CAA IT Code of Conduct for use of the CAA Cellma Medical Records System

Who does this apply to?

This code of conduct applies to medical professionals, AMEs and support staff who have authorised use of the CAA Cellma Medical Records System. This code covers all usage of this Cellma Medical Records System.

Why is this important?

- A key principle of the UK GDPR is ensuring that we process personal data securely by means of ‘appropriate technical and organisational measures’ – this is the ‘security principle’.
- Measures must ensure the ‘confidentiality, integrity and availability’ of our systems and services and the personal data we process within them.

For all parties to be compliant with Article 5(1)(f) of the UK GDPR personal data must be: *'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'*

To protect the confidentiality, integrity and availability of the data stored and processed within the Cellma system, we provide a secure IT environment to safeguard that information, but your actions as a user are also important in helping to keep it secure. It is also crucial that our electronic communication, use of technology and protection of information is consistent with this Code of Conduct, AME Terms and Conditions (where it concerns a medical professional and their support staff), and relevant professional code of conduct.

General principles

- In accessing the CAA Cellma Medical Records System, you should be mindful of the sensitivity of data within and take reasonable steps to protect its confidentiality when using the system.
- The Cellma system and data within it must only be used for its intended business purpose.
- You must not share confidential information about an individual or an organisation except as required for the purposes of medical certification and with the individual's consent, unless you have an alternative lawful basis to do so.
- Whilst there are systems in place to protect the Cellma environment from malware, viruses etc., you should also take steps to ensure that your activity does not put either the device being used for access or the Cellma system at additional or unnecessary risk, e.g.:
    - You must not attempt to gain unauthorised access to Cellma data or system components.
    - Do not try to bypass security settings of any device or application being used to access the system.
    - You should take reasonable measures to ensure that any devices you use to access Cellma are securely maintained and updated.
- Disposal of any device that has been used to access Cellma should be done in a responsible and secure manner.

How you can help

- Ensure that any passwords or access codes provided to you are appropriately protected and that these are never shared with anyone.
- Be aware of your surroundings when accessing Cellma e.g.:
    - Can you be overlooked?

    - Be aware of eavesdropping opportunities
    - Do not leave any devices unlocked when unattended.
- Ensure that the device used to receive your One-Time Password is also secured (e.g. remains under your control and is locked when not in use).
- Do not transfer information out of the Cellma environment e.g., by sending it to personal email accounts or transferring it onto personal devices.
- Ensure that the handling instructions of data are respected in line with the sensitivity, including but not limited to, when dealing with printed information.
- Ensure the operating system, relevant software and web browser running on the device used to access Cellma is maintained and kept up to date.

Remaining vigilant

Various tools and technologies are employed by the CAA and its suppliers in provision of the service and the securing of it. In addition, as a user of the system, you can help by remaining vigilant.

We will never contact you asking for your password. Please report any such activity as suspicious.

You are responsible for any information that you have access to (including your passwords and OTP) and for keeping these safe. In the event of a loss or theft you should raise a Security Incident immediately (*see below*) so that we can take steps to limit any unauthorised or unintended access.

Sometimes things can go wrong, and mistakes can happen, the important thing is to let us know as soon as possible so that we are aware and can follow-up in a timely manner.

You agree to this Code every time you access the CAA Cellma Medical Records System and breaches will be investigated and further action taken if necessary. This may include temporary or permanent removal of your access to the system.

If you would like more information or guidance on anything covered in this Code, please contact the CAA Contact Centre on **0330 022 1972**

If you are reporting a potential Security Incident, please contact us via email as soon as possible via **Medical.Security@caa.co.uk**