EUROPEAN
COMMISSION

Brussels, XXX
PLAN/2702/2025
(POOL/C1/2025/2702/2702-EN.docx)
[…](2026) XXX draft

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

on MyHealth@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 MyHealth@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 23(4) and (8) thereof,

Whereas:

(1) Regulation (EU) 2025/327 seeks to improve natural persons' access to and control over their personal electronic health data in the context of healthcare and to improve the cross-border exchange of such data to ensure continuity of healthcare. To this end, Article 23 of that Regulation tasks the Commission with establishing MyHealth@EU, a central interoperability platform for the cross-border exchange of the priority data categories set out in Article 14 of that Regulation as well as additional categories of data. The exchange of such data is supported by the European electronic health record exchange format referred to in Article 15 of Regulation (EU) 2025/327.

(2) MyHealth@EU under the EHDS builds upon the architecture and processes developed for the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services set up under Commission Implementing Decision 2019/1765[2]. That infrastructure allowed Member States to exchange patient summaries, electronic prescriptions and electronic dispensations on a voluntary basis. MyHealth@EU under the EHDS ought to build upon this experience and the architecture of the services under Commission Implementing Decision 2019/1765 and be updated to reflect technological changes and differences with the EHDS.

(3) To facilitate the exchange of personal electronic health data between national contact points for digital health, the Commission should provide a reference implementation of software for optional use by national contact points for digital health. The reference implementation should be based on the requirements catalogue and be regularly updated to reflect any changes.

-

[1] OJ L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj.

[2] Commission Implementing Decision 2019/1765 of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, and repealing Implementing Decision 2011/890/EU (OJ L 270, 24.10.2019, p. 83, ELI: http://data.europa.eu/eli/dec_impl/2019/1765/oj).

(4) To ensure the semantic interoperability of services in MyHealth@EU, the Commission should provide a central terminology service that enables Member States to provide mappings and translations to and from coding systems and values used in the exchange of personal electronic health data.

(5) National contact points for digital health should exchange personal electronic health data across borders using a secure communication network that should be provided by the Commission.

(6) To allow national contact points for digital health to discover and establish trusted communication between each other, they should use a central configuration service that should be provided by the Commission.

(7) To ensure interoperability, a requirements catalogue should be drawn up by the Commission in cooperation with the MyHealth@EU steering group established by Article 95(1) of Regulation (EU) 2025/327. On the basis of these requirements, technical specifications should be proposed by the Commission and adopted by the steering group. The technical specifications should be in line with the European electronic health record exchange format as set out in Commission Implementing Regulation (EU) …[3] [Implementing Regulation to be adopted on the basis of Article 15(1) of Regulation (EU) 2025/327].

(8) The Commission should propose an annual work plan for the operations and management of the central interoperability platform for approval by the steering group. This work plan ought to be consistent with the two-year work plan of the EHDS Board.

(9) Where a change to the requirements catalogue and technical specifications has a substantial impact on national contact points for digital health, a release management process should be followed for developing and implementing this change. Proposals for major releases of the requirements catalogue should be thoroughly prepared before they are submitted for evaluation and approval to the steering group. To that end, it should be required that a change proposal should be submitted either by a group of members of the steering group or by the Commission, given that it is responsible for managing MyHealth@EU. By contrast, when introducing minor changes that do not have a substantial impact on the exchange of personal electronic health data through MyHealth@EU, such as defects identified following a release, a simplified change management procedure should be applied. Considering that both minor and major releases can vary in complexity, the steering group should be informed and approve the releases and the timeline for their implementation.

(10) In order to ensure high quality in the development and operation of the exchange of personal electronic health data through MyHealth@EU, the Commission, on behalf of the MyHealth@EU steering group, should manage the procedures for authorising the exchange of personal electronic health data.

(11) National contact points for digital health should show that they comply with the requirements catalogue through technical tests and compliance checks. The Commission should facilitate technical tests and conduct compliance checks. Afterwards, the Commission should indicate deviations from the requirements

-

[3] Commission Implementing Regulation (EU) … [Implementing Regulation to be adopted on the basis of Article 15(1) of Regulation (EU) 2025/327] of … (OJ L …, ELI: …).

catalogue. Findings of compliance checks and technical tests should be classified based on factors such as risk and impact. National contact points for digital health should draw up action plans to resolve any identified risks. The Commission should regularly report to the steering group on any outstanding findings and action plans related to them.

(12) A national contact point for digital health should always be compliant with the latest release of the requirements catalogue. To facilitate trust in the network and show to all other national contact points that they are compliant, compliance checks should be conducted on a regular basis. A compliance check ought to be a thorough procedure and be done on a frequency proportionate to the level of risk to protection of personal electronic health data, security and confidentiality which the exchange of personal electronic health data poses. If there are any reasons to suspect a national contact is in breach of the requirements, the Commission should be empowered to initiate an ad-hoc compliance check.

(13) Whenever a national contact point starts the exchange of personal electronic health data, it should be based on an authorisation from the steering group. This ensures that the steering group has control over the exchange of personal electronic health data. To ensure predictability for the national contact points for digital health starting the exchange, the foundation for the steering group decision should be the outcome of a relevant compliance check and technical test.

(14) To ensure interoperability between national contact points for digital health when exchanging personal electronic health data, they should operate using the same release of the requirement catalogue. Technical solutions following those requirements should be thoroughly tested before being used for exchange of personal electronic health data. The steering group should assess the outcome of these tests and authorise a national contact point for digital health to upgrade to a new major release.

(15) Following a compliance check of a national contact point for digital health already exchanging personal electronic health data, the steering group should assess the outcome and give its authorisation for continuing the exchange.

(16) A national contact point for digital health may discover that the exchange of personal electronic health data is not functioning correctly. The Commission, in cooperation with the steering group should detail types of such incidents and identify proper responses to handle them in an operations framework.

(17) There should be a clear definition of what personal electronic health data can be processed through MyHealth@EU and it should correspond to the obligations set out in Regulation (EU) 2025/327.

(18) Article 23 of Regulation (EU) 2025/327 assigns the role of joint controllers to the national contact points for digital health and that of processor to the Commission for providing MyHealth@EU. To ensure uniform conditions in order to implement Regulation (EU) 2025/327, this Regulation should detail the roles and responsibilities of the national contact points for digital health and of the Commission on the basis of that assignment. To that end, this Regulation should set out the subject matter, duration, nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller, insofar as these are not already defined in Regulation

(EU) 2025/327. It should also lay down the respective responsibilities of the joint controllers.

(19) Regulation (EU) 2025/327 establishes that the Commission shall act as processor for the processing of personal data in MyHealth@EU, on behalf of the Member States as joint controllers. In accordance with data protection rules, the processor's obligations are to be set out in a contract or other legal act that is binding on the processor with regard to the controller. This Regulation sets out the Commission's detailed obligations as a processor in a binding legal act. Similarly, joint controllers are to determine their respective responsibilities for compliance with their data protection obligations by means of an arrangement between them unless, and in so far as, the respective responsibilities of the joint controllers are determined by Union or Member State law to which the joint controllers are subject. This Regulation determines the respective responsibilities of the joint controllers by law.

(20) Rules on IT security set out in Commission Decision (EU, Euratom) 2017/47[4] apply to MyHealth@EU.

(21) As MyHealth@EU is an evolution of the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services set up under Commission Implementing Decision 2019/1765, it is appropriate to take lessons learned from it into account. In particular, given that the detailed technical requirements for the exchange of data are essentially equivalent, it is appropriate that where a national contact point for electronic health is already connected in production usage to the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services, and the same contact point is designated as that Member State's national contact point for digital health, that contact point does not have to repeat the initial compliance check for the services that it has in production usage, as it has already proven its ability to connect to the central platform.

(22) (EU) 2025/327 will become applicable in a phased way. The obligations to exchange data through MyHealth@EU will become applicable on 26 March 2029 as regards the exchange of patient summaries, electronic prescriptions and electronic dispensations, and on 26 March 2031 for the exchange of medical imaging studies and related imaging reports, medical test results, including laboratory and other diagnostic results and related reports, and discharge reports. The present Regulation establishes the detailed rules on how MyHealth@EU will function; the obligation on Member States' national contact points to exchange the priority categories of personal electronic health data through MyHealth@EU will become applicable in accordance with Article 105 of Regulation (EU) 2025/327.

(23) 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[5] and delivered its opinion on XX XX 2026[6].

-

[4] Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (OJ L 6, 11.1.2017, p. 40).

[5] 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

(24) This Implementing Regulation introduces binding requirements for cross-border digital public services within the meaning of Regulation (EU) 2024/903. Accordingly, an interoperability assessment has been carried out and the resulting report will be published on the Interoperable Europe Portal when the legal act is adopted.

(25) 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 1
GENERAL PROVISIONS

Article 1
Subject matter

This Regulation lays down the rules regarding the requirements of cybersecurity, technical interoperability, semantic interoperability, operations and service management in relation to the processing by the Commission as processor for MyHealth@EU and its responsibilities towards the joint controllers.

It provides the necessary measures for the technical development of MyHealth@EU, detailed rules concerning the security, confidentiality and protection of personal electronic health data and the conditions for compliance checks necessary to join and remain connected to MyHealth@EU.

Article 2
Definitions

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

1. 'steering group' means the MyHealth@EU steering group established by Article 95(1) of Regulation (EU) 2025/327 for the cross-border infrastructure provided for in Article 23 of that Regulation;

2. 'major release' means a version of the requirements catalogue and technical specifications and their implementation with a substantial impact on the exchange of personal electronic health data through MyHealth@EU;

3. 'minor release' means a version of the requirements catalogue and technical specifications and their implementation that does not have a substantial impact on the exchange of personal electronic health data through MyHealth@EU;

4. 'critical incident' means a serious unplanned disruption of the cross-border exchange of personal electronic health data through MyHealth@EU that puts at risk security, confidentiality and protection of personal electronic health data.

CHAPTER 2
CROSS-BORDER DATA EXCHANGE AND CENTRAL

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).

[6] OJ C …

INTEROPERABILITY PLATFORM FOR DIGITAL HEALTH

Article 3

Central interoperability platform for digital health

1. The Commission shall provide the following services of the central interoperability platform for digital health referred to in Article 23(1) of Regulation (EU) 2025/327:

   (a) a reference implementation software for national contact points for digital health;

   (b) a central terminology service;

   (c) a secure communication network;

   (d) a central configuration service.

2. The Commission shall provide the services referred to in paragraph 1 in accordance with the requirements catalogue referred to in Article 4(2) and technical specifications referred to in Article 4(3).

3. National contact points for digital health may use the reference implementation referred to in paragraph 1, point (a), to support the exchange of personal electronic health data between national contact points for digital health. Where a national contact point for digital health chooses to use alternative solutions, these shall be compliant with the requirements catalogue referred to in Article 4(2) and technical specifications referred to in Article 4(3).

4. National contact points for digital health may use the central terminology service referred to in paragraph 1, point (b), to support the translation and mapping of the coding systems and values to be used in datasets containing personal electronic health data as referred to in Article 15(1), first subparagraph, point (b), of Regulation (EU) 2025/327. The translation and mapping of coding systems and values shall remain the responsibility of the Member States.

5. National contact points for digital health shall use the secure communication network referred to in paragraph 1, point (c) to support the exchange of personal electronic health data between national contact points for digital health. The operation of national infrastructures and national services supporting the secure communication network shall remain the responsibility of national contact points for digital health.

6. National contact points shall use the central configuration service referred to in paragraph 1, point (d) to make their configuration details available to the Commission and to all other national contact points for digital health.

Article 4

Requirements catalogue and technical specifications

1. Where national contact points for digital health perform cross-border exchange of personal electronic health data referred to in Article 23(3) of Regulation (EU) 2025/327, they shall perform it in accordance with the requirements

catalogue referred to in paragraph 2 and the technical specifications referred to in paragraph 3.

2. The Commission, in cooperation with the steering group, shall draw up and maintain the requirements catalogue for the cross-border exchange of personal electronic health data referred to in Article 23(3) of Regulation (EU) 2025/327. That requirements catalogue shall include at least:

   (a) a description of the use cases implemented for the exchange of personal electronic health data;

   (b) requirements for the implementation of the exchange of personal electronic health data;

   (c) frameworks and procedures for the testing, compliance checking, operation, monitoring of incidents of the exchange of personal electronic health data.

3. The Commission, in cooperation with the steering group, shall propose the technical specifications based on the requirements catalogue referred to in paragraph 2.

4. The requirements catalogue referred to in paragraph 2 and the technical specifications referred to in paragraph 3 shall be approved by the steering group.

Article 5

Operations and management of MyHealth@EU

1. The Commission, in cooperation with the steering group, shall perform the following activities for the operations and management of MyHealth@EU:

   (a) elicitation, analysis, and management of requirements and technical specifications;

   (b) coordination of development, testing, and deployment;

   (c) changes to the requirements catalogue;

   (d) incident management;

   (e) ensuring business continuity of the platform.

2. The Commission shall perform the following tasks:

   (a) conduct technical tests for national contact points for digital health of the cross-border exchange of personal electronic health data;

   (b) provide support to the service desks of national contact points for digital health.

3. The Commission, in cooperation with the steering group, shall propose an annual work plan for the activities referred to in paragraphs 1 and 2 for approval by the steering group.

Article 6

Changes to the requirements catalogue

1. Upon request by five or more members of the steering group or on its own initiative, the Commission may submit to the steering group a proposal for changes to a major release. The change proposal shall include at least:

   (a) a description of the changes

   (b) a justification for the changes;

   (c) a timeline for implementation of the changes;

   (d) a major release to address the proposed changes.

2. The steering group shall be responsible for approving the changes to the requirements catalogue referred to in Article 4(2), the timeline for implementation of the changes and the major release.

3. Once the changes referred to in paragraph 2 are approved, the Commission and the national contact points for digital health shall implement them in accordance with the approved implementation timeline and major release.

4. A minor release shall not be subject to the submission of a change proposal. The Commission may submit a change for a minor release to the steering group. Where such a change is submitted, the steering group shall, upon receipt, be responsible for approving the proposal for a minor release, including its implementation timeline. Once the minor release is approved, the Commission and the national contact points for digital health shall implement them in accordance with the approved implementation timeline and minor release.

Article 7

Managing authorisation for cross-border exchange of personal electronic health data

1. The Commission shall, on behalf of the steering group, be responsible for managing the procedures for authorising the exchange of personal electronic health data. They shall be the following:

   (a) authorising a national contact point for digital health to start the exchange of personal electronic health data;

   (b) authorising a national contact point for digital health to continue the exchange of personal electronic health data after an upgrade to the latest major release;

   (c) authorising a national contact point for digital health to continue the exchange of personal electronic health data after an operational compliance check referred to in Article 9, point b;

   (d) addressing critical incidents in the exchange of personal electronic health data.

2. The Commission, in collaboration with the steering group, shall propose the methodology for the procedures on authorisations referred to in paragraph 1, for adoption by the steering group.

3. The steering group shall decide whether or not to grant an authorisation referred to in paragraph 1, points (a), (b) or (c) to a national contact point for digital health on the basis of the requirements laid down in Articles 10 to 12.

4. Where the steering group decides not to grant an authorisation provided for in paragraph 1 to a national contact point for digital health, that national contact point may request the steering group to review its decision.

Article 8

Conditions for joining and remaining connected to MyHealth@EU, compliance checks and technical tests

1. The Commission shall conduct compliance checks and facilitate technical tests to assess the compliance of the exchange of personal electronic health data between national contact points for digital health with the requirements catalogue referred to in Article 4(2) and the technical specifications referred to in Article 4(3).

2. A compliance check shall identify findings on security, confidentiality and protection of the exchange of personal electronic health data through MyHealth@EU. Findings shall be categorised as 'minor', 'medium' or 'critical' depending on levels of compliance as defined in the compliance check framework referred to in Article 4(2), point (c).

3. A technical test shall assess the cross-border exchange of personal electronic health data between national contact points through MyHealth@EU and their conformance with the technical specifications referred to in Article 4(3). Findings shall be categorised as 'minor', 'medium' or 'critical' depending on levels of compliance as defined in the test framework referred to in Article 4(2), point (c).

4. The Commission shall inform the national contact points for digital health of the results of the compliance checks and technical tests referred to in paragraph 1. This information shall contain, as a minimum, findings, observations and recommendations based on the results of the compliance checks and technical tests.

5. Where a compliance check or technical test has identified findings, regardless of their level, the national contact point for digital health concerned shall take measures to close findings after receiving information on the outcome of the compliance check or technical test from the Commission. An action plan containing measures to address the identified findings shall be submitted to the Commission within 15 working days of receipt of information on the findings.

6. After an action plan has been implemented, the national contact point for digital health shall notify the Commission. The Commission shall then assess the relevant evidence and decide to close any of the addressed findings.

7. The Commission shall regularly communicate unresolved findings from compliance checks and technical tests to the steering group.

Article 9

Frequency of compliance checks

The Commission shall assess the compliance of the exchange of personal electronic health data with the requirements catalogue referred to in Article 4(2) and the technical specifications referred to in Article 4(3):

(a) before the start of the exchange of personal electronic health data;

(b) every five years after the latest compliance check;

(c) where the Commission considers that there is a critical risk to the security, confidentiality or protection of personal electronic health data.

Article 10

Authorisation to start the exchange of personal electronic health data

A national contact point for digital health shall obtain authorisation referred to in Article 7(1), second sentence, point (a), before starting the exchange of personal electronic health data. The authorisation shall be based on:

(a) a test result without critical findings pursuant to Article 8(4);

(b) a compliance check result without critical findings pursuant to Article 8(4);

(c) action plans referred to in Article 8(5).

Article 11

Authorisation to upgrade and to continue the exchange of personal electronic health data following an upgrade

1. Each national contact point for digital health shall obtain authorisation referred to in Article 7(1), second sentence, point (b), no later than one month before the end of the timeline referred to in Article 6(3). The authorisation shall be based on a technical test result without critical findings referred to in Article 8(4).

2. Where a national contact point for digital health is not granted authorisation referred to in paragraph 1, the steering group shall adopt mitigation measures, which may include the temporary suspension of the exchange of personal electronic health data.

3. Where the exchange of personal electronic health data is suspended in accordance with paragraph 2, the national contact point for digital health shall take the following measures:

   (a) address the findings that caused the suspension;

   (b) obtain authorisation referred to in Article 7(1), second sentence, point (b);

   (c) implement an upgrade to the latest major release and restore the exchange of personal electronic health data.

Article 12

Continuing the exchange of personal electronic health data following an operational compliance check

1. Each national contact point for digital health shall obtain authorisation referred to in Article 7(1), second sentence, point (c), no later than two months after receiving a compliance check result referred to in Article 8(4). The authorisation shall be based on a compliance check result without critical findings.

2. Where a national contact point for digital health is not granted authorisation referred to in paragraph 1, the steering group shall adopt mitigation measures, which may include the temporary suspension of the exchange of personal electronic health data.

3. When the exchange of personal electronic health data is suspended in accordance with paragraph 2, the national contact point for digital health shall take the following measures:

   (a) resolve findings causing the suspension;

   (b) obtain authorisation referred to in Article 7(1), second sentence, point (c);

   (c) restore the exchange of personal electronic health data.

Article 13

Critical incidents

1. A national contact point for digital health shall notify the chair of the steering group, the Commission and any relevant affected national contact points for digital health as soon as possible, and in any event within 24 hours of becoming aware of a critical incident.

2. Following notification referred to in paragraph 1, or on its own initiative, the Commission, in agrement with the chair of the steering group, shall address the critical incident.

3. The national contact point for digital health whose cross-border exchange of personal electronic health data is affected by the critical incident, and the steering group if necessary, shall take the necessary measures to mitigate the incident. Such measures may include the temporary suspension of the exchange of personal electronic health data.

4. The national contact point for digital health concerned shall, following approval of the steering group, restore the suspended cross-border exchange of personal electronic health data as soon as possible following resolution of the critical incident.

5. The national contact point for digital health whose cross-border exchange of personal electronic health data was affected by the critical incident or the Commission, if a service referred to in Article 3(1) was affected by the critical incident, shall report to the steering group no later than one month after submission of the notification referred to in paragraph 1. This shall include at least the following:

(a) a detailed description of the critical incident, including its severity and impact;

(b) the type of threat or root cause that is likely to have triggered the critical incident;

(c) the mitigation measures already taken and still being taken.

CHAPTER 3
PROCESSING, SECURITY, CONFIDENTIALITY AND PROTECTION OF PERSONAL DATA

Article 14

Processing of personal data in MyHealth@EU

The processing of personal data in MyHealth@EU shall be limited to:

(a) the priority categories of personal electronic health data for primary use referred to in Article 14(1), first subparagraph, of Regulation (EU) 2025/327;

(b) additional categories of personal electronic health data for primary use referred to in Article 14(1), third subparagraph, of Regulation (EU) 2025/327;

(c) personal data necessary to manage MyHealth@EU, including management of the help desk.

Article 15

Responsibilities of the national contact points for digital health as joint controllers

1. In their capacity as joint controllers, the national contact points for digital health shall have the responsibilities listed below.

(a) They shall set up a contact point with a functional mailbox for communication between the joint controllers and between the joint controllers and the processor.

(b) They shall coordinate among each other in the steering group to provide coordinated instructions to the Commission as a processor.

(c) They shall 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) They shall be responsible for informing data subjects about the processing of personal data in MyHealth@EU in accordance with Articles 13 and 14 of Regulation (EU) 2016/679 of the European Parliament and of the Council[7].

(e) They shall 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

[7] 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) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

MyHealth@EU, it shall forward the request to the relevant joint controller and inform the data subject.

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

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

(ii) exchanges of personal data through MyHealth@EU are logged systematically 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) They shall assist each other in identifying and handling any security incidents, including personal data breaches, linked to processing in MyHealth@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 MyHealth@EU;

(ii) any security incidents linked to personal data processing operations in MyHealth@EU;

(iii) any personal data breach, the likely consequences of the breach and the assessment of the risk to the rights and freedoms of natural persons, and any measures taken to address the breach and mitigate the risk to those rights and freedoms;

(iv) any breach of technical or organisational safeguards of the processing operations in MyHealth@EU;

(h) They shall communicate any personal data breaches with regard to processing operations in MyHealth@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, 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 make best efforts to provide such information.

Article 16

Responsibilities of the Commission as processor

In its capacity as processor, the Commission shall have the responsibilities listed below. The Commission may engage third parties as sub-processors to fulfil these responsibilities.

(a) It shall set up and maintain a secure and reliable communication service for national contact points for digital health participating in MyHealth@EU ('central secure communication service').

(b) It shall configure the central secure communication service so as to allow national contact points for digital health to exchange information securely, reliably and efficiently.

(c) It shall take measures to facilitate interoperability and communication between the central secure communication service and the joint controllers of MyHealth@EU.

(d) It shall process personal data only on instructions from the joint controllers of MyHealth@EU, unless required to do so by law to which it is subject. In that case, the Commission shall inform the controller of that legal requirement before processing, unless that law prohibits this on important grounds of public interest. [Article 28(3) second subparagraph EUDPR] The Commission shall immediately inform the joint controllers if, in its opinion, instructions given infringe applicable data protection provisions.

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

(i) putting in place a risk assessment procedure to identify and estimate potential threats to the system;

(ii) ensuring that persons authorised to process personal 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 (EEC, Euratom, ECSC) No 259/68[8], 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 sent through the central secure communication service;

(vi) implementing, whenever necessary, measures to block unauthorised access to the central secure communication service from the domain of national contact points for digital health;

(vii) ensuring that data transported within the central secure communication service 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.

-

[8] OJ L 56, 4.3.1968, p. 1, ELI: http://data.europa.eu/eli/reg/1968/259(1)/oj.

(f) It shall implement a change management procedure and keep the joint controllers informed of any changes that may affect communication with other national infrastructures or the security of those infrastructures.

(g) It shall monitor in real time the performance of all components of its central secure communication service, produce regular statistics and keep records.

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

(i) check 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 authorisation granted;

(iii) monitor to detect security breaches;

(iv) implement changes to mitigate existing security weaknesses;

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

(vi) inform the relevant joint controllers and the European Data Protection Supervisor of any security breach without delay.

(i) It shall publish on its website patient information notices about the processing of personal data in MyHealth@EU, after agreeing their content with the joint controllers.

(j) It shall support the joint controllers by providing information on the central secure communication service of MyHealth@EU, in order to implement the obligations in Articles 32 to 36 of Regulation (EU) 2016/679.

(k) Following termination of the data exchange, it shall delete 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.

(l) It shall 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.

Article 17

Security of MyHealth@EU

The Commission shall ensure the security of MyHealth@EU, in accordance with Commission Decision (EU, Euratom) 2017/46[9].

[9] Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (OJ L 6, 11.1.2017, p. 40, ELI: http://data.europa.eu/eli/dec/2017/46/oj).

CHAPTER 4
TRANSITION

Article 18
Transitional measures

National contact points for e-Health that have exchanged personal electronic health data through the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services pursuant to Implementing Decision 2019/1765 before 26 March 2029 and which have been designated as national contact points for digital health under Article 23(2) of Regulation (EU) 2025/327 may continue to exchange such data in the framework of MyHealth@EU and shall be deemed to comply with the authorisation requirements to start the exchange of personal electronic health data laid down in this Regulation.

CHAPTER 5
FINAL PROVISIONS

Article 19
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 2027.

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

Done at Brussels,

For the Commission
The President
Ursula VON DER LEYEN