Warsaw, April 16th 2026

Draft 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

1. Summary

IS Consulting supports the objective of the draft Regulation: establishing coherent, interoperable requirements for identification and authentication mechanisms applicable to all participants in the cross-border exchange of health data under the EHDS. Identifying and verifying the identity of the patient, health professional and healthcare provider before initiating a data exchange is a necessary precondition for the secure operation of the system, and it is right that this is addressed in a dedicated implementing act.

The draft contains several well-calibrated provisions: the phased escalation of assurance levels (substantial to high), integration with the European Digital Identity Wallet (EUDIW), and delegation to Member States of the definition of healthcare attribute sets. At the same time, the draft requires clarification and strengthening in several areas of material operational and security significance: management of representation and legal guardianship, protection of attributes against misuse, proportionality for smaller healthcare providers, and consistency with NIS2 requirements and current ENISA guidance.

2. Context and basis for this opinion

Identification and authentication of participants in health data exchange is not merely a technical matter. It is the first and most critical line of defense in the security architecture of the cross-border health data exchange system. Compromise of the identification mechanism could lead to unauthorized access to special category data (health data under GDPR Article 9) at scale.

IS Consulting submits this opinion based on practical experience designing identity and access management (IAM) mechanisms for healthcare

systems, knowledge of the eIDAS 2.0 and EUDIW frameworks, and operational familiarity with the realities of the European healthcare sector, including the highly varied digital maturity of healthcare organizations, which is particularly pronounced among small and medium-sized providers.

3. Assessment of the draft: strengths

Phased escalation of assurance levels. The graduated approach (substantial from 2027, high from 2030 for patients, high from 2032 for health professionals) is proportionate to the realistic implementation capacity of Member States and allows sufficient time for the full rollout of electronic identification means, including EUDIW. This is consistent with the philosophy of incrementally raising requirements applied in NIS2.

Integration with EUDIW as the reference mechanism. The ability to issue healthcare attributes to EUDIW (Article 3(3)) and the obligation to accept EUDIW as an identification means (Article 5(2)) ensure coherence with the broader European digital identity ecosystem. EUDIW providing the high assurance level is the appropriate target mechanism.

Delegation to Member States of defining healthcare attribute sets. Article 3(1) allows Member States to determine their own attribute sets, respecting the diversity of health identification systems across countries, while the notification and publication requirement (Article 3(2)) ensures transparency across the system.

Technical specifications for health professional identification (Annex). The tables of mandatory identification fields (hp_identifier, hp_professional_role, healthcare_provider_identifier, and others) are precise and operationally useful. The explicit statement that identifiers are unique within the issuing Member State is the correct approach.

4. Specific observations and recommendations

4.1 Representation and legal guardianship: an operational gap

Article 4(3) provides that the health professional or healthcare provider shall identify a person acting as legal representative or authorized proxy and verify that they satisfy the necessary requirements to act in that capacity. However, the draft does not define how this verification should work

technically, nor what attributes should be transmitted in a cross-border exchange request in cases of representation.

In clinical practice, representation situations are common: parents of children, carers for persons with disabilities, proxies for elderly patients. In a cross-border context, verifying the status of a representative is significantly more difficult than at national level, as representation registers are national and inconsistent across Member States.

The absence of clear requirements regarding representation attributes in the Annex (Table 1) means that NCPs of different Member States may implement this in incompatible ways, creating interoperability gaps from the date of application.

Recommendation 1. Article 4(3) should be supplemented with minimum requirements for verifying representative status in cross-border exchanges: (a) specification of which attributes describing the representation relationship are transmitted between NCPs; (b) a requirement that the attribute exchange mechanism (Article 8) supports representation use cases. We recommend extending the Annex (Table 1) with optional or mandatory fields covering representation (such as relationship_type and representative_identifier), enabling interoperable handling of these cases from the date of application.

4.2 Protection of healthcare attributes against reuse and misuse

The draft regulates the issuance and transmission of healthcare attributes but contains no requirements for protecting those attributes against unauthorized reuse (replay attacks) or aggregation by intermediaries. Healthcare attributes, which include patient identification data and Member State of affiliation, represent a high-value target for attackers.

An electronic attestation of attributes (EAA) issued to EUDIW can technically be presented to multiple parties and reused across sessions unless session binding or nonce mechanisms are implemented. The draft contains no reference to unlikability or selective disclosure requirements, which are material from the perspective of data minimization under GDPR Article 5(1)(c).

Recommendation 2. The draft should include a requirement that the healthcare attribute exchange mechanism support: (a) binding of the attestation to a specific exchange session (session binding or nonce),

limiting the possibility of replay attacks; (b) selective disclosure of attributes consistent with the data minimization principle, so that NCPs transmit only the attributes necessary for identification in the given context rather than the full national attribute set. These requirements should be reflected in the MyHealth@EU requirements catalogue (MyHealth@EU Regulation, Article 4(2)).

4.3 Health professional identification data in the Annex: data minimisation concern

Table 1 of the Annex designates the healthcare_provider_identifier field as mandatory for health professionals. This is the identifier of the facility or organization where the health professional is currently providing treatment. The mandatory status of this field raises concerns from a data minimization perspective.

Information about the facility is necessary for billing and audit purposes, but is not always required for the identification and authentication of the health professional in the context of a data exchange request. For mobile professionals, specialists operating across multiple facilities, or practitioners working in telemedicine contexts, the identifier of a specific facility may be difficult to determine at the moment of the exchange request or may be misleading.

Recommendation 3. We recommend considering a change in the status of the healthcare_provider_identifier field in Table 1 from mandatory to conditionally mandatory, meaning required where available and relevant to the context of the exchange, while retaining mandatory status in Table 2 for the identification of the healthcare provider organization itself. Alternatively, the Regulation or accompanying guidance should clarify how this field is to be populated in cases involving professionals working across multiple entities or in telemedicine settings.

4.4 Mutual recognition of conformity assessments for non-notified eID means

Recital 4 and Article 6(3) provide that where a Member State uses an electronic identification means that has not been notified to the Commission under eIDAS, the high assurance level of that means must be confirmed by an accredited conformity assessment body. This is

systemically correct but raises operational questions about the mutual recognition of such assessments across Member States.

Recommendation 4. The draft should explicitly state whether a conformity assessment confirming the high assurance level performed by an accredited body in one Member State is automatically recognized by other NCPs, or whether separate verification is required. We recommend a reference to the mutual recognition mechanism provided for in eIDAS 2.0, or a provision that the Commission publishes and maintains a list of recognized identification means, analogous to the publication of Member States' healthcare attribute sets under Article 3(2). This would increase predictability and reduce the risk of fragmentation in the market for identification tools.

4.5 Operational resilience of the IAM mechanism

The draft sets assurance level requirements for identification and authentication means but entirely omits the question of the operational resilience of the IAM mechanism itself, specifically what happens when the identification system is unavailable or experiencing delays.

In the healthcare sector, unavailability of the identification mechanism can directly affect continuity of patient care in emergency situations. The absence of a fallback procedure may result in cross-border data exchange being blocked at critical clinical moments. Article 8 defines the mechanism for exchanging identification data but specifies no availability requirements (availability SLA) or contingency procedures.

Recommendation 5. We recommend that Article 8 or the MyHealth@EU requirements catalogue (MyHealth@EU Regulation, Article 4(2)(c)) include minimum availability requirements for the IAM mechanism and procedures for handling situations where a patient identification means is temporarily unavailable, for example an emergency authentication procedure for acute clinical situations, modelled on solutions used in national systems. It is particularly important to specify when a health professional may act without full cross-border identity verification and how such situations should be recorded and accounted for.

5. Technical observations on the Annex

The Annex contains technical specifications for health professional identification data (Table 1) and healthcare provider identification data

(Table 2). In addition to the observation in Recommendation 3, we draw attention to the following points.

Absence of identifier format specifications. The hp_identifier and healthcare_provider_identifier fields are defined semantically but the Annex does not specify their technical format, for example whether URN, OID or a national format should be used. Different national formats may impede technical interoperability, particularly where NCPs need to parse and validate identifiers issued by other Member States. We recommend adding at minimum a requirement for basic formatting principles or a reference to the MyHealth@EU technical specifications.

Absence of a field indicating the validity or current status of professional registration. Table 1 contains no field confirming that the health professional's registration rights are currently active, such as a licence_valid_until or licence_status field. A professional may hold a valid national identifier while their registration has been suspended or has lapsed. In a cross-border exchange, the receiving NCP has no technical basis for verifying the currency of registration rights. We recommend adding an optional field for licence status or a reference to a dynamic registration verification mechanism.

Healthcare provider address as personal data. The healthcare_provider_address field in Table 2 is defined as the official full registered address of the healthcare provider. For small providers, including sole practitioners and private practices, the registered address may also be a private residential address, raising concerns under GDPR. We recommend clarifying that the address transmitted should be a professional correspondence address rather than a private address.

6. Summary

IS Consulting assesses the draft Regulation as an important and necessary component of the EHDS security architecture, built on solid foundations in eIDAS 2.0 and EUDIW. Additionally, Section 5 sets out three technical observations on the Annex: the absence of identifier format specifications, the absence of a field indicating the current validity of professional registration rights, and a GDPR concern regarding the address field for small healthcare providers.

IS Consulting remains available for further discussion of this opinion in the context of public consultations or the MyHealth@EU Steering Group. Our

approach is vendor-agnostic: we do not advocate specific technological solutions but put forward functional and outcome-based requirements whose fulfilment should be verifiable through compliance checks.