Warsaw, April 16th 2026

Draft Commission Implementing Regulation on MyHealth@EU

Transparency disclosure: IS Consulting provides cybersecurity advisory and implementation services for the healthcare sector, including as coordinator of the ASCLEPIUS project (EU Digital Europe Programme, Grant Agreement 101127583). IS Consulting is the author of the ShieldNet cybersecurity ecosystem for SMEs. This opinion is submitted as an independent expert contribution; none of the positions below constitute promotion of commercial solutions or specific vendors.

1. Summary

IS Consulting supports the objective of the draft Regulation: establishing coherent, verifiable rules for the interoperability and security of cross-border personal electronic health data exchange through MyHealth@EU. From a cybersecurity and operational resilience perspective, the draft provides solid foundations. However, several areas require clarification or strengthening, most notably the security requirements applicable to national contact points (NCPs), the critical incident response framework, and the proportionality of requirements for smaller national systems.

2. Context and basis for this opinion

IS Consulting submits this opinion based on practical experience designing and implementing cybersecurity measures in the healthcare sector, at both the organizational level (audits, security architectures, MSSP services) and the European level (ASCLEPIUS project, focused on cybersecurity preparedness for healthcare organizations under Digital Europe).

Our positions are grounded in European regulatory frameworks (GDPR, NIS2, EHDS, ENISA guidance) and operational implementation experience, with particular attention to the specifics of multi-stakeholder systems connecting participants of varying cybersecurity maturity. We write as experts on operational feasibility and proportionality of requirements — not as representatives of technology vendors or advocates for specific market solutions.

3. Assessment strengths

The draft merits a positive assessment in the following areas.

Clear separation of roles. The explicit assignment of the Commission as processor and national contact points as joint controllers (Articles 15–16) establishes unambiguous accountability consistent with GDPR and EUDPR.

Compliance mechanism based on verifiable outcomes. The compliance check system with categorized findings (minor/medium/critical) and mandatory action plans (Article 8) is proportionate and operationally feasible.

Change management procedure. The distinction between major and minor releases (Article 6) limits the risk of operational disruption to national systems and supports predictability.

Transparency of data processed in the platform. Article 14 precisely limits the scope of data processed to categories defined under EHDS, a proper application of the data minimization principle.

Transitional provisions. Article 18, providing continuity for NCPs already connected under eHDSI, is a pragmatic solution that reduces implementation costs.

4. Specific observations and recommendations

4.1 Cybersecurity requirements for national contact points

Article 15(1)(f) obliges NCPs to implement "appropriate organizational, physical and logical security measures." This formulation is systemically correct but insufficient as the sole basis for operationally verifying security in a heterogeneous European environment.

Recommendation 1. The draft should explicitly state that security requirements for NCPs are detailed in the requirements catalogue (Article 4(2)), and that the catalogue itself should include at least: (a) requirements referencing recognised European security frameworks (e.g. ENISA guidelines for the healthcare sector) or equivalent standards such as ISO 27001/IEC 27799; (b) minimum requirements on identity and access management, encryption of data in transit and at rest, event logging, and vulnerability management. This will prevent a situation where "appropriate

measures" is interpreted in a manner that cannot be verified during compliance checks.

4.2 Critical incident management definition and response time

Article 13 defines a critical incident as a "serious unplanned disruption" and imposes a 24-hour notification obligation. The definition is appropriate, but the draft lacks requirements concerning NCPs' internal procedures prior to notification, and minimum detection capabilities at the national level.

The 24-hour notification deadline presupposes that an NCP has the capacity to detect and classify an incident in real time or near-real time. Absence of such capability may make the deadline unachievable, not through lack of good faith, but through absence of adequate monitoring. The draft contains no requirements for minimum Security Operations capabilities (monitoring, SIEM/log management, detection procedures) on the NCP side, leaving this entirely to the requirements catalogue.

Recommendation 2. The draft should indicate that the requirements catalogue (Article 4(2)(c)) covers minimum operational capabilities of NCPs for incident detection and response, including a requirement to have a formal incident response plan as a precondition for authorization to exchange data (Article 10). We also recommend clarifying that the 24-hour notification period runs from the moment an event is classified as a critical incident, not from the first detection of an anomaly, consistent with the approach taken in NIS2 (Article 23).

4.3 Cryptographic requirements and key management

Article 16(1)(e)(vii) requires that data transported within the central secure communication service be encrypted. This is a necessary and correct requirement. However, the draft contains no provisions on cryptographic key management or algorithm requirements. Given the five-year compliance check cycle (Article 9(b)), this creates a risk of outdated cryptographic solutions remaining in use.

Recommendation 3. The requirements catalogue should include requirements for the use of current cryptographic algorithms consistent with ENISA guidance ("Algorithms, Key Sizes and Parameters Report"), and a mechanism for updating these requirements independently of the full major release cycle, particularly in view of post-quantum risks. We recommend that Article 16(1)(e) contain a reference to European

cryptographic guidance, or empower the Commission to issue binding cryptographic recommendations.

4.4 Proportionality for national systems of varying maturity

The draft treats all national contact points uniformly in terms of compliance and security requirements. While systemically justified, this may generate disproportionate burdens for smaller or less mature national systems, particularly in the context of preparing for compliance checks every five years.

Recommendation 4. We recommend introducing a tiered baseline approach in the requirements catalogue, where: (a) a minimum level sets out requirements necessary to obtain and maintain authorization to exchange data; (b) a target level sets out requirements recommended for full operational maturity. This approach, consistent with the philosophy of NIS2 and ENISA guidance for SMEs, would facilitate remediation planning and prevent situations where an NCP suspends data exchange due to gaps in areas that are not operationally critical.

4.5 Data protection and supervisory coordination for multi-NCP breaches

The draft provides for consultation with the European Data Protection Supervisor (Recital 23) and includes detailed provisions on the allocation of responsibilities between joint controllers (Article 15) and the processor (Article 16). However, there is no explicit mechanism for coordination between the EDPS and national supervisory authorities (such as national data protection offices) in the event of a data breach affecting multiple NCPs simultaneously.

Recommendation 5. Article 15(1)(h) should be supplemented with a provision that where a breach concerns the processing operations of more than one NCP, the responsible NCP coordinates notification with the other joint controllers and immediately informs the Commission so that the impact at platform level can be assessed. This would increase the predictability of notification procedures and reduce the risk of inconsistent communications to supervisory authorities in different Member States.

5. Additional observations

The following points do not rise to the level of critical recommendations, but are worth addressing in further work on the Regulation or in accompanying documents (requirements catalogue, operations framework).

Business continuity (BCP/DR). The draft refers to ensuring platform business continuity (Article 5(1)(e)), but specifies no minimum RTO/RPO (Recovery Time/Point Objective) requirements, neither for the Commission as operator of the central platform nor for NCPs. We recommend addressing this in the requirements catalogue.

Vulnerability management. The draft makes no reference to a vulnerability management obligation on the NCP side within the security commitments of Article 15(1)(f). In the healthcare context, vulnerabilities in health data exchange systems are a particularly attractive target for ransomware and APT actors. We recommend inclusion of a formal vulnerability management process requirement in the requirements catalogue.

Supply chain security. Article 16 permits the Commission to engage sub-processors. The draft contains no specific security requirements for sub-processors, referring only to the general GDPR framework (Article 28). Given the nature of the data processed (special category health data), we recommend explicit due diligence requirements for sub-processors and a mandatory notification obligation in the event of changes to the sub-processor list.

6. Summary

IS Consulting assesses the draft MyHealth@EU Regulation positively as a sound legal foundation for secure and interoperable cross-border health data exchange. The recommendations presented above aim to strengthen the draft in areas of greatest operational and security significance, without increasing the overall regulatory burden.

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 technologies or products, but functional and outcome-based requirements that can be verified through compliance checks.