

CPME 2026/079 FINAL

ADOPTED

AUTHOR: CPME BOARD

7 MAY 2026

Feedback on Commission Implementing Regulation on an interoperable, cross-border identification and authentication mechanism for natural persons, health professionals and healthcare providers for the purposes of the cross-border exchange of personal electronic health data

CPME welcomes the opportunity to comment on the draft implementing legislation. We ask to take into consideration the following feedback:

- The methods for identification and authentication of health professionals, and patients in electronic health record (EHR) systems need to be robust, easy, fast and with appropriate levels of security for protecting personal data relevant for clinical activities in compliance with eIDAS Regulations.
- Identification and authentication of doctors in online EHR systems should balance the need for integrity in a certain setting and the security of the digital tool with the administrative burden for this procedure. Such requirements should not delay access to relevant data in clinical practice, create barriers to patient care, or increase the risk of errors in treatment.
- Since a unique health professional identifier is required, the additional obligation to provide details such as given name (including middle name) and date of birth seems duplicative and do not add clear value and can therefore be removed from the list of mandatory data.
- While recognising the potential of the European Digital Identity Wallet, it is important to avoid critical dependency on a single technological solution. Alternative access mechanisms and fallback solutions should be ensured in order to maintain continuity of care in case of technical disruptions.
- Interoperability requirements should support, and not disrupt, well-functioning national systems. The implementation should avoid imposing changes that would unnecessarily interfere with established clinical workflows and existing digital infrastructures in Member States. Implementation therefore requires a high level of organizational and technical safeguards to ensure the integrity, confidentiality, and security of particularly sensitive data.
- Regarding Article 2(1), it should be confirmed whether this refers to a specific number created and assigned by the European Digital Identity Wallets platform mentioned in Recital 2, or by MyHealth@EU as referred to in Recital 3.

- The references to definitions in Article 2 (3), (4), and (5) are unclear. CPME therefore requests further clarification on the definition of ‘attributes’ and ‘healthcare attributes’ and their application in the context of MyHealth@EU and/or European Digital Identity Wallets, with a view to ensuring a high level of security.
- Protective equipment healthcare professionals use while practicing needs to be considered.
- CPME supports single sign-on authentication & identity management federation concepts. ‘One day, one-time login’ to the online EHR system back-end must be common practice, providing for automatic authentication of national components, such as ePrescriptions, patient summaries, etc. This means that the session should remain active until the healthcare professional signs out, which does not invalidate the authentication procedure of locking &unlocking the system when a healthcare professional is required to use another terminal on the same day.
- The financing of implementing and maintaining this mechanism must be covered by national health authorities and not health professionals and/or patients.

Amendment 1 – Annex			
Commission proposal		CPME amendment	
Table 1 - Mandatory data for the health professional		Table 1 - Mandatory data for the health professional	
given_name	First name(s), including middle name(s) where applicable, of the health professional.	given_name	First name(s), including middle name(s) where applicable, of the health professional.
date_of_birth	The point in time on which the health professional was born.	date_of_birth	The point in time on which the health professional was born.