EUROPEAN
COMMISSION

Brussels, XXX
[…](2026) XXX draft

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

on HealthData@EU

(Text with EEA relevance)

This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission.

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

on HealthData@EU

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847[1], and in particular Article 63(7) and Article 75(12), first sentence, thereof,

Whereas:

(1) Regulation (EU) 2025/327 establishes the European Health Data Space and provides for the establishment of the HealthData@EU infrastructure to support and facilitate cross-border access to electronic health data for secondary use.

(2) HealthData@EU should be set up as a cross-border infrastructure connecting the national contact points for secondary use, the Union health data access service and authorised participants to a central platform. The infrastructure should combine components operated by the connected entities with central services provided by the Commission. The Commission should be responsible for developing, deploying and operating the central platform, while each connected entity should remain responsible for its respective components and connection.

(3) The central platform should provide the information technology services needed to support and facilitate the exchange of information. In particular, it should enable the submission and routing of health data access applications referred to in Article 67(3) of Regulation (EU) 2025/327, support the interconnection of national dataset catalogues and, where applicable, dataset catalogues of authorised participants, make the EU dataset catalogue publicly available, and facilitate cooperation between health data access bodies and authorised participants.

(4) To allow the technical implementation of HealthData@EU to evolve while preserving legal certainty, detailed implementation specifications should be set out in technical documentation developed and maintained by the Commission in accordance with the operational decisions of the HealthData@EU steering group. That documentation should spell out the detailed implementation of the requirements, conditions and allocation of responsibilities laid down in this Regulation.

(5) Pursuant to Articles 95 and 96 of Regulation (EU) 2025/327, the HealthData@EU steering group takes operational decisions concerning the development and operation of HealthData@EU, while the Commission develops, maintains, hosts, deploys and operates the central platform and the other central services that it provides in accordance with those decisions. This Regulation specifies the matters on which the steering group should take operational decisions and the preparatory, assessment and implementation tasks to be performed by the Commission.

(6) In order to ensure transparency and predictability in the evolution of the HealthData@EU infrastructure, this Regulation distinguishes between major releases which require connected entities to adapt their systems, and minor releases, which do not. The steering group should take operational decisions on major releases and their implementation timelines. Minor releases should be managed by the Commission in accordance with the approved change-management procedures, and the Commission should inform the steering group in advance. An annual work plan should identify priorities for the operations and management of the central platform. This work plan should be consistent with the two-year work plan of the EHDS Board.

(7) To ensure that only entities capable of participating securely and reliably are connected to HealthData@EU, the Commission should conduct compliance checks before connection and periodically thereafter. Those checks should cover, as applicable, legal eligibility and mandate, technical capability and interoperability, security and data protection, operational capacity, business continuity, incident management, and the minimum requirements relating to qualified expertise and technical, organisational and operational capabilities. The compliance framework should specify the evidence, testing methods and assessment criteria used to verify those requirements in accordance with Article 75 of Regulation (EU) 2025/327.

(8) National contact points for secondary use and the Union health data access service are required by Article 75(3) of Regulation (EU) 2025/327 to connect to HealthData@EU. Once a positive outcome of the initial compliance check confirms that they meet the applicable requirements, their connection should take place without a further authorisation decision. Since their participation is required by Regulation (EU) 2025/327, non-compliance should be addressed through corrective measures and, where necessary to protect the secure and reliable operation of HealthData@EU, temporary disconnection, but not definitive exclusion.

(9) Health-related research infrastructures or similar infrastructures whose functioning is based on Union law, and which provide support for the use of electronic health data for research, policymaking, statistical, patient safety or regulatory purposes may become authorised participants in HealthData@EU in accordance with Article 75(4) of Regulation (EU) 2025/327. Their connection should be subject to an application, a positive outcome of an initial compliance check conducted by the Commission and an operational decision of the steering group, so that their eligibility and operational readiness are verified before connection.

(10) Third countries or international organisations may become authorised participants in HealthData@EU in accordance with Article 75(5) of Regulation (EU) 2025/327 only where, in addition to complying with the general connection requirements, they comply with Chapter V of Regulation (EU) 2016/679 and provide access to health data users located in the Union, on equivalent terms and conditions, to the electronic health data available to their health data access bodies. The Commission should verify compliance with the applicable legal, organisational, technical and security requirements and with the requirement of equivalent access. Connection of such third countries or international organisations should take effect only following a positive outcome of the applicable compliance checks, an operational decision of the steering group confirming their operational readiness to connect, and the adoption of an implementing act pursuant to Article 75(13) of Regulation (EU) 2025/327.

(11) Where a compliance check identifies non-compliance, the entity concerned should be given an opportunity to remedy that non-compliance within a specified period, unless urgent action is necessary to protect HealthData@EU. Where proportionate, such urgent action may include temporary disconnection from HealthData@EU. Definitive exclusion should be limited to authorised participants in cases of serious misconduct or repeated infringements and should be subject to the right to be heard and to a reasoned decision. For an authorised participant connected pursuant to an implementing act adopted under Article 75(13) of Regulation (EU) 2025/327, the steering group should be consulted on a proposed definitive exclusion, while that exclusion should take effect only through the repeal or amendment of that implementing act.

(12) Incidents may require immediate coordinated action even where no non-compliance has been established. Connected entities should therefore cooperate with the Commission in addressing incidents affecting or likely to affect the secure and reliable operation of HealthData@EU. Mandatory notification to the Commission should be limited to significant incidents. Where necessary, the Commission should be able to temporarily disconnect the entity concerned from HealthData@EU as a protective operational measure until reconnection is safe, without prejudging any measures that may be taken following a compliance check.

(13) The effective cross-border functioning of HealthData@EU and the exchange of information between connected entities depend on technical, semantic and organisational interoperability. The common specifications should therefore cover, as appropriate, interfaces and exchange protocols, message structures, identification, authentication, authorisation and trust mechanisms, metadata and semantic assets, secure exchange, logging and traceability, versioning, backward compatibility and conformance testing. The concrete standards and versions required to implement those common specifications should be set out in the technical documentation and should take account of relevant Union interoperability requirements, Interoperable Europe solutions, Union semantic assets and common specifications applicable to common European data spaces. In accordance with Article 75(11) of Regulation (EU) 2025/327, HealthData@EU should support interoperability with other relevant

common European data spaces. Such interoperability does not in itself provide a legal basis for access to or exchange of electronic health data.

(14) Given that HealthData@EU involves the processing of personal data in particular in relation to its operation, this Regulation lays down the requirements to ensure confidentiality, integrity, availability and traceability within the infrastructure. In accordance with, Regulation (EU) 2016/679 [1]and Regulation (EU) 2018/1725[2], appropriate technical and organisational measures should be implemented, and the necessary security controls should be specified in the technical documentation developed and maintained by the Commission. Processing operations carried out within HealthData@EU may involve different controllers and processors. Their responsibilities should therefore be allocated by reference to each processing operation. For processing operations carried out through the central platform, the national contact points for secondary use should act as joint controllers and the Commission should act as processor, in accordance with Article 75(10) of Regulation (EU) 2025/327, without prejudice to processing carried out by the Commission in its capacity as Union health data access service. Where the Commission provides a secure processing environment under Article 75(9) of that Regulation, the national contact points for secondary use or authorised participants that put electronic health data in that environment should act as joint controllers and the Commission should act as processor.

(15) To enable health data access bodies to take account of relevant enforcement measures adopted in other Member States and to coordinate enforcement where necessary, the Enforcement Information Exchange Tool should provide controlled access to the minimum information necessary for those purposes. The health data access body that adopts an enforcement measure should be responsible for recording accurate information and updating it without undue delay. The Commission should operate the tool without affecting the allocation of enforcement competences laid down in Regulation (EU) 2025/327.

(16) This Regulation introduces binding requirements for cross-border digital public services within the meaning of Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024[3]. Accordingly, an interoperability assessment has been carried out, and the resulting report will be published on the Interoperable Europe Portal upon adoption of this Regulation.

-

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (*OJ L 119, 4.5.2016, pp. 1–88, ELI: http://data.europa.eu/eli/reg/2016/679/oj).*

[2] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) PE/31/2018/REV/1(*OJ L 295, 21.11.2018, pp. 39–98, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).*

[3] Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act) PE/73/2023/REV/1 (*OJ L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj*).

(17) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[4] and delivered an opinion on XX 2026.

(18) The measures provided for in this Regulation are in accordance with the opinion of the committee established by Article 98(1) of Regulation (EU) 2025/327.

HAS ADOPTED THIS REGULATION:

CHAPTER I - General Provisions

Article 1 — Subject matter and scope

This Regulation lays down:

(a) the requirements, technical specifications and IT architecture of HealthData@EU, including its central platform, necessary to ensure state-of-the-art data security, confidentiality and protection of electronic health data;

(b) the conditions and compliance checks required for joining and remaining connected to HealthData@EU and the conditions for temporary disconnection or definitive exclusion from HealthData@EU, including specific provisions for cases of serious misconduct or repeated infringements;

(c) the minimum criteria to be met by national contact points for secondary use, the Union health data access service and authorised participants in HealthData@EU;

(d) the responsibilities of the controllers and processors participating in HealthData@EU;

(e) the responsibilities of the controllers and processors participating in the secure processing environment provided by the Commission as referred to in Article 75(9) of Regulation (EU) 2025/327;

(f) common specifications for the architecture of HealthData@EU and for its interoperability with other relevant common European data spaces;

(g) the architecture of, and the rules governing access to and use of, the IT tool referred to in Article 63(7) of Regulation (EU) 2025/327.

Article 2 — Definitions

For the purposes of this Regulation the following definitions shall apply:

[4] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(a) ‘central platform’ means the platform developed, deployed and operated by the Commission pursuant to Article 75(8) of Regulation (EU) 2025/327;

(b) ‘connected entity’ means a national contact point for secondary use, the Union health data access service or an authorised participant connected to HealthData@EU in accordance with this Regulation;

(c) ‘compliance check’ means the process conducted by the Commission, on the basis of the relevant evidence and, where applicable, technical tests, to determine whether an entity meets the requirements and conditions applicable to joining or remaining connected to HealthData@EU;

(d) ‘major release’ means a change to the central platform or to the technical specifications applicable to HealthData@EU that requires one or more connected entities to adapt their systems or connection;

(e) ‘minor release’ means a change to the central platform or to the technical specifications applicable to HealthData@EU that does not require connected entities to adapt their systems or connection;

(f) ‘enforcement measure’ means measures taken by a health data access body pursuant to Article 63 of Regulation (EU) 2025/327, including revocation of a data permit, a periodic penalty payment, an exclusion or other corrective action;

(g) ‘incident’ means an incident within the meaning of Article 6, point (6), of Directive (EU) 2022/2555;

(h) ‘significant incident’ means an incident considered significant in accordance with Article 23(3) of Directive (EU) 2022/2555;

(i) ‘steering group’ means the HealthData@EU steering group established by Article 95(1) of Regulation (EU) 2025/327 for the cross-border infrastructure provided for in Article 75 of that Regulation.

CHAPTER II – Architecture, technical documentation and interoperability requirements of HealthData@EU

Article 3 —HealthData@EU architecture

1. HealthData@EU shall be based on a centrally coordinated architecture comprising:

(a) the central platform;

(b) the information technology systems and components operated by the national contact points for secondary use, the Union health data access service and authorised participants that are necessary for their connection to and participation in HealthData@EU;

(c) the secure connections between the central platform and the systems and components referred to in point (b).

2. The Commission shall be responsible for the development, deployment, operation, security and maintenance of the central platform and of the other central services that it provides. Each connected entity shall be responsible for the development, deployment, operation, security and maintenance of the systems and components under its control and for maintaining its connection to the central platform.

3. The architecture referred to in paragraph 1 shall enable the secure exchange and routing of information between connected entities through the central platform and shall support the interoperability requirements laid down in Article 5.

Article 4 – Components of the central platform

1. The Commission in its capacity as operator of the central platform shall provide the information technology components and services necessary to:

   (a) enable the secure exchange and routing, between connected entities and the central platform, of information necessary for the operation of HealthData@EU, including applications submitted through the central platform, related notifications, decisions, metadata and operational or technical messages;

   (b) enable the submission and automatic forwarding of applications, pursuant to Article 67(3) of Regulation (EU) 2025/327, the exchange of application-related information, including updates, withdrawals, notifications of decisions and, where applicable, information on the results or output referred to in Article 61(4) of that Regulation;

   (c) support metadata management, orchestration and the interconnection of the national dataset catalogues and the dataset catalogues of authorised participants in HealthData@EU;

   (d) establish and make publicly available the EU dataset catalogue referred to in Article 79 of Regulation (EU) 2025/327;

   (e) make available through the central platform the Enforcement Information Exchange Tool referred to in Article 63(7) of Regulation (EU) 2025/327;

   (f) provide the user and access management, configuration, monitoring, orchestration and operational coordination functionalities necessary to support the components and services referred to in points (a) to (e)

2. The functions referred to in paragraph 1, points (a) and (b), shall be limited to the technical submission, transmission, routing and exchange of information. They shall not include the substantive assessment of health data access applications or the adoption of decisions assigned by Regulation (EU) 2025/327 to health data access bodies, the Union health data access service or authorised participants.

3. The components and services referred to in paragraph 1 shall operate in accordance with the technical documentation and the common specifications referred to in Article 5.

Article 5 – Technical documentation and interoperability

1. In accordance with Chapter III, the Commission shall, in cooperation with the steering group, develop, maintain and make available through a single access point, the technical documentation necessary for the connection to, interoperability with and operation of HealthData@EU.
2. The central platform and the systems and components referred to in Article 3(1), point (b), shall support technical, semantic and organisational interoperability.
3. The technical documentation shall specify the technical implementation of the requirements laid down in this Regulation, taking into account relevant Union interoperability requirements, Interoperable Europe solutions, Union semantic assets and common specifications applicable to common European data spaces. It shall include at least:
    (a) a description of the architecture of HealthData@EU, the components and services of the central platform, the interfaces with the systems and components operated by connected entities and the corresponding data flows;
    (b) the interfaces, message formats, message structures and exchange protocols to be implemented by connected entities;
    (c) the technical specifications for the submission, routing and exchange of the information referred to in Article 4(1), points (a) and (b);
    (d) the metadata models, semantic assets and controlled vocabularies to be used, and the specifications for the interconnection, synchronisation and publication of the EU dataset catalogue, the national dataset catalogues and the dataset catalogues of authorised participants;
    (e) the identification, authentication, authorisation, trust and access management requirements;
    (f) the technical and organisational security controls, including requirements concerning encryption, logging, monitoring, integrity, traceability and incident-notification mechanisms;
    (g) the standards and test specifications to be used;
    (h) the versioning, backward-compatibility, release-management and change-management procedures, including the testing and deployment stages and the actions and implementation timelines applicable to connected entities;
    (i) the functional and technical specifications of the Enforcement Information Exchange Tool, including access management, authentication, logging and retention rules.
4. The Commission shall make available the parts of the technical documentation necessary for the initial compliance checks and connection to HealthData@EU sufficiently in

advance of the start of those checks to enable the entities concerned to prepare their system and connection.

5. Connected entities shall implement the technical specifications and procedures applicable to them under the technical documentation in order to establish and maintain a secure, reliable and interoperable connection to the central platform.

CHAPTER III – Governance and evolution of HealthData@EU

Article 6 – Roles and responsibilities

1. The Commission shall perform the preparatory, technical, assessment and implementation tasks necessary to develop, deploy, maintain, host and operate the central platform and the other central services that it provides for HealthData@EU, in accordance with the operational decisions of the steering group.
2. In particular, the Commission shall:
   (a) prepare and maintain the technical documentation referred to in Article 5, the compliance check framework referred to in Article 10, the change proposals referred to in Article 7 and the annual work plan referred to in Article 8;
   (b) coordinate the development, testing, deployment, maintenance, monitoring and business continuity of the central platform and the other central services that it provides;
   (c) conduct the compliance checks referred to in article 11 and perform the related technical tests;
   (d) implement the connection, temporary disconnection, restoration of connection and other operational measures provided for in Chapter IV;
   (e) coordinate the response to incidents in accordance with Article 12;
   (f) monitor the operation, performance, availability and security of the central platform and report to the steering group on its operation, incidents and evolution;
   (g) provide operational support for entities required or seeking to connect and for connected entities, limited to onboarding and connection testing and use of the central platform;
3. The steering group shall take operational decisions concerning:
   (a) the approval of the technical documentation referred to in Article 5;
   (b) the approval of major releases including their implementation timelines in accordance with Article 7;
   (c) the approval of the compliance check framework referred to in Article 11 including subsequent changes that modify its assessment domains, methodology or criteria;

(d) the approval of the annual work plan referred to in Article 9;

(e) the authorisation of the connection of authorised participants referred to in Article 75(4) of Regulation (EU) 2025/327, in accordance with Article 15(5) of this Regulation;

(f) the confirmation of the operational readiness of authorised participants referred to in Article 75(5) of Regulation (EU) 2025/327, in accordance with Article 15(6) of this Regulation;

(g) the definitive exclusion of authorised participants referred to in Article 75(4) of Regulation (EU) 2025/327, in accordance with Article 16(5) of this Regulation.

4. The Commission shall provide the steering group with the information necessary for the adoption of the operational decisions referred to in paragraph 3 and shall implement those decisions within the limits of its responsibilities under Regulation (EU) 2025/327.

Article 7 – Change management

1. At the request of five or more members of the steering group or on its own initiative, the Commission may submit to the steering group a proposal for a change to the technical documentation that requires a major release.

2. The change proposal shall include at least:

(a) a description of the proposed change and corresponding modifications to the technical documentation;

(b) the reason and objectives for the proposed change;

(c) an assessment of the expected technical, interoperability, security and operational impact on the central platform and connected entities;

(d) the actions required from the Commission and connected entities;

(e) the proposed testing, deployment and rollback arrangements;

(f) the proposed implementation timeline, including an appropriate transition period, taking account of the scope of the required adaptations and the expected implementation effort.

~~3.~~ Where the steering group has taken an operational decision approving the change proposal, the Commission and the connected entities shall implement the corresponding major release in accordance with the approved timeline.

4. Minor releases shall not require the submission of a change proposal or an individual operational decision of the steering group. The Commission shall manage and deploy minor releases in accordance with the procedures referred to in paragraph 5 and shall inform the steering group and connected entities sufficiently in advance of their scope, expected operational impact and deployment date.

5. The procedures set out in the technical documentation pursuant to Article 5(3), point (h), shall govern:
   (a) the preparation and assessment of change proposals;
   (b) the planning, testing, deployment and rollback of major and minor releases;
   (c) the versioning of the technical documentation and maintenance of a change log;
   (d) the communication of approved timelines, expected impacts and required actions;
   (e) the notification by connected entities of the completion of implementation.

Article 8 – Annual work plan

1. Each year, the Commission shall submit to the steering group a draft annual work plan for the following calendar year in sufficient time to enable the steering group to approve it before the beginning of that year.
2. The annual work plan shall identify, where relevant:
   (a) priorities for the development, maintenance, lifecycle management and major releases of the central platform and the other central services provided by the Commission;
   (b) planned major releases and significant changes to the technical documentation;
   (c) planned activities relating to onboarding and compliance checks;
   (d) measures relating to security, resilience, business continuity and incident preparedness;
   (e) planned work relating to interoperability and the development of common specifications;
   (f) the main implementation milestones, dependencies and expected actions of the Commission and connected entities.

CHAPTER IV – Conditions for joining and remaining connected to HealthData@EU

Section 1 - Common requirements and procedures

Article 9 – Minimum criteria for entities required or seeking to connect to *HealthData@EU*

1. Without prejudice to the specific conditions laid down in Articles 13 to 16, national contact points for secondary use, the Union health data access service and entities seeking to become authorised participants shall:
   (a) ensure the availability of qualified expertise in information technology, cybersecurity, data protection and health data governance;

(b) have the technical capabilities necessary to implement the technical documentation and the common specifications referred to in article 5, establish and maintain a secure and reliable connection to the central platform, and participate in the required technical tests;

(c) have documented governance and operational arrangements defining responsibilities for the operation, security and compliance of the systems and components under their control;

(d) maintain appropriate risk management, incident response, business continuity and disaster recovery arrangements;

(e) have the operational capacity to participate in compliance checks, testing, change management and incident coordination and to implement corrective measures within the timelines set by the Commission;

(f) designate operational, technical and security contacts for communication with the Commission and the other connected entities and keep their contact details up to date.

2. An entity may rely on external expertise or service providers to meet the criteria referred to in paragraph 1. Such reliance shall not affect the entity's responsibility for compliance with this Regulation.

3. The Commission shall verify compliance with the criteria set out in paragraphs 1 and 2 through the compliance checks referred to in Article 11.

Article 10 – Compliance check framework

~~1.~~ The Commission shall prepare, maintain and update a compliance check framework for assessing whether entities meet the requirements and conditions to join and remain connected to HealthData@EU.

2. The compliance check framework shall cover at least:

(a) the legal eligibility, status and mandate of the entity concerned and any conditions specific to its category of participation;

(b) compliance with the minimum criteria set out in Article 9;

(c) compliance with the technical documentation and the common specifications referred to in Article 5;

(d) technical capability, interoperability and connection readiness;

(e) information security, confidentiality and data-protection requirements;

(f) operational capacity, business continuity, disaster recovery and incident management;

(g) the capacity to participate in releases, compliance checks and corrective-action procedures.

3. The compliance check framework shall specify:

(a) the forms of assessment, evidence requirements, technical tests and verification methods to be used;

(b) the criteria for determining whether the outcome of a compliance check is positive or negative;

(c) the scope, intervals and risk-based elements of regular compliance checks;

(d) the criteria and procedures for additional compliance checks;

(e) the determination and verification of corrective measures and implementation timelines;

(f) the reporting and reassessment procedures.

4. For entities referred to in Article 75(4) of Regulation (EU) 2025/327, the framework shall include criteria for verifying that the entity falls within the category established by that provision and that its activities support one or more of the purposes listed therein.

   For third countries and international organisations referred to in Article 75(5) of Regulation (EU) 2025/327, the framework shall include criteria for checking compliance with the legal, organisational, technical and security requirements set out in that provision, including the requirements relating to equivalent access, Chapter V of Regulation (EU) 2016/679 and secure processing environments.

5. For the purposes of Articles 14 and 16, the compliance check framework shall set out criteria for assessing serious misconduct, repeated infringements and the proportionality of possible measures. Those criteria shall take account of:

   (a) the nature, gravity and duration of the conduct or infringement;

   (b) its actual or potential impact on security, confidentiality, integrity, availability, interoperability or other connected entities;

   (c) whether the conduct was intentional or resulted from serious negligence;

   (d) the degree of cooperation by the entity concerned and its implementation of corrective measures;

   (e) the number, nature, frequency and proximity in time of previous infringements.

6. The Commission may make editorial or reference updates to the compliance check framework that do not alter its assessment domains, methodology or criteria. It shall inform the steering group of such updates.

Article 11– Initial, regular and additional compliance checks

1. Before an entity joins HealthData@EU, the Commission shall conduct an initial compliance check on the basis of the compliance check framework referred to in Article 10.

2. The Commission shall conduct regular compliance checks at least every five years from the completion of the preceding initial or regular compliance check. The compliance check framework may provide for a shorter interval where justified by the entity's participation regime, the risks involved or the outcome of a previous compliance check.

3. The Commission may conduct an additional compliance check where:

   (a) it has reasonable grounds including following a significant incident or repeated operational failure, to consider that a connected entity may no longer comply with the applicable requirements or conditions;

   (b) the connected entity notifies a material change to its systems, organisation or legal status.

4. The entity subject to a compliance check shall cooperate with the Commission and provide the information, evidence and access to testing facilities necessary to perform the check. Connected entities shall notify the Commission without undue delay of any material change to the information or circumstances on which their most recent compliance check was based.

5. Upon completion of a compliance check, the Commission shall issue a report to the entity concerned. The report shall:

   (a) set out the assessment, and, where applicable, the results of technical tests carried out as part of that check;

   (b) indicate whether the outcome of the compliance check is positive or negative. The outcome shall be positive where the entity meets the applicable requirements and conditions and negative where one or more of those requirements or conditions are not met.

6. Where the outcome of a compliance check is negative, the Commission shall identify the non-compliance, specify the corrective measures required and set a reasonable timeline for their implementation. Before finalising those measures and that timeline, the Commission shall give the entity concerned an opportunity to provide observations on the factual assessment, technical feasibility and timing. An entity that is not yet connected shall not be connected until a positive outcome has been issued. For a connected entity, failure to implement the corrective measures within the specified timeline may lead to the measures provided for in Article 14 or Article 16, as applicable.

7. Following implementation of the corrective measures, the Commission shall verify their implementation and update the outcome of the compliance check where appropriate. The Commission shall inform the steering group of the results of compliance checks and any outstanding corrective measures.

Article 12 – Incident management

1. Connected entities shall cooperate with the Commission in addressing incidents affecting or likely to affect the secure and reliable operation of HealthData@EU.

2. Connected entities shall notify the Commission without undue delay, after becoming aware of a significant incident affecting or likely to affect the secure and reliable operation of HealthData@EU.
3. The notification referred to in paragraph 2 shall include at least:
   (a) a description of the significant incident, including, where known, the type of threat or root cause that is likely to have triggered the incident;
   (b) its severity and actual or potential impact;
   (c) the mitigation measures taken or planned;
   (d) the expected duration of the incident and the estimated time required to restore normal operation.
4. The Commission shall coordinate the operational measures necessary to mitigate the incident, ensure continuity and protect the secure and reliable operation of HealthData@EU.
5. Where necessary to contain the incident or prevent a serious risk to HealthData@EU, the Commission may temporarily disconnect the connected entity concerned. The Commission shall notify the entity and the steering group without undue delay of the reasons for, scope of and expected duration of the temporary disconnection. Where the urgency of the situation does not allow the entity to submit observations before disconnection, the Commission shall give it an opportunity to submit observations as soon as possible afterwards.
6. The Commission shall restore the connection without undue delay once it has verified, where necessary in cooperation with the connected entity concerned, that the incident has been resolved and that reconnection does not compromise the secure and reliable functioning of HealthData@EU.
7. Where necessary for operational coordination, the Commission shall inform the steering group and affected connected entities of incidents affecting the central platform or more than one connected entity.
8. A temporary disconnection under this Article shall constitute an operational protective measure and shall not prejudge the application of Article 14 or Article 16.

Section 2 – National contact points for secondary use and the Union health data access service

Article 13 – Conditions for joining HealthData@EU

1. A national contact point for secondary use designated by a Member State or the Union health data access service shall notify the Commission when it is ready to connect to HealthData@EU and shall provide the information and evidence necessary for the initial compliance check referred to in Article 11(1).

2. The Commission shall enable the connection of the entity concerned where:

   (a) it has been designated or established in accordance with Article 75(1) or (2) of Regulation (EU) 2025/327;

   (b) it meets the minimum criteria laid down in Article 9;

   (c) it has implemented the technical documentation and the common specifications referred to in Article 5 that are applicable to its connection;

   (d) the initial compliance check has resulted in a positive outcome.

3. The Commission shall inform the steering group when a national contact point for secondary use or the Union health data access service has been connected.

Article 14 – Conditions for remaining connected to HealthData@EU and temporary disconnection

1. To remain connected to HealthData@EU, national contact points for secondary use and the Union health data access service shall:

   (a) continue to meet the minimum criteria laid down in Article 9;

   (b) comply with the technical documentation and the common specifications referred to in Article 5;

   (c) cooperate with compliance checks, incident management and change-management procedures;

   (d) implement corrective measures within the timeline specified by the Commission under Article 11(6).

2. Where non-compliance persists after the expiry of the timeline referred to in Article 12(6), or in cases of serious misconduct or repeated infringements, the Commission shall take appropriate and proportionate measures necessary to protect the secure and reliable operation of HealthData@EU. Such measures may include temporary disconnection until the non-compliance has been remedied.

3. Where the conduct or non-compliance creates an immediate serious risk to the security or reliable operation of HealthData@EU, the Commission may temporarily disconnect the entity before the expiry of the corrective-action timeline.

4. Before adopting a measure under paragraph 2, the Commission shall give the entity concerned an opportunity to submit observations. A measure adopted pursuant to paragraphs 2 and 3 shall specify:

   (a) its reasons and legal basis;

   (b) its scope and date of effect;

   (c) its duration or review date;

   (d) and the conditions for restoring the connection.

Where urgent action under paragraph 3 does not allow prior observations, the Commission shall give the entity an opportunity to submit observations as soon as possible afterwards.

5. The Commission shall restore the connection without undue delay once it has verified that the conditions referred to in paragraph 4, second subparagraph, point (d), have been fulfilled.

6. The steering group shall be informed of the results of compliance checks and of measures adopted pursuant to this Article.

Section 3 – Authorised participants

Article 15 – Conditions for joining HealthData@EU

1. An entity referred to in Article 75(4) or (5) of Regulation (EU) 2025/327 may submit to the Commission an application to become an authorised participant in HealthData@EU and request the initial compliance check referred to in Article 11(1).

2. The application shall include:

   (a) the identity, legal status and legal basis of the applicant;

   (b) the category of authorised participant for which it is applying;

   (c) a description of its mandate, activities and the purposes for which it seeks to participate in HealthData@EU;

   (d) evidence that it meets the minimum criteria laid down in Article 9 and the other requirements applicable to its participation regime;

   (e) the information necessary to perform the initial compliance check;

   (f) the contact details referred to in Article 9(1), point (f).

3. An applicant referred to in Article 75(4) of Regulation (EU) 2025/327 shall additionally demonstrate that:

   (a) it is a health-related research infrastructure or similar infrastructure whose functioning is based on Union law;

   (b) it provides support for the use of electronic health data for one or more of the purposes listed in that provision.

4. An applicant referred to in Article 75(5) of Regulation (EU) 2025/327 shall additionally demonstrate that:

   (a) it complies with the rules of Chapter IV of that Regulation;

   (b) it provides health data users located in the Union with access, on equivalent terms and conditions, to electronic health data held in its jurisdiction;

   (c) how transfers of personal data caused by access of health data users under its jurisdiction would comply with Chapter V of Regulation (EU) 2016/679;

(d) it meets the applicable legal, organisational, technical and security requirements, including the requirements for secure processing environments.

5. Where the Commission concludes that an applicant referred to in Article 75(4) of Regulation (EU) 2025/327 satisfies the conditions set out in paragraphs 2 and 3 and the initial compliance check has resulted in a positive outcome, it shall submit the compliance check report to the steering group. On the basis of that positive outcome, the steering group shall take an operational decision authorising the applicant's connection to HealthData@EU. The Commission shall enable the connection following that decision.

6. Where the Commission concludes that an applicant referred to in Article 75(5) of Regulation (EU) 2025/327 satisfies the conditions set out in paragraphs 2 and 4 and the initial compliance check has resulted in a positive outcome, it shall submit the compliance check report to the steering group. The steering group shall take an operational decision confirming the applicant's operational readiness to connect. The connection shall take effect only following the adoption and entry into force of an implementing act adopted pursuant to Article 75(13) of Regulation (EU) 2025/327.

7. Where the initial compliance check has a negative outcome, the procedure laid down in Article 11(6) and (7) shall apply.

Article 16 – Conditions for remaining connected to HealthData@EU, temporary disconnection and definitive exclusion

1. To remain connected to HealthData@EU, an authorised participant shall:

   (a) continue to satisfy the eligibility and participation conditions applicable to it under Article 75(4) or (5) of Regulation (EU) 2025/327;

   (b) continue to meet the minimum criteria laid down in Article 9;

   (c) comply with the technical documentation and the common specifications referred to in Article5;

   (d) cooperate with compliance checks, incident management and change-management procedures;

   (e) implement corrective measures within the timeline specified by the Commission under Article 11(6);

   (f) in the case of a participant referred to in Article 75(5) of Regulation (EU) 2025/327, continue to meet the conditions concerning equivalent access, international transfers and secure processing environments.

2. Where non-compliance persists after the expiry of the timeline referred to in Article 11(6), or in cases of serious misconduct or repeated infringements, the Commission shall take appropriate and proportionate measures necessary to protect the secure and reliable operation of HealthData@EU. Such measures may include temporary disconnection until

the non-compliance has been remedied.-Before adopting such measures, the Commission shall give the authorised participant an opportunity to submit observations.

3. Where the conduct or non-compliance creates an immediate serious risk to the security or reliable operation of HealthData@EU, the Commission may temporarily disconnect the authorised participant before the expiry of the corrective action timeline. Where urgent action does not allow prior observations, the Commission shall give the authorised participant an opportunity to submit observations afterwards.

4. A measure adopted pursuant to paragraphs 2 and 3 shall specify:

   (a) its reasons and legal basis;

   (b) its scope and date of effect;

   (c) its duration or review date;

   (d) and the conditions for restoring the connection.

   The Commission shall restore the connection without undue delay once it has verified that the conditions referred to in point (d) have been fulfilled.

5. Where serious misconduct or repeated infringements justify the definitive exclusion of an authorised participant referred to in Article 75(4) of Regulation (EU) 2025/327, the Commission shall:

   (a) notify the authorised participant of the proposed definitive exclusion and the reasons for it;

   (b) give the authorised participant an opportunity to submit observations within a reasonable period;

   (c) submit a reasoned proposal to the steering group, together with the observations submitted by the authorised participant.

   The steering group shall take an operational decision on the proposed definitive exclusion. Where it decides to exclude the authorised participant, the Commission shall give effect to that decision by terminating the participant's connection.

6. Where serious misconduct or repeated infringements justify the definitive exclusion of an authorised participant referred to in Article 75(5) of Regulation (EU) 2025/327, the Commission shall:

   (a) notify the authorised participant of the proposed definitive exclusion and the reasons for it;

   (b) give the authorised participant an opportunity to submit observations within a reasonable period;

   (c) consult the steering group on the proposed definitive exclusion;

   (d) decide whether to initiate the procedure to repeal or amend the implementing act adopted pursuant to Article 75(13) of Regulation (EU) 2025/327.

Definitive exclusion shall take effect only upon the adoption and entry into force of the implementing act repealing or amending the act by which that authorised participant was connected.

Pending that decision, the Commission may maintain a temporary disconnection where necessary to protect the secure and reliable operation of HealthData@EU.

7. A decision or proposal concerning definitive exclusion shall state the reasons, scope and date of effect of the exclusion and, where applicable, the conditions under which the entity may submit a new application.

8. The Commission shall inform the steering group of the results of compliance checks, outstanding corrective measures, temporary disconnections and restorations of connection under this Article.

CHAPTER V - Security and personal data protection

Section 1 - Responsibilities of the controllers and processors for the central platform of HealthData@EU

Article 17 - Processing of personal data in the central platform of HealthData@EU

The processing of personal data through the central platform of HealthData@EU shall be limited to:

(a) personal data submitted as part of a health data access application or a health data request in accordance with Article 67(2), point (a), and Article 69(2), point (a), of Regulation (EU) 2025/327;

(b) personal data shared through the Enforcement Information Exchange Tool, for the purposes of exchanging information on enforcement measures under Chapter VI of this Regulation;

(c) personal data of users of the central platform of HealthData@EU, such as records of their activities in the central platform, necessary to manage the central platform, including user support and helpdesk management.

Article 18 - Responsibilities of national contact points for secondary use as joint controllers

1. In their capacity as joint controllers within the meaning of Article 26(1) of Regulation (EU) 2016/679, the national contact points for secondary use shall::

(a) set up a contact point with a functional mailbox for the communication between the joint controllers and between the joint controllers and the Commission as processor;

(b) coordinate among themselves in the steering group to provide coordinated instructions to the Commission as processor;

(c) send any necessary instructions to the Commission, as the processor, through the steering group, as agreed with the other joint controllers in the group;

(d) ensure that data subjects are provided, including through the central platform where appropriate, information about the processing of personal data in HealthData@EU in accordance with Articles 13 and 14 of Regulation (EU) 2016/679, as applicable;

(e) address data subject requests for exercise of data subject rights as provided for by Regulation (EU) 2016/679. Where a joint controller receives a request that falls outside its responsibilities for HealthData@EU, it shall forward the request to the relevant joint controller and inform the data subject. Where a joint controller receives a request that, under that allocation or applicable national arrangements, should be handled by another joint controller or competent body, it shall forward the request without undue delay and inform the data subject thereof;

(f) take all appropriate organisational, physical and logical security measures to ensure that each national contact point for secondary use operates securely and document these measures. Those measures shall ensure that:

i. persons authorised to process personal data exchanged through HealthData@EU are under an appropriate statutory obligation of confidentiality or have committed themselves to confidentiality;

ii. exchanges of personal data taking place through HealthData@EU are logged systematically in accordance with the logging requirements specified in the technical documentation referred to in Article 5(1), in order to keep a record of personal data exchanges, including the identity of actors involved, the categories of personal data and the purposes for which they were exchanged;

(g) assist each other in identifying and handling any security incidents, including personal data breaches, linked to processing in HealthData@EU. In particular, the joint controllers shall notify each other and the Commission of:

i. any risks to the security of the personal data processed in HealthData@EU;

ii. any security incidents linked to personal data processing operations in HealthData@EU;

iii. any personal data breaches, the likely consequences of the personal data breaches and the assessment of the risk to the rights and freedoms of natural persons in accordance with Regulation (EU) 2016/679, and any measures taken to address the breach and mitigate the risk to the rights and freedoms of natural persons;

iv. any breaches of the technical or organisational safeguards of the processing operations in HealthData@EU;

(h) notify personal data breaches regarding processing operations in HealthData@EU to the competent data protection supervisory authorities and, where required, to data subjects, in accordance with Articles 33 and 34 of Regulation (EU) 2016/679;

2. If a joint controller requires information from another joint controller, in order to comply with its obligations laid down in Articles 33 and 34 of Regulation (EU) 2016/679, it shall send a specific request to the relevant functional mailbox referred to in paragraph 1, point (a). The other joint controller shall use their best efforts to provide such information.

Article 19 – Responsibilities of the Commission as processor for HealthData@EU

1. In its capacity as processor, the Commission shall:

(a) ensure the establishment, operation and maintenance of secure exchange services, including routing and coordination functionalities forming part of the central platform;

(b) ensure that the routing and coordination functionalities enable the secure, reliable and efficient routing of information between connected entities;

(c) implement the technical and organisational measures necessary to ensure interoperability between the central platform and connected entities, in accordance with the technical documentation referred to in Article 5(1);

(d) process personal data only on documented instructions from the joint controllers of HealthData@EU, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union law. In that case, the Commission shall inform the joint controllers of that legal requirement before processing, unless that law prohibits this on important grounds of public interest.

(e) put in place the necessary measures to ensure a level of security of data processed in the central platform appropriate to the risks. These measures shall be documented in a security plan which shall be kept up to date. These measures shall include:

i. establishing a risk assessment procedure to identify and assess potential threats to the system taking into account, where relevant, information provided by the joint controllers concerning risks related to their systems or processing operations in HealthData@EU;

ii. ensuring that persons authorised to process data are under an appropriate statutory obligation of confidentiality, such as that laid down in Article 17 of the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the Union, laid down in Council Regulation No 31

(EEC), 11 (EAEC)[5], or have committed themselves to confidentiality;

iii. taking adequate measures to ensure that its staff and contractors understand their responsibilities regarding information security and the protection of sensitive non-classified information;

iv. implementing technical and organisational security measures to prevent unauthorised access to personal data;

v. ensuring the integrity of information transmitted through the central platform;

vi. implementing, whenever necessary, measures to block unauthorised access to the central platform from the connected entities;

vii. ensuring that data transported within the central platform are encrypted;

viii. taking appropriate physical security measures, including:

(1) controlling access to the facilities and maintaining a visitor register for tracing purposes;

(2) ensuring that external persons granted access to premises are escorted by duly authorised staff.

(f) implement a change management procedure and keep the joint controllers informed in due time of changes that may affect communication with other national infrastructures, the security of those infrastructures or the security of processing operations in HealthData@EU;

(g) monitor on a regular basis the performance of all components of its central platform, produce regular statistics and keep records;

(h) implement audit and review procedures in order to:

i. check the correspondence between the implemented security measures and the security plan referred to in point (e);

ii. control on a regular basis the integrity of system files, security parameters and authorisations granted;

iii. monitor the HealthData@EU infrastructure to detect security or personal data breaches;

iv. implement changes to mitigate existing security weaknesses;

v. lay down a security incident management procedure setting out the reporting and escalation scheme;

[5] (ELI: http://data.europa.eu/eli/reg/1962/31(1)/oj)

vi. inform the relevant joint controllers of any security or personal data breach without delay.

(i) support the joint controllers by providing information on how the obligations in Articles 32 to 36 of Regulation (EU) 2016/679 are reflected in the central platform of HealthData@EU;

(j) Following termination of the data provision of HealthData@EU, it shall delete or return all personal data processed on behalf of a controller and certify to the controller that it has done so, unless applicable law requires storage of the personal data;

(k) provide the joint controllers all information necessary to demonstrate compliance with its obligations as processor and the security plan referred to in point (e). It shall allow for, and contribute to independent audits, including inspections and reviews of security measures, including at the request of the joint controllers, subject to conditions that comply with Protocol (No 7) to the Treaty on the Functioning of the European Union on the privileges and immunities of the European Union.

2. The Commission may engage third parties as sub-processors to fulfil these responsibilities.

Article 20 - Security of HealthData@EU

The Commission shall ensure the security of HealthData@EU, in accordance with this Regulation, and Commission Decision (EU, Euratom) 2017/46.

Section 2 - Responsibilities of the joint controllers and processors in the secure processing environment managed by the Commission

Article 21 – Processing of personal data in a secure processing environment provided by the Commission

In a secure processing environment provided by the Commission in accordance with Article 75(9) of Regulation (EU) 2025/327, the Commission shall, in its capacity as processor, only process the following categories of data:

(a) electronic health data for secondary use necessary for implementing a data permit issued pursuant to Article 68(3) of Regulation (EU) 2025/327 or for generating a response in anonymised statistical format to a health data request approved under Article 69 of that Regulation;

(b) electronic health data for secondary use made available on the basis of an access approval by an authorised participant referred to in Article 68(8) of that Regulation;

(c) personal data necessary to manage the secure processing environment, including access management for authorised natural persons listed in the data permit issued pursuant to Article 68(3) of Regulation (EU) 2025/327 or the access approval referred to in Article 68(8) of Regulation (EU) 2025/327.

Article 22 – Responsibilities of the joint controllers of the secure processing environment provided by the Commission

1. Without prejudice to Articles 73 and 74 of Regulation (EU) 2025/327 and to the tasks of health data access bodies prior to and following making data available in a secure processing environment, the national contact points for secondary use and authorised participants acting as joint controllers pursuant to Article 75(9) of Regulation (EU) 2025/327 for processing operations in a secure processing environment shall:

   (a) set up a contact point with a functional mailbox for the communication between the joint controllers and between the joint controllers and the Commission as a processor;

   (b) coordinate among themselves to provide, and document coordinated instructions to the Commission as processor;

   (c) send to the Commission only documented instructions agreed by the relevant joint controllers and keep a record of those instructions;

   (d) inform data subjects about the processing of personal data in the secure processing environment in accordance with Articles 13 and 14 of Regulation (EU) 2016/679, as applicable;

   (e) address data subject requests for exercise of data subject rights as provided for by Regulation (EU) 2016/679. Where a joint controller receives a request that falls outside its responsibilities for the secure processing environment, it shall forward the request to the relevant joint controller and inform the data subject.

   (f) notify any personal data breaches regarding the processing operation in the secure processing environment to the competent data protection supervisory authorities and, where required so, to data subjects, in accordance with Articles 33 and 34 of Regulation (EU) 2016/679.

2. If a joint controller, in order to comply with its obligations laid down in Articles 33 and 34 of Regulation (EU) 2016/679, needs information from another joint controller, it shall send a specific request to the relevant functional mailbox referred to in paragraph 1, point (a). The other joint controller shall use its best efforts to provide such information.

Article 23 – Responsibilities of the Commission as processor of the secure processing environment

1. In its capacity as processor in a secure processing environment, the Commission shall:

(a) process the personal data only on documented instructions from the joint controllers of the secure processing environment, unless required to do so by law. In such a case, the Commission shall inform the controller of that legal requirement before processing, unless that law prohibits this on important grounds of public interest;

(b) support the joint controllers by providing information on the secure processing environment, in order to implement the obligations in Articles 32 to 36 of Regulation (EU) 2016/679;

(c) following termination of the provision of the secure processing environment, without undue delay and in accordance with instructions from the joint controllers, delete or return all personal data processed on behalf of a controller and certify to the controller that it has done so, unless applicable Union or Member State law requires storage of the personal data;

(d) provide the joint controllers with all information necessary to demonstrate compliance with its obligations as processor and allow for, including at the request of controllers, and contribute to the performance of independent audits, including inspections, and reviews on security measures, subject to conditions that comply with Protocol (No 7) to the Treaty on the Functioning of the European Union on the privileges and immunities of the European Union;

(e) ensure that the secure processing environment it provides complies with the requirements laid down in Article 73 of Regulation (EU) 2025/327 and with the implementing acts referred to in Article 73(5) of that Regulation.

2. The Commission may engage third parties as sub-processors to fulfil these responsibilities.

CHAPTER VI - Enforcement Information Exchange Tool

Article 24 — Development, architecture and purpose of the Enforcement Information Exchange Tool

1. The Commission shall develop, operate and maintain an Enforcement Information Exchange Tool as a component of the central platform and make it available to the users referred to in Article 25(1).

2. The Enforcement Information Exchange Tool shall comprise:

(a) a secure interface enabling health data access bodies and the Union health data access service to record and update information on enforcement measures;

(b) a central repository for the information recorded pursuant to Article 25;

(c) functionalities enabling authorised users to consult and search the information recorded in the tool and to be informed of new records and changes to existing records;

(d) identity, access management and logging functionalities necessary to restrict access to authorised users and to ensure the traceability of actions conducted in the tool.

3. The Enforcement Information Exchange Tool shall support:

(a) the notification to other health data access bodies of enforcement measures taken pursuant to Article 63(3) of Regulation (EU) 2025/327, in accordance with Article 63(6) of that Regulation;

(b) the transparency and coordination of enforcement measures referred to in Article 63 of Regulation (EU) 2025/327, in particular periodic penalty payments, the revocation of data permits and exclusions.

4. The Enforcement Information Exchange Tool shall operate in accordance with the technical documentation referred to in Article 5. That documentation shall specify, in particular, the detailed functional and technical specifications relating to the interfaces, access management, authentication, notifications, searching, logging, security and retention of information.

Article 25 - Access to, content and updating of enforcement information

1. Access to the information recorded in the Enforcement Information Exchange Tool shall be limited to:

(a) individual users authorised by the health data access bodies of the Member States;

(b) individual users authorised by the Union health data access service;

(c) Commission users for whom access is necessary for the operation, maintenance, security, support or audit of the tool.

2. The health data access body that adopts an enforcement measure pursuant to Article 63(3) of Regulation (EU) 2025/327 shall record that measure in the Enforcement Information Exchange Tool without undue delay.

The first subparagraph shall also apply to the Commission where it acts as the Union health data access service in accordance with Article 56 of Regulation (EU) 2025/327. Recording the measure in the tool shall constitute its notification to the other health data access bodies for the purposes of Article 63(6) of Regulation (EU) 2025/327.

3. The Enforcement Information Exchange Tool shall also enable health data access bodies to record enforcement measures taken pursuant to Article 63(4) of Regulation (EU) 2025/327, in particular periodic penalty payments and exclusions, where the health data access body considers that the exchange of that information is necessary for the purposes of transparency or coordination.

The information recorded in the Enforcement Information Exchange Tool shall be limited to what is necessary for the purposes referred to in Article 24(3).

4. Each record shall include, at least, where applicable:

   (a) the health data access body or the Union health data access service that adopted the enforcement measure;

   (b) the type of enforcement measure;

   (c) the legal basis of the enforcement measure;

   (d) the date on which the measure was adopted and, where different, the date from which it applies;

   (e) the duration and expiry date of the measure;

   (f) the health data holder or health data user concerned and the identifiers strictly necessary to distinguish that holder or user;

   (g) a concise description of the non-compliance concerned and the reasons for the enforcement measure;

   (h) the current legal status of the enforcement measure;

   (i) a reference to the relevant administrative decision;

   (j) where necessary for the purposes referred to in Article 24(3), the relevant administrative decision, or an extract or summary thereof;

   (k) where the decision has been published, a link to the website on which it is available.

5. For the purposes of paragraph 4, point (h), the legal status shall indicate whether the measure:

   (a) is in force;

   (b) is under administrative or judicial review, where such review proceedings have been initiated;

   (c) has been suspended;

   (d) has been revoked;

   (e) has expired;

   (f) is otherwise no longer applicable.

   Where relevant, the record shall also indicate whether the administrative decision has become final and whether the initiation of administrative or judicial review has suspended its effects.

6. The health data access body or the Union health data access service that recorded the information shall be responsible for its accuracy and completeness.

7. The Commission shall not be responsible for assessing the legality or substantive accuracy of the enforcement measures recorded in the tool. Where the Commission identifies information that is manifestly incomplete or internally inconsistent, it may request the

health data access body or the Union health data access service that recorded the information to verify and, where appropriate, correct or complete it.

CHAPTER VII - Final provisions

Article 26 — Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from 26 March 2029.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission

The President

[…]

[Choose between the two options, depending on the person who signs.]

On behalf of the President

[…]

[Position]