



General

1. This Code of Conduct and related materials apply to UK CAA medical information of all types.
2. This information may consist of:
 - digital or hard copy CAA Medical health records (including those concerning all specialties and GP / NHS medical records);
 - digital or printed X-rays, photographs, slides and imaging reports, outputs and images;
 - digital media (including, for example, data tapes, CD-ROMs, DVDs, USB disc drives, removable memory sticks, and other internal and external media compatible with CAA information systems);
 - computerised records, including those that are processed in networked, mobile or standalone systems;
 - email, text and other message types.
3. All individuals who work with, or under contract to, an UK CAA certificated AME or AeMC have a general responsibility for the security of information that they create or use in the performance of their duties.
4. Medical information is generally held under legal and ethical obligations of confidentiality. Information provided in confidence should not be used or disclosed in a form that might identify an individual without their consent.
5. Applicant health information and their interests must be protected through a number of measures:
 - Procedures to ensure that all staff are at all times fully aware of their responsibilities regarding confidentiality;
 - Recording personal information accurately and consistently;
 - Keeping personal information private;
 - Keeping personal information physically secure;
 - Disclosing and using information with appropriate care.
6. Applicant medical information should be recorded accurately and consistently: If records are inaccurate, future decisions could be impacted or influenced.
7. Keeping personal information physically and electronically secure. You should not leave portable computers, medical notes or files in easily accessible areas. Ideally, store all files and portable equipment under lock and key when not actually being used.
8. With electronic records, staff must:
 - Always log-out of any computer system or application when work on it is finished.
 - Not leave a terminal unattended and logged in.



Health Professional (Non-AME) Code of Conduct

- Not share usernames and passwords with other people. If other staff have need to access records, then appropriate access should be organised for them – this must not be by using others' access identities.
 - Change passwords at regular intervals to prevent anyone else using them.
 - Always clear the screen of a previous applicant's information before seeing another.
9. All staff must be appropriately trained so that they are fully aware of their personal responsibilities in respect of record keeping and records management and that they are competent to carry out their designated duties. The CAA Medical Records Management system should not be used until training has been completed. Training should include the use of the CAA Medical Records Management system and it should be done through application to the CAA Medical department.
10. All examination and investigation documents related to an application or assessment for medical certification must be made available by the Health Professional to the UK CAA when requested by the UK CAA for audit purposes. The Health Professional shall co-operate with CAA regulatory investigations of applicants.

IT & Medical Records System

11. Access to UK CAA Medical Records Management system shall be limited to AMEs their named staff members within their medical practice and Health Professionals who review and advise on specialisms (e.g cardiology, ophthalmology). All named staff members must be notified to the UK CAA and agreed by the UK CAA. All staff must be technically competent to carry out their tasks whilst using the System.
12. Health Professionals will be issued with Secure Logon Identifiers by the UK CAA in order to access the System. Each person with a Secure Logon will be required to agree electronically with the UK CAA's IT Terms and Conditions. Health Professionals will ensure that passwords are not divulged to any other person, and that under no circumstances will Health Professionals log on using another person's secure ID.
13. The UK CAA will not be responsible for the provision, installation, operation and maintenance of any software, hardware and other equipment associated with the System at any Health Professionals premises.
14. The title and all intellectual property rights in all information, data, programs, procedures embodied in the System remains with the UK CAA at all times.
15. The UK CAA provides access to the System for the sole purpose of allowing AMEs, their named staff or Medical Professionals (e.g Cardiologists, Ophthalmologists) to retrieve medical records held electronically by the Authority for the purpose of undertaking periodic assessments and managing case reviews for the purpose of certificatory decision-making. Access to medical records other than those of pilots or ATCOs being referred to the Health Professional is prohibited.



Health Professional (Non-AME) Code of Conduct

16. Access to applicant records are monitored by the UK CAA and AMEs, their named staff or Medical Professionals should be able to demonstrate compliance with this clause.

GDPR

17. Report breaches possible breaches or risk of breach;
 - If staff identify possible breaches or risk of breaches, then they must raise these concerns with their manager or other appropriate colleagues, e.g. the local Data Manager.
 - Staff must be encouraged and supported by management to report organisational systems or procedures that need modification.
 - Staff must be made aware of local procedures for reporting where breaches of confidentiality or abuses of applicant data are taking place.
 - Any potential, or actual, data breach must be notified to the UK CAA Medical Data Asset Manager via ameoversight@caa.co.uk as soon as identified, along with details of any mitigating actions taken.
18. The Health Professional, before using the system to access an individual pilot/ATCOs medical record, must have received a referral from an AME by which the AME warrants that they have obtained consent from the applicant for the Health Professional to review the applicants record.
19. Health Professionals will observe Medical Confidentiality and the requirements of the UK General Data Protection Regulations (UK GDPR) pertaining to the processing, storage and transmission of personal data which is obtained by access to the System.
20. The Health Professional must be transparent with regard to how and why they are processing sensitive personal data of the applicant.
21. Health Professional will not use any information, data, programs or procedures obtained from the System for any purpose other than for the medical assessment of pilots and ATCOs for the purposes of certification.
22. The CAA reserves the right to use electronic mechanisms to audit connections to the System by Health Professionals.
23. Attention to the UK CAA Medical Department [Fair Processing Notice](#) is maintained at all times.

These Terms and Conditions are subject to periodic amendment by the UK CAA.

Glossary of Terms:

AME – Aeromedical Examiner

UK CAA – United Kingdom Civil Aviation Authority

‘The System’ – the IT application software that the AME / AME Support staff is able to log on to and submit medical data to the UK CAA database.

ATCO – Air Traffic Controller

UK GDPR – UK General Data Protection Regulations