bitkom

Position Paper

May 2026

Implementing Act

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

Summary

The success of the cross-border identification and authentication mechanism is a direct precondition for the value MyHealth@EU is intended to deliver to patients and clinicians. If patients cannot be reliably identified across borders, and if healthcare professionals cannot be securely authenticated in a way that works in clinical practice, the framework will not deliver its intended benefits.

Against this background, Bitkom proposes selected improvements that, in the view of our member companies, would materially improve how the framework operates in practice.

General Aspects

- **Technology-open implementation**

Reference implementation on the infrastructure-level of the Member States should be followed to have a standardized and binding implementation for Member States. This allows good and fast cross-border operation, aligned development and easier rollout of new features on Member State level. On Industry level it should be kept open to preserve competition, enable innovation and avoid unnecessary dependency on a single implementation path.

- **Predictable specification and release regimes**

Providers need predictable specification and release regimes in order to invest and implement reliably. Early publication of specifications, binding lead times, test environments, piloting and realistic transition periods are necessary to allow vendors to build with confidence. Without sufficient predictability, implementation risks will increase and market readiness may be delayed.

- **Proportionate compliance and escalation mechanisms**

Compliance and escalation mechanisms should be proportionate. Suspensions should only apply where there are material risks. Clear criteria, transparent procedures and realistic remediation periods are needed. This would ensure that enforcement is effective without creating disproportionate operational risks for providers and healthcare services.

- **Standardised roles and liability models for private operators**

The framework should include standardised roles and liability models for private operators. Without standardised Controller, Processor and Subprocessor models, the development of privately operated EHDS services will be too slow and too costly. Clear allocation of responsibilities is necessary for scalable implementation and for legal certainty across Member States.

- **Qualified Electronic Attestations of Attributes**

While certain healthcare attributes should be mandatory as Qualified Electronic Attestations of Attributes (QEAAs), such as an electronic patient record or a patient's health insurance number, others, such as an access token for an ePrescription, should be issued as non-qualified electronic attestations. This approach provides the highest level of trust for healthcare attributes where it is necessary, while preserving flexibility for other attributes. It also helps ensure the right balance between data protection, security, and practical usability.

- **Access paths without unnecessary identification**

For many healthcare-related use cases, identification of the natural person is not necessary, for example where a person holds a valid ePrescription token, access title or comparable instrument. The framework should make clear that such mechanisms must remain usable without additional patient identification, provided they are permitted under Member State law. Identification requirements should be proportionate and should not create unnecessary friction in established healthcare processes.

Detailed Feedback

Article 3: Harmonisation of National Attribute Sets

Healthcare attributes issued to EUDI Wallets under Article 3(3) of the draft CIR should, where they concern particularly sensitive and legally relevant healthcare data, be required to be QEAAs rather than merely non-qualified Electronic Attestations of Attributes. This should apply in particular to healthcare attributes such as an electronic patient record or a patient's health insurance number. These attributes constitute special-category data under Article 9 GDPR and therefore warrant the highest level of

trust, security, and accountability in their digital attestation. QEAAs provide this level of trust, as they are issued by QEAA Providers subject to conformity assessment, ensuring consistent quality, security, and accountability across the EU.

In addition, QEAAs benefit from mandatory cross-border legal recognition under Article 45f of eIDAS 2.0, ensuring uniform legal effect in all 27 Member States. This is essential for a cross-border healthcare framework, where patients and healthcare professionals must be able to rely on the legal validity and trustworthiness of healthcare attributes across borders.

At the same time, not all healthcare-related attributes require the same level of assurance. Attributes with a more technical or temporary function, such as an access token for an ePrescription, may appropriately be issued as non-qualified electronic attestations. This allows the framework to preserve the necessary flexibility and to strike the right balance between data protection, security, and practical usability.

Article 3 allows each Member State to define its own healthcare attribute set, subject to publication but without harmonisation. This risks creating 27 incompatible attribute sets and shifting integration costs to every receiving NCPeH and downstream system. A harmonised minimum core dataset for healthcare attributes is needed alongside national flexibility in order to prevent fragmentation.

Article 4: Non-discriminatory access and representative authorisation

Article 4 introduces specific requirements for online interactions that may impose a disproportionate burden on online healthcare providers, including online pharmacies. Requirements for identification and authentication should be applied in a way that does not discriminate between healthcare providers operating online and those operating in physical settings, provided that equivalent levels of security, assurance and auditability are achieved. The framework should clarify that equivalent outcomes, rather than specific methods, are required.

Furtermore, Article 4 should include a clear description of how another natural person can be authorised to act on behalf of a patient. Representative/proxy cases are a core part of healthcare services, including relatives, such as parents acting for their infants, children supporting their parents, and persons acting for individuals in care.

These cases must work smoothly in practice. The framework should therefore provide clearer guidance on how representative authorisation should be implemented, and which rules, duties and safeguards should apply.

Article 5: Fallback when the patient has no EUDI Wallet

From 26 March 2029, HPs and HCPs must accept healthcare attributes via the EUDI Wallet. However, EUDI Wallet rollout may be uneven across Member States, and many cross-border patients, including elderly patients, acutely unwell patients and undocumented patients, may not be able to use one.

There is need for an explicit fallback through the patient's national means of identification and for a non-discrimination principle based on digital identity status. Patients should also be able to share their healthcare attributes through non-EUDI Wallet paths in a safe and user-friendly way. Where patient identification is not necessary, the framework should also allow for processes that do not require patient identification.

Article 6: Healthcare Professional authentication and authorisation

Article 6 should make clear that online pharmacies are covered as healthcare providers and that pharmacists providing services through online pharmacies are recognised as healthcare professionals. This clarification is necessary to ensure that identification, authentication and authorisation mechanisms apply consistently across physical and online healthcare settings.

Furthermore, the draft leaves the choice of national authentication entity, the authorisation mechanism and revocation propagation entirely to Member States. This creates a risk of fragmentation and may lead to parallel structures that do not fit existing clinical workflows. Cross-border recognition should be built on existing national HP credentialing schemes, such as SITHS in Sweden and equivalent schemes in other Member States, rather than creating a parallel layer.

Second, the framework should explicitly recognise single sign-on, session continuity and step-up authentication patterns. These patterns are necessary to make the requirement workable in real clinical workflows.

Third, the relevant data elements should be aligned with HPRO and HCID code systems already used in MyHealth@EU. This should include the unique HP identifier, role, specialty and organisational affiliation.

Annex

- **Clinician date of birth as a GDPR data-minimisation concern**

The Annex, Table 1, requires the HP's date of birth as part of the cross-border identification payload. This raises a GDPR data-minimisation concern. The HP identifier, in combination with the country code and issuing authority, should be sufficient for unique identification. Including the date of birth introduces direct personal data of healthcare workers without a clear purpose linked to Article 5(1)(c) GDPR.

- **No binding code system for the HP role**

The Annex does not provide a binding code system for hp_professional_role. Without a binding code system, such as HPRO, ISCO-08, SNOMED CT or HL7 PractitionerRole, Member States will populate the field inconsistently and every receiving NCPeH will need bilateral mappings. In addition, there is no specialty field, although such a field is needed for meaningful role-based access decisions across borders.

- **No audit-correlation fields, undermining Article 9 EHDS**

Recital 3 links cross-border identification to the access-logging duty in Article 9 EHDS. However, the Annex contains no exchange or correlation identifier and no request timestamp. Under-specified audit fields will lead to inconsistent national implementations.

Conclusion

Bitkom supports the development of a robust, interoperable cross-border identification and authentication mechanism under the EHDS. The clarifications and additions set out above would, in our view, materially improve how the framework operates in practice: for the clinicians who will rely on it every day, for the healthcare providers responsible for implementing it, and for the European software vendors building the tools that increasingly support clinical care.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Verena Benz | Head of Pharma digital
P +49 30 27576-270 | v.benz@bitkom.org

Responsible Bitkom committee
WG Pharma digital