and by any means.
Commonwealth or **Cth**	means the Commonwealth of Australia.
Compromise	means any action that results in the loss, corruption or unauthorised Disclosure of protected information, or damage to any Material containing the information.
Compromised Account	means, in relation to an Authorised DAME Personnel's user account on an ICT System, an account that has been Compromised. This includes an account for which the password or other access mechanism has been Compromised.
Copyright Act	is the *Copyright Act 1968* (Cth).
Cutover Date	is 21 March 2016, being the date MRS 2.0 is launched as an online tool as described at section 13.2.
DAME Activity	means an activity performed by a DAME for the purpose of fulfilling their role as described at section 13.1. It includes training on the Use of MRS Online, as described at subsection 13.4.1.
DAME Organisation	means the organisation for which the DAME works in performing DAME Activities.
DAME Personnel	means any natural person who is an employee, officer, agent or subcontractor of a DAME Organisation (other than a DAME).
Data Breach	means a situation in which Personal Information contained in an MRS Record Held or Used by a DAME or a DAME Organisation is Compromised, lost or is Used/Disclosed without authorisation.
DBR Plan	means a DAME Organisation's Data Breach response plan, as described at section 13.12.
Disclose	includes, in relation to the disclosure of Personal Information or an MRS Record, make accessible to others.
Disused Records	has the meaning given at subsection 13.6.1.
Existing DAME	has the meaning given at subsection 13.18.1.
Existing Material	means Material developed independently of DAME Activities that is incorporated in or supplied as part of a Relevant Record.
Firewall	means a device that controls the flow of traffic between two ICT networks, acts as a filter on Material passing between the networks and allows only authorised traffic to pass through it.

Term/Abbreviation	Meaning
Holds	means, in relation to the holding of Personal Information or MRS Records, controls, possesses or has a right/power to deal with.
ICT System	means an information technology system used by a DAME Organisation that enables DAMEs and Authorised DAME Personnel to access MRS Online in order to perform or support DAME Activities. It includes all data, software, applications and business systems held within, or transmitted over, the organisation's ICT environment.
Individual	means, in relation to Personal Information, the individual to whom the information relates.
Intellectual Property Rights or IP Rights	means all copyright, patents, registered and unregistered trademarks (including service marks), registered designs, and other rights resulting from intellectual activity (other than Moral Rights).
Law	means any applicable statute, regulation or subordinate legislation in force from time to time in Australia, whether made by a State, Territory or the Commonwealth. It includes the common law and rules of equity as applicable from time to time.
Material	includes documents, equipment, software (including source code and object code versions), goods, information and data stored by any means including all copies and extracts of them.
Moral Right	has the meaning given at section 189 of the Copyright Act.
MRS 2.0	means the new version of MRS Online, as described at clause 13.2.
MRS Online	includes MRS 2.0.
MRS Records	means the information contained in MRS Online, as described at subsection 13.2.3. It includes Personal Information contained in a record, as well as specialist medical reports and clinical test results.
OAIC	means the Office of the Australian Information Commissioner.
Privacy Act	is the *Privacy Act 1988* (Cth).
Privacy Policy	means a DAME Organisation's privacy policy, as described at subsection 13.11.1.
Reasonable Steps	has the meaning give at subsection 13.9.2.
Redundant Account	means, in relation to a user account on an ICT System, the account of an Authorised DAME Personnel who has left the DAME Organisation or who no longer requires access to MRS 2.0.

Term/Abbreviation	Meaning
Relevant Record	means an MRS Record created, or uploaded to MRS, by or at the direction of a DAME for a DAME Activity.
Terms and Conditions	means the terms and conditions on which CASA permits DAMEs to Use MRS Online, as set out in this chapter 13.
Use	includes, in relation to the use of Personal Information or an MRS Record, accessing, viewing, handling, cross-matching, searching, downloading, copying, printing, storing or otherwise handling that information/record.

13.9.2 The term **Reasonable Steps** means, in relation to ensuring the quality and security of MRS Records, or to correcting or destroying an MRS Record, such steps as are reasonable in the circumstances, having regard to the following:

a. the amount and sensitivity of the information;

b. the resources and business model of the DAME Organisation;

c. the risks and possible adverse consequences for the Individual if the steps are not taken;

d. the information handling practices of the DAME Organisation, as set out in its Privacy Policy;

e. the practicability of taking the steps, including the time and cost involved;

f. in relation to steps taken to verify an Individual's identity, the steps are not unduly invasive and do not require the Individual to supply more information than is necessary for verification.

For further guidance about Reasonable Steps required to protect Personal Information in MRS Records, DAMEs should have regard to Part A of the OAIC's Guide to Securing Personal Information.

13.9.3 The terms **DAME** and **doctor** have the meanings given at section 11.1.

13.9.4 The terms **Australian Privacy Principles (APPs)**, **Personal Information** and **Sensitive Information** have the meanings given in section 6 of the Privacy Act.

13.9.5 Other abbreviations used in this chapter 13 (e.g. **CASA**, **CASR, CO** and **MRS Online**) have the meanings given at section 1.1 of this Handbook.

13.10. Interpretation

13.10.1 In this chapter 13, unless otherwise stated:

a. words in the singular number include the plural and words in the plural number include the singular

b. headings are inserted for convenience only and do not affect the interpretation of these Terms and Conditions

c. words in text boxes operate as guidance notes only and are not to be regarded as obligatory provisions

d. all references to parts, sections and subsections are to parts, sections and subsections of this chapter

e. all references to chapters are to chapters of this Handbook, and

f. where any word or phrase is given a defined meaning, any other part of speech or other grammatical form in respect of that word or phrase has a corresponding meaning.

13.10.2 To the extent that there is any inconsistency between this chapter 13 and any other chapter, the provisions of this chapter 13 will prevail.

Part 4 — Privacy Management Framework

13.11. Establish privacy practices, procedures and systems

13.11.1 Each DAME must ensure their DAME Organisation develops, implements, communicates and enforces a Privacy Policy applicable to the organisation's management of MRS Records. The policy must be:

a. clearly expressed; and

b. reviewed at least annually or whenever any new risk is identified.

13.11.2 If the DAME Organisation already has a Privacy Policy that can be applied or adapted to the DAME's management of MRS Records, the DAME can satisfy subsection 13.11.1 by using that policy and updating it as required.

13.11.3 As a minimum, the Privacy Policy must describe processes for each of the following:

a. ensuring the Personal Information the DAME Organisation collects and Discloses is accurate, up-to-date and complete;

b. using, storing and disclosing Personal Information;

c. receiving and responding to privacy enquiries and complaints;

d. allowing individuals to promptly and easily access and correct their Personal Information;

e. employing appropriate measures (e.g. access control mechanisms, Firewalls, routing controls, copy protection and encryption measures) to ensure access is limited to:

(i) DAMEs;

(ii) on a need-to-know basis - Authorised DAME Personnel;

f. identifying, assessing and managing security risks with Personal Information, including steps for:

(i) ensuring Personal Information is appropriately handled by DAMEs and DAME Personnel (e.g. staff training and accountability/oversight measures);

(ii) safely transferring and tracking the movement of Personal Information inside the DAME Organisation (e.g. measures for controlling the use of portable storage devices);

(iii) suspending or deactivating any Compromised Account or Redundant Account;

(iv) conducting regular reviews of security controls;

g. responding to any Data Breach in accordance with a DBR Plan;

h. destroying Personal Information that is no longer required for any legitimate business purpose, as required by APPs 4.3 and 11.2 (but in the case of MRS Records only where directed or authorised by CASA).

13.11.4 DAMEs must ensure these processes are systematically reviewed to ensure they remain effective and appropriate. Their Privacy Policy must demonstrate how and how often these reviews will occur.

DAMEs should prepare their Privacy Policy in accordance with the OAIC's Guide to developing an APP privacy policy. The RACGP's privacy policy template on handling patients' health records can be amended to include MRS Records.

13.11.5 CASA may, at any time, request a DAME to provide their Privacy Policy to check it is adequate for the purposes of this Part 4. The DAME must promptly comply with any request of this sort.

13.12. DBR Plan

13.12.1 This section 13.12 applies to DBR Plans, to the extent they can be applied to Data Breaches.

13.12.2 Each DAME must ensure their DAME Organisation develops, implements, communicates and enforces a DBR Plan setting out actions to be taken in response to a Data Breach and the personnel responsible for performing them. The plan must be:

a. clearly expressed;

b. reviewed at least annually or whenever any new risk is identified.

13.12.3 If the DAME Organisation already has a DBR Plan that can be applied or adapted to the DAME's management of MRS Records, the DAME can satisfy subsection 13.12.1 by using that plan and updating it as required.

13.12.4 As a minimum, the DBR Plan must describe the following:

a. a strategy for assessing and containing Data Breaches, including the roles of personnel responsible for implementing the strategy;

b. procedures for detecting Data Breaches, such as:

(i) network 'security alarm' tools (e.g. intrusion detection/data loss prevention software, audit analysis and countermeasures against malicious code);

(ii) training for DAMEs and DAME Personnel to identify and report errors in handling Personal Information;

c. how a breach can be identified and what constitutes a breach (including internal errors or failures to follow information handling processes);

d. when and how a breach should be:

(i) notified to the affected individual and other third parties (which, in the case of MRS Records, include CASA) so they can take steps to mitigate its effects;

(ii) if required — escalated to the DAME Organisation's response team;

e. how the identification and response to a Data Breach will be recorded;

f. processes for evaluating the risks associated with a breach and for implementing measures to prevent future breaches.

DAMEs should prepare their DBR Plan in accordance with the OAIC's Data breach notification guide: a guide to handling personal information and security breaches. Further guidance on preparing a DBR Plan is available at section 2 of the CISS.

13.12.5 CASA may, at any time, request a DAME to provide their DBR Plan to check whether it is adequate for the purposes of this section 13.12. The DAME must promptly comply with any request of this sort.

Part 5 — Dealing with MRS Records

13.13. Dealings by DAMEs

13.13.1 A DAME must not Collect, Use or Disclose an MRS Record except in accordance with this section 13.13. In particular, a DAME must not Use an MRS Record unless they genuinely need to do so for a DAME Activity.

13.13.2 A DAME may Collect, Use and Disclose an MRS Record where the collection, Use or disclosure is for any of the following:

a. for the purpose of performing a DAME Activity;

b. for the purpose of managing or operating MRS Online;

c. in response to a request by CASA.

13.13.3 A DAME may Use or Disclose an MRS Record containing Personal Information in any of the following circumstances:

a. they reasonably believe that:

(i) the Use or disclosure is necessary to lessen or prevent a serious threat to an Individual's life, health or safety; and

(ii) it is unreasonable or impracticable to obtain the Individual's consent;

b. they notify CASA of the matters in paragraph a and identify any person to whom an MRS Record is Disclosed;

c. where the notice under paragraph b relates to a disclosure, the disclosure occurs within five days after the notice is given.

13.13.4 A DAME may Collect, Use and Disclose an MRS Record if the collection, Use or disclosure is required or authorised by Law.

13.13.5 Where the DAME discloses an MRS Record under subsection 13.13.4, the DAME must notify CASA of the reasons for the disclosure and the identity of the entity to which the record was disclosed.

13.13.6 A DAME may Disclose an MRS Record containing Personal Information to an Individual if the DAME is reasonably satisfied the disclosure is reasonably necessary for a DAME Activity or for the Individual's health treatment.

13.13.7 If:

a. an Individual asks a DAME for access to an MRS Record containing Personal Information; but

b. the DAME determines the request cannot be granted under subsection 13.13.6,

the DAME may not Disclose the record but may notify the Individual they can request it from CASA under APP 12.1 or under the *Freedom of Information Act 1982* (Cth).

13.13.8 Where a DAME is permitted under subsection 13.13.6 to Disclose to an Individual an MRS Record containing Personal Information, the DAME may not disclose it to anyone else unless that disclosure is permitted under another provision of this section 13.13.

13.14. Dealings by Authorised DAME Personnel

13.14.1 This section 13.14 applies to any Authorised DAME Personnel for whom a DAME or their DAME Organisation is responsible.

13.14.2 A DAME must ensure Authorised DAME Personnel do not Collect, Use or Disclose an MRS Record except in accordance with this section 13.14. In particular, a DAME must ensure that Authorised DAME Personnel do not Use an MRS Record unless they genuinely need to do so in support of DAME Activities.

13.14.3 Authorised DAME Personnel may only Collect and Use an MRS Record where the collection, Use or disclosure is for the following:

a. for the purpose of performing a duty in support of DAME Activities;

b. for the purpose of administrative management or operation of MRS Online;

c. in response to a request by CASA.

13.14.4 Where an Individual requests Personal Information contained in an MRS Record, such information must only be disclosed by the DAME, excepting system information about periodic and special test requirements relating to medical certification.

> *For further guidance about the Use and Disclosure of Personal Information in MRS Records, DAMEs should have regard to:*
>
> *(a) the CISS;*
>
> *(b) section 3 of the AMA Privacy and Health Record Resource Handbook;*
>
> *(c) Part B of the OAIC's Guide to Securing Personal Information.*

Part 6 — Integrity of MRS Records

13.15. Quality of MRS Records

13.15.1 DAMEs must take Reasonable Steps to ensure that, whenever they Collect, Use or Disclose Personal Information contained in an MRS Record, that information is accurate, up-to-date and complete.

13.15.2 As appropriate, the steps a DAME must take under subsection 13.15.1 may include the following:

a. implementing procedures to monitor the quality and accuracy of the Personal Information it Holds and where practical, to update that information on a regular basis;

b. ensuring that updated or new Personal Information, once verified, is promptly added to relevant MRS Records;

c. where the DAME proposes to Use or Disclose Personal Information that has not been verified recently, contacting the Individual to check it is still accurate and up-to-date;

d. conducting due diligence to ensure that Personal Information Collected from a third party is reliable (e.g. by checking that it has appropriate quality practices);

e. assessing the quality of Personal Information before using it for a new purpose.

13.15.3 DAMEs must not upload or create an MRS Record that contains defamatory, misleading, inflammatory or offensive Material.

13.16. Storage and security of MRS Records

13.16.1 DAMEs will take Reasonable Steps to protect against Data Breaches in relation to any MRS Records they Hold or Use or their DAME Organisation Holds or Uses.

13.16.2 DAMEs must ensure that all MRS Records containing Personal Information are stored and managed and in compliance with the security requirements described at Part 8.

13.16.3 In accordance with those requirements, DAMEs must ensure access to those records will be restricted to themselves and to Authorised DAME Personnel within their DAME Organisation.

13.17. Destruction of Personal Information in Disused Records

13.17.1 This section 13.17 applies to MRS Records containing Personal Information, being records the DAME no longer requires for any Use or disclosure allowed under the APPs (**Disused Records**).

13.17.2 DAMEs must not destroy or de-identify any MRS Records except as authorised or required in writing by CASA.

13.17.3 In relation to any Disused Record a DAME Holds, the DAME must destroy or de-identify any Personal Information in that record where authorised or required by CASA under subsection 13.17.2.

13.17.4 Where a DAME is required to keep a Disused Record, they must ensure the record is stored separately from the DAME Organisation's operational information and preserved in accordance with any reasonable requirements set by CASA.

13.18. Destruction of MRS Records on demand

13.18.1 CASA may, at any time, request in writing for a DAME to destroy an MRS Record Held by the DAME (other than a Relevant Record).

13.18.2 Unless subsection 13.18.3 applies, a DAME must do the following:

a. promptly comply with any demand made by CASA under subsection 13.18.1;

b. if required by CASA — provide CASA with an assurance it has complied with the request.

13.18.3 A DAME is not required to comply with a request by CASA under subsection 13.18.1 to destroy Material in an MRS Record if the DAME is required by Law to retain the Material and has so informed CASA in writing.

13.18.4 If CASA makes a request under subsection 13.18.1 relating to Material contained in an MRS Record that the DAME:

a. has Disclosed to another person pursuant to subsections 13.13.3 or 13.13.4; or

b. knows has otherwise been placed so that it is beyond the possession or control of the DAME or the DAME Organisation,

the DAME must provide full particulars (so far as they are known to the DAME) of the whereabouts of that Material and the identities of those who possess or control it.

13.19. Removal of Relevant Records

13.19.1 CASA may effectively remove from MRS, or may direct a DAME to effectively remove from MRS, a Relevant Record to the extent CASA reasonably considers that the record:

a. contains a defamatory, misleading, inflammatory or offensive statement; or

b. affects, or is likely to affect, MRS Online's security or integrity.

13.19.2 Where CASA exercises its rights under subsection 13.19.1:

a. it must give the responsible DAME written notice of the removal and provide reasons for its decision; and

b. it may direct the DAME to:

(i) upload a replacement record addressing CASA's concerns; and

(ii) notify CASA when it has done so.

Part 7 — Correction of Relevant Records

13.20. Correction of Relevant Record at CASA's request

13.20.1 This Part 7 applies where CASA is required under APP 13 to correct or alter Personal Information contained in a Relevant Record.

13.20.2 CASA may request a DAME to do the following:

a. correct or alter Personal Information in a Relevant Record;

b. upload the amended record to MRS;

c. notify CASA when it has done so.

13.20.3 If a DAME refuses to comply with a request under subsection 13.20.2, CASA may direct the DAME to do the following:

a. attach to the record a statement prepared by the Individual in relation to the Personal Information contained in the record;

b. upload the record and statement to MRS;

c. notify CASA when it has done so.

13.21. Correction of Relevant Record on DAME's initiative

13.21.1 Where a DAME is satisfied a Relevant Record it Holds is incorrect, or an Individual is able to establish it is incorrect, the DAME must (subject to subsection 13.21.3) take Reasonable Steps to correct the information so that it is accurate, complete and up-to-date.

13.21.2 Where this information is in a Relevant Record that is over 15 years old, the DAME must not alter the record, but must do the following:

a. prepare a statement to:

(i) note the information is not correct;

(ii) describe the correct information or else identify where it is Held;

b. attach the statement to the record;

c. upload the record and the statement to MRS;

d. notify CASA when it has done so.

13.21.3 The DAME must not correct, alter or attach a statement to any Relevant Record without first notifying CASA in writing that the DAME intends to do so.

13.21.4 A DAME must not alter any MRS Record other than a Relevant Record except as authorised or required in writing by CASA.

13.22. Correction of Relevant Record at Individual's request

13.22.1 Where an Individual requests a DAME to correct Personal Information in a Relevant Record, the DAME must respond to the request within 30 days and must not charge for the request or for any corrections it makes.

13.22.2 If the DAME refuses an Individual's request under subsection 13.22.1, the DAME must:

a. give the Individual a written notice setting out the reasons for its refusal;

b. provide CASA with a copy of that notice.

13.22.3 If the DAME agrees to an Individual's request under subsection 13.22.1, it may correct or alter the Relevant Record in accordance with the procedure described at section 13.21.

Part 8 — Protective security

13.23. Overview of security measures

13.23.1 DAMEs must ensure that their DAME Organisations implement appropriate safeguards to protect MRS Records they Collect, Hold or Use. These safeguards must include measures for maintaining the following security types for the purposes required under the organisation's Privacy Policy:

Security type	Meaning
a. Physical security	includes physical measures designed to: • prevent Data Breaches and to detect and respond to intruders; • ensure appropriate storage of MRS Records Held by the organisation; and • ensure the secure destruction of MRS Records, or of Personal Information in Disused Records, where required or authorised by CASA.
b. Information security	means a procedural system implemented to protect against Data Breaches.
c. ICT security	means technological measures designed to ensure the ICT System: • restricts MRS access to DAMEs and Authorised DAME Personnel (e.g. access control mechanisms and encryption measures); • can monitor and audit the Use of MRS Records within the DAME Organisation; and • prevent and detect Data Breaches (e.g. copy protection, Firewalls, routing controls, intrusion detection/data loss prevention software). These measures include those required under clause 13.24.
d. Personnel security	means a procedural system implemented to ensure that the only people who are able to access MRS are: • DAMEs; • Authorised DAME Personnel whose suitability for having access has been determined by an appropriate evaluation process.

13.23.2 The security safeguards required under subsection 13.23.1 must reflect:

a. the sensitivity of the MRS Records they are designed to protect, and

b. the damage CASA or the Individual could suffer as a result of any Data Breach relating to those records.

For further guidance about security measures required to protect Personal Information in MRS Records, DAMEs should have regard to:

(a) the CISS;

(b) sections 3 and 4 of the AMA Privacy and Health Record Resource Handbook; and

(c) Part B of the OAIC's Guide to Securing Personal Information.

13.24. User account management within DAME Organisation

13.24.1 This section 13.24 applies to ICT Systems, to the extent they allow access to MRS.

13.24.2 Each DAME must ensure their DAME Organisation employs an ICT System with the following features for managing user accounts:

a. control mechanisms to ensure access to the system is limited to:

(i) DAMEs;

(ii) on a need-to-know basis — Authorised DAME Personnel;

b. access mechanisms (e.g. passwords) that:

(i) are sufficiently secure and robust to manage the risk of Data Breaches;

(ii) oblige users to change their password at least every 90 days or whenever they suspect their password has been Compromised;

(iii) do not permit users to reuse any password they have used within the past year;

(iv) suspend access after five unsuccessful log-on attempts or where an account has been inactive for more than 60 days;

c. audit logs and security controls to:

(i) monitor and audit the Use of MRS Records within each account;

(ii) identify any Data Breach or misuse of access privileges, whether attempted or actual;

(iii) protect the integrity of MRS Records Held by the organisation.

13.24.3 Each DAME must ensure their DAME Organisation employs the following practices for managing user accounts on ICT Systems:

a. any Redundant Account is deactivated within a reasonable period after it becomes redundant;

b. any Compromised Account is suspended or deactivated as soon as practicable after the DAME Organisation becomes aware it has been compromised,

in accordance with the procedures documented in the organisation's Privacy Plan, as required under paragraph 13.11.3f(iii).

13.25. Notification of changes and Data Breaches

A DAME must promptly notify CASA if any of the following occur:

a. their contact details change;

b. there is a material change in the legal structure or beneficial control of the DAME Organisation;

c. any Authorised DAME Personnel no longer require MRS access (e.g. due to a change in their position or responsibilities);

d. the DAME knows or suspects MRS Online's security has been Compromised by a Data Breach.

Part 9 — Intellectual Property

13.26. Scope of this Part

This Part 9 applies to Relevant Records and other Material uploaded to MRS by a DAME.

13.27. Existing Material

Nothing in this Part 9 affects the ownership of IP rights in any Material to which this part applies or any IP Rights in existing Material.

13.28. IP Rights in Material uploaded to MRS

13.28.1 A DAME must not upload Material to MRS unless they satisfying either of the following:

a. own the IP Rights in that Material;

b. have all rights and licences to upload it and to allow it to be used for DAME Activities or other MRS purposes.

13.28.2 Each DAME grants to CASA a fee-free, non-exclusive, irrevocable, world-wide licence to Use, reproduce, adapt, communicate and publish the Material for any purpose relating to its functions under section 9 of the *Civil Aviation Act 1988* (Cth). The licence granted to CASA under this subsection 13.28.2 includes rights to:

a. sublicense the Material to any person; and

b. to Disclose the Material to any of the persons described at subregulation 67.180 (4) of the CASR for the purpose of an examination under subregulation 67.180 (2) of the CASR.

13.28.3 CASA grants to each DAME a fee-free, non-exclusive, irrevocable, world-wide licence to Use, reproduce, adapt, communicate and publish the Material they have accessed or downloaded from MRS for DAME Activities. The licence granted to DAMEs under this subsection is subject to the restrictions imposed by Part 5.

13.28.4 To the extent permitted by Law and for the benefit of CASA, a DAME consents, and must use best endeavours to ensure that each author of the Material consents in writing to the use by CASA of the Material, even if the use may otherwise be an infringement of the author's Moral Rights (other than the right not to have authorship of their work falsely attributed).

Part 10 — General terms and conditions

13.29. Duty to provide assistance

Where requested by CASA, a DAME must provide reasonable assistance in relation to any inquiry, investigation or complaint in connection with MRS Online's operation, including any Data Breach.

13.30. Duty to provide evidence of compliance measures

13.30.1 CASA may, at any time, request a DAME to provide any information CASA may reasonably require (including details about what security measures or procedures its DAME Organisation has implemented) to be satisfied the DAME has complied with its obligations under Part 4 to Part 8.

13.30.2 A DAME must promptly comply with any request made by CASA under subsection 13.30.1.

13.31. Duty to improve compliance measures where directed

13.31.1 If CASA reasonably considers the compliance measures a DAME or their DAME Organisation has employed are insufficient to fulfil any of the DAME's obligations under Part 4 to Part 8, it may direct the DAME to implement whatever improvements CASA reasonably considers are required to remedy that deficiency.

13.31.2 A DAME must promptly comply with any direction made by CASA under subsection 13.31.1.

13.32. No warranty for accuracy of MRS Records

13.32.1 CASA operates MRS Online so that DAMEs can upload and access MRS records, subject to any access controls. However CASA is not responsible for the quality or content of any MRS Records uploaded by DAMEs.

13.32.2 These Terms and Conditions reference several external resources on Personal Information security. CASA is not responsible for those publications and does not warrant the accuracy of their contents.

13.32.3 CASA accepts no liability for any loss a DAME may suffer as a result of using or relying on the contents of any of the following:

a. an MRS record;

b. any other Material accessed through MRS;

c. any external resource referred to in these Terms and Conditions.

13.32.4 CASA does not guarantee continuity of access to, or operation of, MRS.

13.33. Transitional arrangements for Existing DAMEs

13.33.1 This section 13.33 applies to doctors and other medical practitioners approved by CASA as DAMEs as at the Cutover Date (**Existing DAMES**).

13.33.2 If, at the Cutover Date, the DAME Organisation of an Existing DAME does not have:

a. a Privacy Policy complying with section 13.11; or

b. a DBR Plan complying with section 13.12; or

c. practices for managing Redundant Accounts or Compromised Accounts in accordance with section 13.24,

the DAME will not breach their obligations under those sections if they do all of the following:

d. notify CASA in writing by 1st May 2016 that they do not yet comply with any of those requirements and specify which ones;

e. ensure the DAME Organisation takes all steps necessary to remedy that non-compliance by 1st June 2016 (or any later date agreed by CASA);

f. confirm to CASA by 8th June 2016 (or any later date agreed by CASA) they have complied with paragraph e.

13.33.3 For the avoidance of doubt, subsection 13.33.2 does not derogate from:

a. any other obligations of an Existing DAME under these Terms and Conditions; or

b. any obligations already applying to an Existing DAME under:

(i) the Privacy Act, CASR or any other Law; or

(ii) any code of conduct or ethics, including the codes referred to at subsection 13.7.1.