Bio-curity D4.1 Appendix v1.0: Quotations

Changes Tracker

This document is an amended version of the original Appendix D4.1. In the table below we summarise the changes.

Affected area	Changes	Version
Appendix	The original version contained an incomplete list of quotations per criteria, missing quotations were added in the current version.	1.0

The criteria for the deliverable D4.1 stem from a body of literature consisting of law, regulations and standards. To gather these criteria, a thematic analysis was performed. The codes that resulted from this thematic analysis form the basis of the criteria included in D4.1. This document shows the snippets of original text (quotations) that were grouped together under a certain code. This document lists all codes, and within each code all quotations that were marked with said code.

Transparency and Accountability

Consent management

1. The Wet op de geneeskundige behandelingsovereenkomst states in Article 448(2): "In carrying out the obligation laid down in paragraph 1, the care provider is guided by what the patient should reasonably know with regard to: b. the expected consequences and risks to the health of the patient in the case of the proposed examination, the proposed treatment, the procedures to be performed and in the event of non-treatment;
2. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 15a(1): "The healthcare provider only makes the client's data available via an electronic exchange system, insofar as the healthcare provider has established that the client has given explicit permission for this."
3. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 15g: "If the client has a legal representative, the rights accruing to the client under this paragraph will be exercised by this representative, on the understanding that, contrary to Article 5, paragraph 1, of the General Data Protection Regulation Implementation Act, permission for the processing of personal data , is also required of the client who has reached the age of twelve but not yet sixteen, unless the client in question cannot be considered capable of a reasonable assessment of his interests in this matter."
4. The General Data Protection Regulation states in Article 6(1): "1. The processing is lawful only if and to the extent that at least one of the following conditions is met: a) the data subject has given consent to the processing of his personal data for one or more specific purposes;

5. The General Data Protection Regulation states in Article 7(1): "When processing is based on consent, the controller must be able to demonstrate that the data subject has given consent to the processing of his or her personal data."
6. The General Data Protection Regulation states in Article 7(3): "The data subject has the right to withdraw his consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Before the data subject gives his consent, he will be informed of this. Withdrawing consent is as easy as giving it."
7. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), that the data subject has the right to withdraw consent at any time, without prejudice to the lawfulness of processing based on consent before its withdrawal;
8. The General Data Protection Regulation states in Article 17: "1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall be obliged to erase personal data without undue delay where one of the following applies: (b) the data subject withdraws consent on which the processing is based in accordance with point (a) of Article 6(1) or point (a) of Article 9(2), and there is no other legal basis for the processing;
9. The General Data Protection Regulation states in Article 18: "2. Where processing is restricted pursuant to paragraph 1, personal data, with the exception of storage, shall only be processed with the consent of the data subject or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest for the Union or for a Member State.
10. The Medical Devices states in Article 63(1): "Informed consent shall be written, dated and signed by the person performing the interview referred to in point (c) of paragraph 2, and by the subject or, where the subject is not able to give informed consent, his or her legally designated representative after having been duly informed in accordance with paragraph 2. Where the subject is unable to write, consent may be given and recorded through appropriate alternative means in the presence of at least one impartial witness. In that case, the witness shall sign and date the informed consent document. The subject or, where the subject is not able to give informed consent, his or her legally designated representative shall be provided with a copy of the document or the record, as appropriate, by which informed consent has been given. The informed consent shall be documented. Adequate time shall be given for the subject or his or her legally designated representative to consider his or her decision to participate in the clinical investigation."
11. The Medical Devices states in Article 64(1): "In the case of incapacitated subjects who have not given, or have not refused to give, informed consent before the onset of their incapacity, a clinical investigation may be conducted only where, in addition to the conditions set out in Article 62(4), all of the following conditions are met: (d) no incentives or financial inducements are given to subjects or their legally designated representatives, except for compensation for expenses and loss of earnings directly related to the participation in the clinical investigation;
12. The Medical Devices states in Article 64(1): "In the case of incapacitated subjects who have not given, or have not refused to give, informed consent before the onset of their incapacity, a clinical investigation may be conducted only where, in addition to the conditions set out in Article 62(4), all of the following conditions are met: (e) the clinical investigation is essential with respect to

incapacitated subjects and data of comparable validity cannot be obtained in clinical investigations on persons able to give informed consent, or by other research methods;

13. The Medical Devices states in Article 65(1): "A clinical investigation on minors may be conducted only where, in addition to the conditions set out in Article 62(4), all of the following conditions are met: (i) if during a clinical investigation the minor reaches the age of legal competence to give informed consent as defined in national law, his or her express informed consent shall be obtained before that subject can continue to participate in the clinical investigation."
14. The Wet op de geneeskundige behandelingsovereenkomst states in Article 448(2): "In carrying out the obligation laid down in paragraph 1, the care provider is guided by what the patient should reasonably know with regard to: a. the nature and purpose of the intended examination, the proposed treatment or the procedures to be performed;
15. The Medical Devices states in Article 65(1): "A clinical investigation on minors may be conducted only where, in addition to the conditions set out in Article 62(4), all of the following conditions are met: (a) the informed consent of their legally designated representative has been obtained;
16. ISO 27701 states in Article 7.2.3 Vaststellen wanneer en hoe toestemming moet worden verkregen: "The organization should establish and document a process by which it can demonstrate whether, when and how consent to process PII has been obtained from PII subjects."
17. ISO 27701 states in Article 7.2.4 Toestemming verkrijgen en registreren: "The organization should obtain and record consent from PII subjects in accordance with documented processes."
18. ISO 27701 states in Article 7.3.4 In een mechanisme voorzien om toestemming aan te passen of in te trekken: "The organization should provide a mechanism for PII subjects to modify or withdraw their consent."
19. NEN 7510-2 states in Article 18.1.4 Privacy and protection of personal data: "Organizations that process personal health information should manage the informed consent of clients."

Accountability record

20. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and any joint controllers, and, where applicable, of the controller's representative and the data protection officer;
21. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: d) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;
22. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: f) if possible, the envisaged periods within which the different categories of data must be erased;
23. The General Data Protection Regulation states in Article 30: "2. The processor and, where applicable, the processor's representative, shall keep records of all categories of processing activities they have carried out on behalf of a controller. This register contains the following information:
24. The General Data Protection Regulation states in Article 30: "2. The processor and, where applicable, the processor's representative, shall keep records of all categories of processing

activities they have carried out on behalf of a controller. This register contains the following information: (a) the name and contact details of the processors and of each controller on behalf of which the processor is acting, and, where applicable, of the representative of the controller or processor and of the data protection officer;

25. The General Data Protection Regulation states in Article 30: "2. The processor and, where applicable, the processor's representative, shall keep records of all categories of processing activities they have carried out on behalf of a controller. This register contains the following information: (c) where applicable, transfers of personal data to a third country or an international organisation, specifying that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documents concerning the appropriate safeguards;
26. The General Data Protection Regulation states in Article 30: "3. The register referred to in paragraphs 1 and 2 shall be in written form, including in electronic form.
27. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (e) keep identifiable logs of access to the secure processing environment for the period of time necessary to verify and audit all processing operations in that environment;
28. The AI Act states in Article 12(1): "High-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events (‘logs’) while the high-risk AI systems is operating. Those logging capabilities shall conform to recognised standards or common specifications."
29. The AI Act states in Article 12(3): "In particular, logging capabilities shall enable the monitoring of the operation of the high-risk AI system with respect to the occurrence of situations that may result in the AI system presenting a risk within the meaning of Article 65(1) or lead to a substantial modification, and facilitate the post-market monitoring referred to in Article 61."
30. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 15e: "Without prejudice to the provisions of Article 15 of the General Data Protection Regulation, a copy as referred to in Article 15d, first paragraph, shall include at the request of the client: b. who has viewed or requested certain information and on what date.""
31. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 15e: "Without prejudice to the provisions of Article 15 of the General Data Protection Regulation, a copy as referred to in Article 15d, first paragraph, shall include at the request of the client: a. who has made certain information available via the electronic exchange system and on what date;
32. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documents regarding the appropriate safeguards;
33. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: c) a description of the categories of data subjects and of the categories of personal data;

34. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: b) the processing purposes;

Accountability

35. The General Data Protection Regulation states in Article 5(2): "The controller is responsible for and can demonstrate compliance with paragraph 1 (“accountability”)."
36. The General Data Protection Regulation states in Article 7(1): "When processing is based on consent, the controller must be able to demonstrate that the data subject has given consent to the processing of his or her personal data."
37. The General Data Protection Regulation states in Article 12(2): "The controller shall facilitate the exercise of the data subject's rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to comply with the data subject's request for his rights under Articles 15 to 22, unless the controller demonstrates that it is unable to identify the data subject."
38. The General Data Protection Regulation states in Article 21: "1. The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to processing of personal data concerning him/her which is based on point (e) or (f) of Article 6(1), including profiling on the basis of those provisions. The controller shall cease processing the personal data unless he can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims .
39. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and any joint controllers, and, where applicable, of the controller's representative and the data protection officer;
40. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: d) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;
41. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: f) if possible, the envisaged periods within which the different categories of data must be erased;
42. The General Data Protection Regulation states in Article 30: "2. The processor and, where applicable, the processor's representative, shall keep records of all categories of processing activities they have carried out on behalf of a controller. This register contains the following information:
43. The General Data Protection Regulation states in Article 30: "2. The processor and, where applicable, the processor's representative, shall keep records of all categories of processing activities they have carried out on behalf of a controller. This register contains the following information: (a) the name and contact details of the processors and of each controller on behalf of which the processor is acting, and, where applicable, of the representative of the controller or processor and of the data protection officer;

44. The General Data Protection Regulation states in Article 30: "2. The processor and, where applicable, the processor's representative, shall keep records of all categories of processing activities they have carried out on behalf of a controller. This register contains the following information: (c) where applicable, transfers of personal data to a third country or an international organisation, specifying that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documents concerning the appropriate safeguards;
45. The General Data Protection Regulation states in Article 30: "3. The register referred to in paragraphs 1 and 2 shall be in written form, including in electronic form.
46. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (e) keep identifiable logs of access to the secure processing environment for the period of time necessary to verify and audit all processing operations in that environment;
47. The Medical Devices states in Article 63(1): "Informed consent shall be written, dated and signed by the person performing the interview referred to in point (c) of paragraph 2, and by the subject or, where the subject is not able to give informed consent, his or her legally designated representative after having been duly informed in accordance with paragraph 2. Where the subject is unable to write, consent may be given and recorded through appropriate alternative means in the presence of at least one impartial witness. In that case, the witness shall sign and date the informed consent document. The subject or, where the subject is not able to give informed consent, his or her legally designated representative shall be provided with a copy of the document or the record, as appropriate, by which informed consent has been given. The informed consent shall be documented. Adequate time shall be given for the subject or his or her legally designated representative to consider his or her decision to participate in the clinical investigation."
48. The AI Act states in Article 12(1): "High-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events (‘logs’) while the high-risk AI systems is operating. Those logging capabilities shall conform to recognised standards or common specifications."
49. The AI Act states in Article 12(3): "In particular, logging capabilities shall enable the monitoring of the operation of the high-risk AI system with respect to the occurrence of situations that may result in the AI system presenting a risk within the meaning of Article 65(1) or lead to a substantial modification, and facilitate the post-market monitoring referred to in Article 61."
50. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 15e: "Without prejudice to the provisions of Article 15 of the General Data Protection Regulation, a copy as referred to in Article 15d, first paragraph, shall include at the request of the client: b. who has viewed or requested certain information and on what date.""
51. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 15e: "Without prejudice to the provisions of Article 15 of the General Data Protection Regulation, a copy as referred to in Article 15d, first paragraph, shall include at the request of the client: a. who has made certain information available via the electronic exchange system and on what date;
52. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: (e) where applicable, transfers of personal data to a third country or an international organisation,

including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documents regarding the appropriate safeguards;

53. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: c) a description of the categories of data subjects and of the categories of personal data;
54. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: b) the processing purposes;
55. ISO 27701 states in Article 6.10.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst: "The organization should ensure that persons acting under its authority who have access to PII are bound by a duty of confidentiality."
56. ISO 27701 states in Article 7.2.1 Doeleinde identificeren en documenteren: ""The organization should identify and document the specific purposes for which the PII is processed.
57. ISO 27701 states in Article 7.2.2 Rechtsgrond identificeren: "The organization should establish, document and comply with the relevant legal basis for processing PII for the identified purposes."
58. ISO 27701 states in Article 7.2.3 Vaststellen wanneer en hoe toestemming moet worden verkregen: "The organization should establish and document a process by which it can demonstrate whether, when and how consent to process PII has been obtained from PII subjects."
59. ISO 27701 states in Article 7.2.4 Toestemming verkrijgen en registreren: "The organization should obtain and record consent from PII subjects in accordance with documented processes."
60. ISO 27701 states in Article 7.4.3 Juistheid en kwaliteit: "The organization should ensure and document that PII throughout its lifecycle is as accurate, complete and current as necessary for the purposes for which the PII is processed."

Data minimization

61. The General Data Protection Regulation states in Article 5(1): ""1. Personal data must: (c) are adequate, relevant and limited to what is necessary for the purposes for which they are processed (‘data minimisation’);
62. The General Data Protection Regulation states in Article 17: "1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall be obliged to erase personal data without undue delay where one of the following applies: a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
63. The General Data Protection Regulation states in Article 25: "1. Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of risks to the rights and freedoms of natural persons subject to the processing, the controller shall implement, both in determining the means of processing and in the processing itself, appropriate technical and organizational measures, such as pseudonymization, designed with the aim of effectively implementing data protection principles, such as data minimization and to include necessary safeguards in the processing to comply with the requirements of this Regulation and to protect the rights of the data subjects.

64. The General Data Protection Regulation states in Article 25: "2. The controller takes appropriate technical and organizational measures to ensure that, in principle, only personal data is processed that is necessary for each specific purpose of the processing. This obligation applies to the amount of personal data collected, the extent to which it is processed, the period for which it is stored and its accessibility. In particular, these measures ensure that personal data are, in principle, not made accessible to an unlimited number of natural persons without human intervention.
65. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: f) if possible, the envisaged periods within which the different categories of data must be erased;
66. The European Health Data Space states in Article 4(2): "In line with the data minimisation principle provided for in Regulation (EU) 2016/679, Member States may establish rules providing for the categories of personal electronic health data required by different health professions. Such rules shall not be based on the source of electronic health data."
67. The European Health Data Space states in Article 44(2): "The health data access bodies shall provide the electronic health data in an anonymised format, where the purpose of processing by the data user can be achieved with such data, taking into account the information provided by the data user."
68. The Data Act states in Article 6(1): "A third party shall process the data made available to it pursuant to Article 5 only for the purposes and under the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned, and shall delete the data when they are no longer necessary for the agreed purpose."
69. ISO 27701 states in Article 7.4.1 Het verzamelen beperken: "The organization should limit the collection of PII to the minimum that is relevant, proportionate and necessary for the purposes identified."

Communication

70. The Wet op de geneeskundige behandelingsovereenkomst states in Article 448(1): "The care provider informs the patient in a clear manner that is appropriate to his or her comprehension, and consults with the patient in a timely manner about the intended examination and the proposed treatment and about the developments regarding the examination, the treatment and the patient's state of health. The care provider shall inform a patient who has not yet reached the age of twelve in such a way as is appropriate to his comprehension."
71. The Wet op de geneeskundige behandelingsovereenkomst states in Article 448(2): "In carrying out the obligation laid down in paragraph 1, the care provider is guided by what the patient should reasonably know with regard to: b. the expected consequences and risks to the health of the patient in the case of the proposed examination, the proposed treatment, the procedures to be performed and in the event of non-treatment;
72. The General Data Protection Regulation states in Article 12(1): "The controller shall take appropriate measures to ensure that the data subject receives the information referred to in Articles 13 and 14 and the communication referred to in Articles 15 to 22 and 34 in relation to the processing in a concise, transparent, intelligible and easily accessible form and in receives clear and plain language, especially when the information is specifically addressed to a child. The information shall be provided in writing or by other means, including, where appropriate, electronic means. If requested by the data subject, the information may be communicated orally, provided that the identity of the data subject is proven by other means."

73. The General Data Protection Regulation states in Article 14: "3. The controller shall provide the information referred to in paragraphs 1 and 2: b) if the personal data will be used for communication with the data subject, at the latest at the time of the first contact with the data subject; or
74. The Medical Devices states in Article 65(1): "A clinical investigation on minors may be conducted only where, in addition to the conditions set out in Article 62(4), all of the following conditions are met: (b) the minors have received the information referred to in Article 63(2) in a way adapted to their age and mental maturity and from investigators or members of the investigating team who are trained or experienced in working with children;
75. The Wet op de geneeskundige behandelingsovereenkomst states in Article 448(2): "In carrying out the obligation laid down in paragraph 1, the care provider is guided by what the patient should reasonably know with regard to: a. the nature and purpose of the intended examination, the proposed treatment or the procedures to be performed;

AI Monitoring

76. The AI Act states in Article 12(3): "In particular, logging capabilities shall enable the monitoring of the operation of the high-risk AI system with respect to the occurrence of situations that may result in the AI system presenting a risk within the meaning of Article 65(1) or lead to a substantial modification, and facilitate the post-market monitoring referred to in Article 61."
77. The AI Act states in Article 14(4): "The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (a)fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible;
78. The AI Act states in Article 20(1): "Providers of high-risk AI systems shall keep the logs automatically generated by their high-risk AI systems, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law. The logs shall be kept for a period that is appropriate in the light of the intended purpose of high-risk AI system and applicable legal obligations under Union or national law."
79. The AI Act states in Article 9(2): "The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise the following steps: (c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;
80. The AI Act states in Article 29(4): "Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor when they have identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis."

Oversight

81. The AI Act states in Article 14(1): "High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use."

82. The AI Act states in Article 14(4): "The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (a)fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible;
83. The AI Act states in Article 14(4): "The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (b)remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;
84. The AI Act states in Article 14(4): "The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (c)be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available;

Transparency

85. The General Data Protection Regulation states in Article 5(1): ""1. Personal data must: (a) processed in a manner that is lawful, fair and transparent in relation to the data subject ('lawfulness, fairness and transparency');
86. The General Data Protection Regulation states in Article 12(1): "The controller shall take appropriate measures to ensure that the data subject receives the information referred to in Articles 13 and 14 and the communication referred to in Articles 15 to 22 and 34 in relation to the processing in a concise, transparent, intelligible and easily accessible form and in receives clear and plain language, especially when the information is specifically addressed to a child. The information shall be provided in writing or by other means, including, where appropriate, electronic means. If requested by the data subject, the information may be communicated orally, provided that the identity of the data subject is proven by other means."
87. The AI Act states in Article 13(1): "High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider set out in Chapter 3 of this Title."

Auditability

88. The Wet elektronische gegevensuitwisseling zorg states in Article 4.1(3): "The officials referred to in the first paragraph are, insofar as this is necessary for the performance of their duties, authorized to inspect data, including health data, to make copies thereof and if this cannot be done on site, the data for that purpose for a short period of time against written evidence to be issued by them, and to demand information in this regard from the relevant care provider or care provider."
89. The General Data Protection Regulation states in Article 30: "4. Upon request, the controller or processor and, where applicable, the representative of the controller or processor shall make the register available to the supervisory authority.
90. The Data Act states in Article 30(1): "The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of

smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements: (c) data archiving and continuity: foresee, if a smart contract must be terminated or deactivated, a possibility to archive transactional data, the smart contract logic and code to keep the record of the operations performed on the data in the past (auditability); and

Proportionality

91. The Wet op de geneeskundige behandelingsovereenkomst states in Article 458(1): "Contrary to the provisions of Article 457, paragraph 1, information about the patient or access to the data from the file may be provided to another person on request without the patient's consent for the purpose of statistics or scientific research in the field of public health, if: a) requesting permission is not reasonably possible and with regard to the conduct of the research such guarantees have been provided that the privacy of the patient is not disproportionately harmed, or
92. ISO 27701 states in Article 7.4.1 Het verzamelen beperken: "The organization should limit the collection of PII to the minimum that is relevant, proportionate and necessary for the purposes identified."

Rights and Interests of Data Subject

Information to be provided

93. The Wet op de geneeskundige behandelingsovereenkomst states in Article 448(1): "The care provider informs the patient in a clear manner that is appropriate to his or her comprehension, and consults with the patient in a timely manner about the intended examination and the proposed treatment and about the developments regarding the examination, the treatment and the patient's state of health. The care provider shall inform a patient who has not yet reached the age of twelve in such a way as is appropriate to his comprehension."
94. The General Data Protection Regulation states in Article 12(3): "The controller shall provide the data subject without undue delay and in any event within one month of receipt of the request pursuant to Articles 15 to 22 with information on the action taken on the request. Depending on the complexity of the requests and the number of requests, that period may be extended by a further two months if necessary. The controller shall inform the data subject of such an extension within one month of receipt of the request, stating the reasons for the delay. Where the data subject submits his request electronically, the information shall be provided electronically if possible, unless the data subject requests otherwise."
95. The General Data Protection Regulation states in Article 13: "1. Where personal data relating to a data subject are collected from that person, the controller shall provide the data subject with the following information at the time of obtaining the personal data: a) the identity and contact details of the controller and, where applicable, of the controller's representative;
96. The General Data Protection Regulation states in Article 13: "1. Where personal data relating to a data subject are collected from that person, the controller shall provide the data subject with the following information at the time of obtaining the personal data: c) the processing purposes for which the personal data are intended, as well as the legal basis for the processing;
97. The General Data Protection Regulation states in Article 13: "1. Where personal data relating to a data subject are collected from that person, the controller shall provide the data subject with the following information at the time of obtaining the personal data: d) the legitimate interests of the controller or of a third party, where the processing is based on point (f) of Article 6(1);

98. The General Data Protection Regulation states in Article 13: "1. Where personal data relating to a data subject are collected from that person, the controller shall provide the data subject with the following information at the time of obtaining the personal data: f) where applicable, that the controller intends to transfer the personal data to a third country or an international organisation; whether or not there is an adequacy decision by the Commission; or, in the case of transfers referred to in Article 46, Article 47 or the second subparagraph of Article 49(1), which are the appropriate or suitable safeguards, how a copy of them can be obtained or where they can be consulted."
99. The General Data Protection Regulation states in Article 14: ""1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: a) the identity and contact details of the controller and, where applicable, of the controller's representative;
100. The General Data Protection Regulation states in Article 14: ""1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: c) the processing purposes for which the personal data are intended and the legal basis for the processing;
101. The General Data Protection Regulation states in Article 14: ""1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: f) where applicable, that the controller intends to transfer the personal data to a recipient in a third country or to an international organisation; whether or not there is an adequacy decision by the Commission; or, in the case of transfers referred to in Article 46, Article 47 or the second subparagraph of Article 49(1), what are the appropriate or suitable safeguards, how a copy of them can be obtained or where they can be consulted.
102. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: a) the period for which the personal data will be stored, or if that is not possible, the criteria for determining that period;
103. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: b) the legitimate interests of the controller or of a third party, where the processing is based on point (f) of Article 6(1);
104. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), that the data subject has the right to withdraw consent at any time, without prejudice to the lawfulness of processing based on consent before its withdrawal;
105. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: f) the source from which the personal data originate and, where applicable, whether they come from publicly available sources;
106. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data

subject: (g) the existence of automated decision-making, including profiling referred to in Article 22(1) and (4), and, at least in those cases, useful information about the underlying logic, as well as the importance and expected consequences of that processing for the data subject.

107. The General Data Protection Regulation states in Article 14: "3. The controller shall provide the information referred to in paragraphs 1 and 2: b) if the personal data will be used for communication with the data subject, at the latest at the time of the first contact with the data subject; or

108. The General Data Protection Regulation states in Article 14: "3. The controller shall provide the information referred to in paragraphs 1 and 2: c) if provision of the data to another recipient is envisaged, at the latest at the time when the personal data are first disclosed.

109. The General Data Protection Regulation states in Article 14: "5. Paragraphs 1 to 4 shall not apply if and insofar as: (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions referred to in Article 89(1) and safeguards, or insofar as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the purposes of such processing. In such cases, the controller shall take appropriate measures to protect the data subject's rights, freedoms and legitimate interests, including making the information public;

110. The General Data Protection Regulation states in Article 15: ""1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, to obtain access to those personal data and to the following information: d) if possible, the period for which the personal data are expected to be stored, or if that is not possible, the criteria for determining that period;

111. The General Data Protection Regulation states in Article 19: "The controller shall inform each recipient to whom personal data have been disclosed of any rectification or erasure of personal data or restriction of processing pursuant to Article 16, Article 17(1) and Article 18, unless this proves impossible or involves a disproportionate effort. The controller shall provide the data subject with information about these recipients if the data subject requests it."

112. The Data Act states in Article 3(2): "Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (a) the nature and volume of the data likely to be generated by the use of the product or related service;

113. The Data Act states in Article 3(2): "Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (d) whether the manufacturer supplying the product or the service provider providing the related service intends to use the data itself or allow a third party to use the data and, if so, the purposes for which those data will be used;

114. The Data Act states in Article 3(2): "Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (e) whether the seller, renter or lessor is the data holder and, if not, the identity of the data holder, such as its trading name and the geographical address at which it is established;

115. The Data Act states in Article 3(2): "Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (b) whether the data is likely to be generated continuously and in real-time;

116. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 15e: "Without prejudice to the provisions of Article 15 of the General Data Protection Regulation, a copy as referred to in Article 15d, first paragraph, shall include at the request of the client: b. who has viewed or requested certain information and on what date.""
117. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 15e: "Without prejudice to the provisions of Article 15 of the General Data Protection Regulation, a copy as referred to in Article 15d, first paragraph, shall include at the request of the client: a. who has made certain information available via the electronic exchange system and on what date;
118. The Data Act states in Article 3(2): "Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (c) how the user may access those data;
119. The Data Act states in Article 3(2): "Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (f) the means of communication which enable the user to contact the data holder quickly and communicate with that data holder efficiently;
120. The Data Act states in Article 3(2): "Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (g) how the user may request that the data are shared with a third-party;
121. ISO 27701 states in Article 6.7.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen: "The organization should inform the customer of the circumstances in which it uses cryptography to protect the PII it processes."
122. The organization should ensure that PII data subjects understand the purpose for which their PII is being processed.""

Purpose Limitation

123. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 15f(1): "A health insurer does not have access to electronic exchange systems."
124. The General Data Protection Regulation states in Article 5(1): ""1. Personal data must: (b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the original purposes in accordance with Article 89(1) (‘purpose limitation’);
125. The General Data Protection Regulation states in Article 25: "2. The controller takes appropriate technical and organizational measures to ensure that, in principle, only personal data is processed that is necessary for each specific purpose of the processing. This obligation applies to the amount of personal data collected, the extent to which it is processed, the period for which it is stored and its accessibility. In particular, these measures ensure that personal data are, in principle, not made accessible to an unlimited number of natural persons without human intervention.
126. The European Health Data Space states in Article 46(7): "Data users shall have the right to access and process the electronic health data in accordance with the data permit delivered to them on the basis of this Regulation."
127. The Data Act states in Article 6(1): "A third party shall process the data made available to it pursuant to Article 5 only for the purposes and under the conditions agreed with the user, and

subject to the rights of the data subject insofar as personal data are concerned, and shall delete the data when they are no longer necessary for the agreed purpose."

128. The Data Act states in Article 6(2): "The third party shall not: (c) make the data available it receives to another third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user;

129. The Data Act states in Article 6(2): "The third party shall not: (d) make the data available it receives to an undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper pursuant to Article [...] of [Regulation on contestable and fair markets in the digital sector (Digital Markets Act)];

130. (e) use the data it receives to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose;

131. ISO 27701 states in Article 6.11.3.1 Bescherming van testgegevens: "PII should not be used for testing purposes; fake or artificial PII should then be used."

132. ISO 27701 states in Article 7.2.1 Doeleinde identificeren en documenteren: ""The organization should identify and document the specific purposes for which the PII is processed.

133. ISO 27701 states in Article 7.4.2 Het verwerken beperken: "The organization should limit the processing of PII to what is adequate, relevant and necessary for the identified purposes."

134. NEN 7512 states in Article 6.1.11 Geldigheid gebruikte kader : "A [kader] (exchange agreement, connection conditions, etc.) has in principle a limited lifespan and a targeted scope."

Right to data access

135. The Wet op de geneeskundige behandelingsovereenkomst states in Article 456: "On request, the care provider will provide the patient with access to and copies of the data from the file. The provision does not take place insofar as this is necessary in the interest of protecting the privacy of another person."

136. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 15d(1): "If the client requests access to or copy of the file of the relevant client, or of the data relating to this client that the healthcare provider makes available via an electronic exchange system, the inspection or copy will be made available at the request of the client, at reasonable intervals, by provided electronically by the healthcare provider."

137. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: c) that the data subject has the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning him, as well as the right to object to processing and the right to data portability;

138. The General Data Protection Regulation states in Article 15: "3. The controller shall provide the data subject with a copy of the personal data being processed. If the data subject requests additional copies, the controller may charge a reasonable fee based on administrative costs. Where the data subject submits his request electronically, and does not request any other arrangement, the information shall be provided in a commonly used electronic format.

139. The General Data Protection Regulation states in Article 20: "1. The data subject shall have the right to obtain personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and shall have the right to transmit those data to another controller, without having to are hindered by the controller to whom the personal data was disclosed, if: (a) the processing is based on consent pursuant to

point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and b) the processing is carried out by automated means.

140. The European Health Data Space states in Article 3(1): "Natural persons shall have the right to access their personal electronic health data processed in the context of primary use of electronic health data, immediately, free of charge and in an easily readable, consolidated and accessible form."

141. The Data Act states in Article 3(1): "Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user."

142. The Data Act states in Article 4(1): "Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible

143. ISO 27701 states in Article 7.3.8 Een kopie verstrekken van verwerkte PII: "The organization should be able to provide a copy of the processed PII upon request by the PII subject."

Right to be informed

144. The General Data Protection Regulation states in Article 13: "1. Where personal data relating to a data subject are collected from that person, the controller shall provide the data subject with the following information at the time of obtaining the personal data: f) where applicable, that the controller intends to transfer the personal data to a third country or an international organisation; whether or not there is an adequacy decision by the Commission; or, in the case of transfers referred to in Article 46, Article 47 or the second subparagraph of Article 49(1), which are the appropriate or suitable safeguards, how a copy of them can be obtained or where they can be consulted."

145. The General Data Protection Regulation states in Article 14: "4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data was obtained, the controller shall provide the data subject with information about that other purpose and any relevant further information referred to in paragraph 2 before such further processing.

146. The General Data Protection Regulation states in Article 15: ""1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, to obtain access to those personal data and to the following information: c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

147. The General Data Protection Regulation states in Article 15: "1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, to obtain access to those personal data and to the following information: (h) the existence of automated decision-making, including profiling referred to in Article 22(1) and (4), and, at least in those cases, useful information about the underlying logic, as well as the importance and expected consequences of that processing for the data subject.

148. The General Data Protection Regulation states in Article 15: "2. When personal data are transferred to a third country or an international organisation, the data subject shall have the right to be informed of the appropriate safeguards in accordance with Article 46 on the transfer.

149. The General Data Protection Regulation states in Article 18: "3. A data subject who has obtained restriction of processing in accordance with paragraph 1 shall be informed by the controller before the restriction of processing is lifted."
150. The European Health Data Space states in Article 3(10): "Natural persons shall have the right to obtain information on the healthcare providers and health professionals that have accessed their electronic health data in the context of healthcare. The information shall be provided immediately and free of charge through electronic health data access services. "
151. The AI Act states in Article 9(4): “The risk management measures referred to in paragraph 2, point (d) shall be such that any residual risk associated with each hazard as well as the overall residual risk of the high-risk AI systems is judged acceptable, provided that the high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. Those residual risks shall be communicated to the user.
152. ISO 27701 states in Article 6.13.1.1 Verantwoordelijkheden en procedures: "As part of the overall information security incident management process, the organization should establish responsibilities and procedures for identifying and recording PII-related breaches. In addition, the organization should establish responsibilities and procedures regarding notification to parties, where required, of PII-related breaches (including the timing of such notifications) and disclosure to authorities, account taking into account the applicable laws and/or regulations."

Erasure of data

153. The Wet op de geneeskundige behandelingsovereenkomst states in Article 455(1): "The care provider destroys the data from the file after a written or electronic request to that effect from the patient."
154. The General Data Protection Regulation states in Article 5(1): ""1. Personal data must: d) are accurate and updated as necessary; all reasonable steps must be taken to erase or rectify without undue delay (“accuracy”) personal data which are inaccurate having regard to the purposes for which they are processed;
155. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: c) that the data subject has the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning him, as well as the right to object to processing and the right to data portability;
156. The General Data Protection Regulation states in Article 15: ""1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, to obtain access to those personal data and to the following information: e) that the data subject has the right to request from the controller that personal data be rectified or erased, or that the processing of personal data concerning him or her be restricted, as well as the right to object to such processing;
157. The General Data Protection Regulation states in Article 17: "1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall be obliged to erase personal data without undue delay where one of the following applies:
158. The General Data Protection Regulation states in Article 17: "1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall be obliged to erase personal data without undue

delay where one of the following applies: e) the personal data must be erased for compliance with a legal obligation under Union or Member State law to which the controller is subject;

159. The General Data Protection Regulation states in Article 17: "1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall be obliged to erase personal data without undue delay where one of the following applies: (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)

160. The General Data Protection Regulation states in Article 19: "The controller shall inform each recipient to whom personal data have been disclosed of any rectification or erasure of personal data or restriction of processing pursuant to Article 16, Article 17(1) and Article 18, unless this proves impossible or involves a disproportionate effort. The controller shall provide the data subject with information about these recipients if the data subject requests it."

161. ISO 27701 states in Article 7.4.5 PII aan het einde van de verwerking niet-identificeerbaar maken en wissen: "The organization should erase or convert PII into a form that no longer allows PII subjects to be identified or re-identified once the original PII is no longer needed for the identified purpose(s)."

Data portability

162. The Wet elektronische gegevensuitwisseling zorg states in Article 1.5(2): "The requirements can relate to the realization of data portability."

163. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: c) that the data subject has the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning him, as well as the right to object to processing and the right to data portability;

164. The General Data Protection Regulation states in Article 20: "1. The data subject shall have the right to obtain personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and shall have the right to transmit those data to another controller, without having to are hindered by the controller to whom the personal data was disclosed, if: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and b) the processing is carried out by automated means.

165. The General Data Protection Regulation states in Article 20: "2. When exercising his or her right to data portability under paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

166. The European Health Data Space states in Article 3(8): "Natural persons shall have the right that, where priority categories of personal electronic health data referred to in Article 5 are transmitted or made available by the natural person according to the European electronic health record exchange format referred to in Article 6, such data shall be read and accepted by other healthcare providers."

167. The Data Act states in Article 5(1): "Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time."

168. The Data Act states in Article 6(2): "The third party shall not: (f) prevent the user, including through contractual commitments, from making the data it receives available to other parties."

Rectification of data

169. The General Data Protection Regulation states in Article 5(1): ""1. Personal data must: d) are accurate and updated as necessary; all reasonable steps must be taken to erase or rectify without undue delay (“accuracy”) personal data which are inaccurate having regard to the purposes for which they are processed;

170. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: c) that the data subject has the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning him, as well as the right to object to processing and the right to data portability;

171. The General Data Protection Regulation states in Article 15: ""1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, to obtain access to those personal data and to the following information: e) that the data subject has the right to request from the controller that personal data be rectified or erased, or that the processing of personal data concerning him or her be restricted, as well as the right to object to such processing;

172. The General Data Protection Regulation states in Article 16: "The data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by providing a supplementary statement."

173. The General Data Protection Regulation states in Article 19: "The controller shall inform each recipient to whom personal data have been disclosed of any rectification or erasure of personal data or restriction of processing pursuant to Article 16, Article 17(1) and Article 18, unless this proves impossible or involves a disproportionate effort. The controller shall provide the data subject with information about these recipients if the data subject requests it."

174. The European Health Data Space states in Article 3(7): "Member States shall ensure that, when exercising the right to rectification under Article 16 of Regulation (EU) 2016/679, natural persons can easily request rectification online through the electronic health data access services referred to in paragraph 5, point (a), of this Article. "

Right to object to processing

175. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: c) that the data subject has the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning him, as well as the right to object to processing and the right to data portability;

176. The General Data Protection Regulation states in Article 15: ""1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, to obtain access to those personal data and to the following information: e) that the data subject has the right to request from the controller that personal data be rectified or erased, or that the processing of personal data concerning him or her be restricted, as well as the right to object to such processing;

177. The General Data Protection Regulation states in Article 21: "1. The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to processing

of personal data concerning him/her which is based on point (e) or (f) of Article 6(1), including profiling on the basis of those provisions. The controller shall cease processing the personal data unless he can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims .

178. The General Data Protection Regulation states in Article 21: "2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing, including profiling related to direct marketing.

179. The General Data Protection Regulation states in Article 21: "6. Where personal data are processed for scientific or historical research purposes or for statistical purposes pursuant to Article 89(1), the data subject shall have the right, on grounds relating to his particular situation, to object to the processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out in the public interest."

180. ISO 27701 states in Article 7.3.5 In een mechanisme voorzien om bezwaar te maken tegen verwerking: "The organization should provide a mechanism for PII data subjects to object to the processing of their PII."

Information about rights

181. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 15c(1): "The healthcare provider provides the client with information about his rights with regard to electronic data exchange, the way in which he can exercise his rights and about the functioning of the electronic exchange system used for the data exchange. If new categories of healthcare providers join the electronic exchange system, or if the operation of the electronic exchange system is otherwise substantially changed, the healthcare provider will inform the client about this change, as well as about the possibility of amending or changing the permission given, as referred to in Article 15a. to pull."

182. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: c) that the data subject has the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning him, as well as the right to object to processing and the right to data portability;

183. The General Data Protection Regulation states in Article 15: ""1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, to obtain access to those personal data and to the following information: e) that the data subject has the right to request from the controller that personal data be rectified or erased, or that the processing of personal data concerning him or her be restricted, as well as the right to object to such processing;

184. The General Data Protection Regulation states in Article 17: "1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall be obliged to erase personal data without undue delay where one of the following applies: (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)

185. The General Data Protection Regulation states in Article 21: "4. The right referred to in paragraphs 1 and 2 shall be expressly brought to the attention of the data subject at the latest at

the time of the first contact with the data subject and shall be presented clearly and separately from any other information.

186. The Data Act states in Article 3(2): "Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (h) the user's right to lodge a complaint alleging a violation of the provisions of this Chapter with the competent authority referred to in Article 31."

Rights and interests of others

187. The Wet op de geneeskundige behandelingsovereenkomst states in Article 455(2): "Paragraph 1 does not apply insofar as the request concerns data of which it is reasonably likely that the retention is of considerable importance to someone other than the patient, and insofar as the provisions laid down by or pursuant to the law preclude destruction."

188. The Wet op de geneeskundige behandelingsovereenkomst states in Article 456: "On request, the care provider will provide the patient with access to and copies of the data from the file. The provision does not take place insofar as this is necessary in the interest of protecting the privacy of another person."

189. The Wet op de geneeskundige behandelingsovereenkomst states in Article 457(1): "Without prejudice to the provisions of Article 448 paragraph 4, second sentence, the care provider shall ensure that no information about the patient or access to or copies of the data from the file is provided to anyone other than the patient without the patient's consent. If provision takes place, this will only take place insofar as this does not harm another person's privacy. The provision may take place without observing the restrictions referred to in the previous sentences, if required by or pursuant to the law."

190. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 15a(3): "The healthcare provider only makes the client's data available via an electronic exchange system, insofar as the consultation of that data by another healthcare provider does not harm the privacy of anyone other than the client."

191. The General Data Protection Regulation states in Article 6(1): "1. The processing is lawful only if and to the extent that at least one of the following conditions is met: d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

192. The European Health Data Space states in Article 4(4): "Where access to electronic health data has been restricted by the natural person, the healthcare provider or health professionals shall not be informed of the content of the electronic health data without prior authorisation by the natural person, including where the provider or professional is informed of the existence and nature of the restricted electronic health data. In cases where processing is necessary in order to protect the vital interests of the data subject or of another natural person, the healthcare provider or health professional may get access to the restricted electronic health data. Following such access, the healthcare provider or health professional shall inform the data holder and the natural person concerned or his/her guardians that access to electronic health data had been granted. Member States' law may add additional safeguards."

Restriction of processing

193. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: c) that the data subject has the right to request from the controller access to and

rectification or erasure of personal data or restriction of processing concerning him, as well as the right to object to processing and the right to data portability;

194. The General Data Protection Regulation states in Article 15: ""1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, to obtain access to those personal data and to the following information: e) that the data subject has the right to request from the controller that personal data be rectified or erased, or that the processing of personal data concerning him or her be restricted, as well as the right to object to such processing;

195. The General Data Protection Regulation states in Article 18: "1. The data subject shall have the right to obtain from the controller the restriction of processing where one of the following applies: a) the accuracy of the personal data is contested by the data subject, for a period that enables the controller to verify the accuracy of the personal data;

196. The General Data Protection Regulation states in Article 18: "1. The data subject shall have the right to obtain from the controller the restriction of processing where one of the following applies: c) the controller no longer needs the personal data for the processing purposes, but the data subject needs them for the establishment, exercise or defense of legal claims;

197. The General Data Protection Regulation states in Article 18: "3. A data subject who has obtained restriction of processing in accordance with paragraph 1 shall be informed by the controller before the restriction of processing is lifted."

Storage Limitation

198. The General Data Protection Regulation states in Article 5(1): ""1. Personal data must: e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data are processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), provided that the appropriate technical and organizational measures required by this Regulation are implemented. taken to protect the rights and freedoms of the data subject ("storage limitation");

199. ISO 27701 states in Article 7.4.7 Bewaring: "The organization should not retain PII for longer than is necessary for the purposes for which the PII is processed."

200. NEN 7512 states in Article 6.1.11 Geldigheid gebruikte kader : "A [kader] (exchange agreement, connection conditions, etc.) has in principle a limited lifespan and a targeted scope."

201. NEN 7512 states in Article 6.3.3 Bewaren, archiveren en vernietigen : "After the termination of the timeframe, relevant data must be retained, archived or deleted by the communication parties, taking into account the legal provisions."

Right to share data

202. The European Health Data Space states in Article 3(8): "Natural persons shall have the right to give access to or request a data holder from the health or social security sector to transmit their electronic health data to a data recipient of their choice from the health or social security sector, immediately, free of charge and without hindrance from the data holder or from the manufacturers of the systems used by that holder.

203. The Data Act states in Article 11(1): "The data holder may apply appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and to ensure compliance with Articles 5, 6, 9 and 10, as well as with the agreed contractual terms for making data available. Such technical protection measures shall not be used as a means to hinder

the user's right to effectively provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation implementing Union law as referred to in Article 8(1)."

204. The Data Act states in Article 3(2): "Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (g) how the user may request that the data are shared with a third-party;

Rights of minors

205. The Wet op de geneeskundige behandelingsovereenkomst states in Article 465(1): "If the patient has not yet reached the age of twelve, the obligations arising for the care provider from this department towards the patient are fulfilled by the care provider towards the parents who exercise authority over the patient or towards his guardian."

206. The General Data Protection Regulation states in Article 6(1): "1. The processing is lawful only if and to the extent that at least one of the following conditions is met: f) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where the interests or fundamental rights and freedoms of the data subject which require the protection of personal data outweigh those interests, in particular when the person concerned is a child.

207. The Medical Devices states in Article 65(1): "A clinical investigation on minors may be conducted only where, in addition to the conditions set out in Article 62(4), all of the following conditions are met: (b) the minors have received the information referred to in Article 63(2) in a way adapted to their age and mental maturity and from investigators or members of the investigating team who are trained or experienced in working with children;

Right to restrict access

208. The European Health Data Space states in Article 3(9): "Notwithstanding Article 6(1), point (d), of Regulation (EU) 2016/679, natural persons shall have the right to restrict access of health professionals to all or part of their electronic health data. Member States shall establish the rules and specific safeguards regarding such restriction mechanisms. "

209. The European Health Data Space states in Article 4(4): "Where access to electronic health data has been restricted by the natural person, the healthcare provider or health professionals shall not be informed of the content of the electronic health data without prior authorisation by the natural person, including where the provider or professional is informed of the existence and nature of the restricted electronic health data. In cases where processing is necessary in order to protect the vital interests of the data subject or of another natural person, the healthcare provider or health professional may get access to the restricted electronic health data. Following such access, the healthcare provider or health professional shall inform the data holder and the natural person concerned or his/her guardians that access to electronic health data had been granted. Member States' law may add additional safeguards."

Data Management and Quality

Identification

210. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 4: "A healthcare provider uses a client's citizen service number with the aim of guaranteeing that

the personal data to be processed in the context of the provision of healthcare relate to that client."

211. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 5: "The healthcare provider determines the identity and citizen service number of a client: a. when the client turns to the care provider for the first time to obtain care; b. insofar as this is reasonably necessary for the implementation of Article 12 of the Citizen Service Number (General Provisions) Act.""

212. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 6(1): "The healthcare provider establishes the identity of the client on the basis of a document as referred to in Article 1 of the Compulsory Identification Act, which the client provides for inspection on request."

213. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 8: "The healthcare provider includes the citizen service number of the client in its administration when recording personal data with regard to the provision of healthcare."

214. The Data Act states in Article 3(2): "Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (e) whether the seller, renter or lessor is the data holder and, if not, the identity of the data holder, such as its trading name and the geographical address at which it is established;

215. ISO 27701 states in Article 7.4.5 PII aan het einde van de verwerking niet-identificeerbaar maken en wissen: "The organization should erase or convert PII into a form that no longer allows PII subjects to be identified or re-identified once the original PII is no longer needed for the identified purpose(s)."

216. NEN 7510-2 states in Article 14.1.1.2 Validation of output data: "Health information systems that process personal health information should provide personal identification information that helps healthcare providers confirm that the requested electronic health record corresponds to the client being treated."

217. NEN 7510-2 states in Article 14.1.1.1 Uniquely identify care recipients: "Health information systems that process personal health information should: a) ensure that each client can be uniquely identified within the system; b) …"

Data format

218. The European Health Data Space states in Article 45(2): "The data access application shall include: (b) a description of the requested electronic health data, their format and data sources, where possible, including geographical coverage where data is requested from several Member States;

219. The European Health Data Space states in Article 46(6): "The data permit shall set out the general conditions applicable to the data user, in particular: (a) types and format of electronic health data accessed, covered by the data permit, including their sources;

220. The European Health Data Space states in Article 56(3): "The data quality and utility label shall comply with the following elements: (a) for data documentation: meta-data, support documentation, data model, data dictionary, standards used, provenance;

221. The European Health Data Space states in Article 56(3): "The data quality and utility label shall comply with the following elements: (d) coverage: representation of multi-disciplinary electronic health data, representativity of population sampled, average timeframe in which a natural person appears in a dataset;

222. The Data Act states in Article 3(2): "Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (a) the nature and volume of the data likely to be generated by the use of the product or related service;

223. The Data Act states in Article 28(1): "Operators of data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services: (b) the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists shall be described in a publicly available and consistent manner;

224. The Data Act states in Article 3(2): "Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (b) whether the data is likely to be generated continuously and in real-time;

Data description

225. The European Health Data Space states in Article 45(2): "The data access application shall include: (b) a description of the requested electronic health data, their format and data sources, where possible, including geographical coverage where data is requested from several Member States;

226. The European Health Data Space states in Article 56(3): "The data quality and utility label shall comply with the following elements: (d) coverage: representation of multi-disciplinary electronic health data, representativity of population sampled, average timeframe in which a natural person appears in a dataset;

227. The European Health Data Space states in Article 56(3): "The data quality and utility label shall comply with the following elements: (e) information on access and provision: time between the collection of the electronic health data and their addition to the dataset, time to provide electronic health data following electronic health data access application approval;

228. The European Health Data Space states in Article 56(3): "The data quality and utility label shall comply with the following elements: (f) information on data enrichments: merging and adding data to an existing dataset, including links with other datasets;"

229. The Data Act states in Article 28(1): "Operators of data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services: (a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described to allow the recipient to find, access and use the data;

Data permit

230. The European Health Data Space states in Article 44(1): "The health data access body shall ensure that access is only provided to requested electronic health data relevant for the purpose of processing indicated in the data access application by the data user and in line with the data permit granted."

231. The European Health Data Space states in Article 46(6): "The data permit shall set out the general conditions applicable to the data user, in particular: (a) types and format of electronic health data accessed, covered by the data permit, including their sources;

232. The European Health Data Space states in Article 46(7): "Data users shall have the right to access and process the electronic health data in accordance with the data permit delivered to them on the basis of this Regulation."

233. The European Health Data Space states in Article 46(9): "A data permit shall be issued for the duration necessary to fulfil the requested purposes which shall not exceed 5 years. This duration may be extended once."

234. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (d) ensure that data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only;

Interoperability

235. The Data Act states in Article 28(1): "Operators of data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services: (a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described to allow the recipient to find, access and use the data;

236. The Data Act states in Article 28(1): "Operators of data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services: (b) the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists shall be described in a publicly available and consistent manner;

237. The Data Act states in Article 28(1): "Operators of data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services: (c) the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously or in real-time in a machine-readable format;

238. The Data Act states in Article 28(1): "Operators of data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services: (d) the means to enable the interoperability of smart contracts within their services and activities shall be provided."

Data source

239. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: f) the source from which the personal data originate and, where applicable, whether they come from publicly available sources;

240. The General Data Protection Regulation states in Article 15: ""1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, to obtain access to those personal data and to the following information: g) where the personal data is not collected from the data subject, all available information about the source of that data;

241. The European Health Data Space states in Article 45(2): "The data access application shall include: (b) a description of the requested electronic health data, their format and data sources, where possible, including geographical coverage where data is requested from several Member States;

242. The European Health Data Space states in Article 46(6): "The data permit shall set out the general conditions applicable to the data user, in particular: (a) types and format of electronic health data accessed, covered by the data permit, including their sources;

Data quality

243. The European Health Data Space states in Article 56(3): "The data quality and utility label shall comply with the following elements: (b) technical quality, showing the completeness, uniqueness, accuracy, validity, timeliness and consistency of the data;

244. The European Health Data Space states in Article 56(3): "The data quality and utility label shall comply with the following elements: (c) for data quality management processes: level of maturity of the data quality management processes, including review and audit processes, biases examination;

245. The Data Act states in Article 28(1): "Operators of data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services: (a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described to allow the recipient to find, access and use the data;

246. The AI Act states in Article 10(2): "Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular, (a) the relevant design choices; (b) data collection; (c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation; (d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent; (e) a prior assessment of the availability, quantity and suitability of the data sets that are needed; (f) examination in view of possible biases; (g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed."

247. ISO 27701 states in Article 7.4.3 Juistheid en kwaliteit: "The organization should ensure and document that PII throughout its lifecycle is as accurate, complete and current as necessary for the purposes for which the PII is processed."

Data accuracy

248. The General Data Protection Regulation states in Article 5(1): ""1. Personal data must: d) are accurate and updated as necessary; all reasonable steps must be taken to erase or rectify without undue delay (“accuracy”) personal data which are inaccurate having regard to the purposes for which they are processed;

249. The General Data Protection Regulation states in Article 18: "1. The data subject shall have the right to obtain from the controller the restriction of processing where one of the following applies: a) the accuracy of the personal data is contested by the data subject, for a period that enables the controller to verify the accuracy of the personal data;

250. ISO 27701 states in Article 7.4.3 Juistheid en kwaliteit: "The organization should ensure and document that PII throughout its lifecycle is as accurate, complete and current as necessary for the purposes for which the PII is processed."

Data anonymization

251. The Wet op de geneeskundige behandelingsovereenkomst states in Article 458(1): "Contrary to the provisions of Article 457, paragraph 1, information about the patient or access to the data from the file may be provided to another person on request without the patient's consent for the

purpose of statistics or scientific research in the field of public health, if: b) requesting permission, given the nature and purpose of the research, cannot reasonably be required and the care provider has ensured that the data is provided in such a form that it can reasonably be prevented that it can be traced back to individual natural persons.""

252. The European Health Data Space states in Article 44(2): "The health data access bodies shall provide the electronic health data in an anonymised format, where the purpose of processing by the data user can be achieved with such data, taking into account the information provided by the data user."

253. ISO 27701 states in Article 7.4.5 PII aan het einde van de verwerking niet-identificeerbaar maken en wissen: "The organization should erase or convert PII into a form that no longer allows PII subjects to be identified or re-identified once the original PII is no longer needed for the identified purpose(s)."

Data governance

254. The European Health Data Space states in Article 46(9): "A data permit shall be issued for the duration necessary to fulfil the requested purposes which shall not exceed 5 years. This duration may be extended once."

255. The European Health Data Space states in Article 55(1): "The health data access bodies shall inform the data users about the available datasets and their characteristics through a metadata catalogue. Each dataset shall include information concerning the source, the scope, the main characteristics, nature of electronic health data and conditions for making electronic health data available."

256. The AI Act states in Article 10(2): "Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular, (a) the relevant design choices; (b) data collection; (c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation; (d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent; (e) a prior assessment of the availability, quantity and suitability of the data sets that are needed; (f) examination in view of possible biases; (g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed."

Data management

257. The General Data Protection Regulation states in Article 30: "2. The processor and, where applicable, the processor's representative, shall keep records of all categories of processing activities they have carried out on behalf of a controller. This register contains the following information:

258. The AI Act states in Article 10(2): "Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular, (a) the relevant design choices; (b) data collection; (c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation; (d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent; (e) a prior assessment of the availability, quantity and suitability of the data sets that are needed; (f) examination in view of possible biases; (g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed."

259. The AI Act states in Article 17(1): "Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects: (f) systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems;"

Data access application

260. The European Health Data Space states in Article 44(1): "The health data access body shall ensure that access is only provided to requested electronic health data relevant for the purpose of processing indicated in the data access application by the data user and in line with the data permit granted."

261. The European Health Data Space states in Article 45(2): "The data access application shall include: (a) a detailed explanation of the intended use of the electronic health data, including for which of the purposes referred to in Article 34(1) access is sought;

262. The European Health Data Space states in Article 45(2): "The data access application shall include: (b) a description of the requested electronic health data, their format and data sources, where possible, including geographical coverage where data is requested from several Member States;

Data quality management

263. The European Health Data Space states in Article 56(3): "The data quality and utility label shall comply with the following elements: (c) for data quality management processes: level of maturity of the data quality management processes, including review and audit processes, biases examination;

Information Security

Security measures

264. The Wet elektronische gegevensuitwisseling zorg states in Article 1.4(2): ""A data exchange is only designated if the data is secured along the entire path between sender and receiver and is exchanged based on: a. a quality standard as referred to in Article 1, first paragraph, of the Healthcare Quality, Complaints and Disputes Act; or b. legislation or regulations that specify which data are necessary for the provision of good care or with a view to it.""

265. The General Data Protection Regulation states in Article 25: "1. Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of risks to the rights and freedoms of natural persons subject to the processing, the controller shall implement, both in determining the means of processing and in the processing itself, appropriate technical and organizational measures, such as pseudonymization, designed with the aim of effectively implementing data protection principles, such as data minimization and to include necessary safeguards in the processing to comply with the requirements of this Regulation and to protect the rights of the data subjects.

266. The General Data Protection Regulation states in Article 32: "1. Taking into account the state of the art, the costs of implementation, as well as the nature, scope, context and purposes of the

processing and the varying likelihood and severity of risks to the rights and freedoms of individuals, the controller and the processor shall appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, where appropriate, the following:

267. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (a) restrict access to the secure processing environment to authorised persons listed in the respective data permit;

268. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (b) minimise the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the secure processing environment through state-of-the-art technological means;

269. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (c) limit the input of electronic health data and the inspection, modification or deletion of electronic health data hosted in the secure processing environment to a limited number of authorised identifiable individuals;

270. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (d) ensure that data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only;

271. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (e) keep identifiable logs of access to the secure processing environment for the period of time necessary to verify and audit all processing operations in that environment;

272. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (f) ensure compliance and monitor the security measures referred to in this Article to mitigate potential security threats."

273. The European Health Data Space states in Article 50(2): "The health data access bodies shall ensure that electronic health data can be uploaded by data holders and can be accessed by the data user in a secure processing environment. The data users shall only be able to download non-personal electronic health data from the secure processing environment."

274. The European Health Data Space states in Article 50(3): "The health data access bodies shall ensure regular audits of the secure processing environments."

275. The Data Act states in Article 11(1): "The data holder may apply appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and to ensure compliance with Articles 5, 6, 9 and 10, as well as with the agreed contractual terms for

making data available. Such technical protection measures shall not be used as a means to hinder the user's right to effectively provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation implementing Union law as referred to in Article 8(1)."

276. The Medical Devices states in Article Annex I, 17(4): "Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended."

277. ISO 27701 states in Article 6.11.1.2 Toepassingen op openbare netwerken beveiligen: "The organization should ensure that PII transferred over untrusted data transfer networks is encrypted prior to transfer."

278. ISO 27701 states in Article 6.12.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: "The organization should specify in agreements with suppliers whether PII is processed and what minimum technical and organizational measures the supplier must comply with …"

279. ISO 27701 states in Article 7.4.9 Beheersmaatregelen voor de overdracht van PII: "The organization should subject PII sent over a data transfer network (e.g., to another organization) to appropriate controls designed to ensure that the data reaches its intended destination."

280. NEN 7512 states in Article 6.2.5 Encryption: "1) Exchange must be done securely as follows by means of layered security ('defence in depth'), recognizing the following security layers: secure network, encrypted message and encrypted channel. The required layering of security is as follows:

Legal basis

281. The General Data Protection Regulation states in Article 6(1): "1. The processing is lawful only if and to the extent that at least one of the following conditions is met: a) the data subject has given consent to the processing of his personal data for one or more specific purposes;

282. The General Data Protection Regulation states in Article 6(1): "1. The processing is lawful only if and to the extent that at least one of the following conditions is met: c) the processing is necessary for compliance with a legal obligation to which the controller is subject;

283. The General Data Protection Regulation states in Article 6(1): "1. The processing is lawful only if and to the extent that at least one of the following conditions is met: d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

284. The General Data Protection Regulation states in Article 6(1): "1. The processing is lawful only if and to the extent that at least one of the following conditions is met: f) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where the interests or fundamental rights and freedoms of the data subject which require the protection of personal data outweigh those interests, in particular when the person concerned is a child.

285. The General Data Protection Regulation states in Article 13: "1. Where personal data relating to a data subject are collected from that person, the controller shall provide the data subject with the following information at the time of obtaining the personal data: c) the processing purposes for which the personal data are intended, as well as the legal basis for the processing;

286. The General Data Protection Regulation states in Article 13: "1. Where personal data relating to a data subject are collected from that person, the controller shall provide the data subject with the following information at the time of obtaining the personal data: d) the legitimate interests of the controller or of a third party, where the processing is based on point (f) of Article 6(1);

287. The General Data Protection Regulation states in Article 14: ""1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: c) the processing purposes for which the personal data are intended and the legal basis for the processing;

288. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: b) the legitimate interests of the controller or of a third party, where the processing is based on point (f) of Article 6(1);

289. The General Data Protection Regulation states in Article 17: "3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: b) for compliance with a legal processing obligation laid down in Union or Member State law to which the controller is subject, or for the performance of a task carried out in the public interest or to exercise official authority vested in the controller;

290. The General Data Protection Regulation states in Article 17: "3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (c) for reasons of public interest in the field of public health in accordance with points (h) and (i) of Article 9(2) and Article 9(3);

291. The General Data Protection Regulation states in Article 6(1): "1. The processing is lawful only if and to the extent that at least one of the following conditions is met: b) the processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;

292. NEN 7512 states in Article 6.1.10 Basis : "The communication parties must ensure to each other that they have a valid basis for processing personal health information."

Confidentiality

293. The Wet op de geneeskundige behandelingsovereenkomst states in Article 457(1): "Without prejudice to the provisions of Article 448 paragraph 4, second sentence, the care provider shall ensure that no information about the patient or access to or copies of the data from the file is provided to anyone other than the patient without the patient's consent. If provision takes place, this will only take place insofar as this does not harm another person's privacy. The provision may take place without observing the restrictions referred to in the previous sentences, if required by or pursuant to the law."

294. The Wet elektronische gegevensuitwisseling zorg states in Article 1.4(2): ""A data exchange is only designated if the data is secured along the entire path between sender and receiver and is exchanged based on: a. a quality standard as referred to in Article 1, first paragraph, of the Healthcare Quality, Complaints and Disputes Act; or b. legislation or regulations that specify which data are necessary for the provision of good care or with a view to it.""

295. The General Data Protection Regulation states in Article 5(1): ""1. Personal data must: (f) processed, by taking appropriate technical or organizational measures, in such a way that their appropriate security is ensured, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage (‘integrity and confidentiality ”).""

296. The General Data Protection Regulation states in Article 14: "5. Paragraphs 1 to 4 shall not apply if and insofar as: d) the personal data must be kept confidential for reasons of professional secrecy under Union or Member State law, w"

297. The General Data Protection Regulation states in Article 32: "1. Taking into account the state of the art, the costs of implementation, as well as the nature, scope, context and purposes of the processing and the varying likelihood and severity of risks to the rights and freedoms of

individuals, the controller and the processor shall appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, where appropriate, the following: b) the ability to ensure on an ongoing basis the confidentiality, integrity, availability and resilience of the processing systems and services;

298. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (d) ensure that data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only;

299. The Medical Devices states in Article 109(1): "Unless otherwise provided for in this Regulation and without prejudice to existing national provisions and practices in the Member States on confidentiality, all parties involved in the application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks in order to protect the following: (a) personal data, in accordance with Article 110; (b) commercially confidential information and trade secrets of a natural or legal person, including intellectual property rights; unless disclosure is in the public interest; (c) the effective implementation of this Regulation, in particular for the purpose of inspections, investigations or audits."

300. ISO 27701 states in Article 6.7.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen: "The organization should inform the customer of the circumstances in which it uses cryptography to protect the PII it processes."

301. ISO 27701 states in Article 6.10.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst: "The organization should ensure that persons acting under its authority who have access to PII are bound by a duty of confidentiality."

302. ISO 27701 states in Article 6.11.1.2 Toepassingen op openbare netwerken beveiligen: "The organization should ensure that PII transferred over untrusted data transfer networks is encrypted prior to transfer."

303. NEN 7510-2 states in Article 8.2.1 Classification of information: "Organizations that process personal health information, must uniformly classify such information as confidential."

Access control

304. The European Health Data Space states in Article 3(9): "Notwithstanding Article 6(1), point (d), of Regulation (EU) 2016/679, natural persons shall have the right to restrict access of health professionals to all or part of their electronic health data. Member States shall establish the rules and specific safeguards regarding such restriction mechanisms. "

305. The European Health Data Space states in Article 4(2): "In line with the data minimisation principle provided for in Regulation (EU) 2016/679, Member States may establish rules providing for the categories of personal electronic health data required by different health professions. Such rules shall not be based on the source of electronic health data."

306. The European Health Data Space states in Article 4(4): "Where access to electronic health data has been restricted by the natural person, the healthcare provider or health professionals shall not be informed of the content of the electronic health data without prior authorisation by the natural person, including where the provider or professional is informed of the existence and nature of the restricted electronic health data. In cases where processing is necessary in order to protect the vital interests of the data subject or of another natural person, the healthcare provider or health professional may get access to the restricted electronic health data. Following such access, the healthcare provider or health professional shall inform the data holder and the

natural person concerned or his/her guardians that access to electronic health data had been granted. Member States' law may add additional safeguards."

307. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (a) restrict access to the secure processing environment to authorised persons listed in the respective data permit;

308. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (b) minimise the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the secure processing environment through state-of-the-art technological means;

309. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (c) limit the input of electronic health data and the inspection, modification or deletion of electronic health data hosted in the secure processing environment to a limited number of authorised identifiable individuals;

310. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (d) ensure that data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only;

311. The Data Act states in Article 11(1): "The data holder may apply appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and to ensure compliance with Articles 5, 6, 9 and 10, as well as with the agreed contractual terms for making data available. Such technical protection measures shall not be used as a means to hinder the user's right to effectively provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation implementing Union law as referred to in Article 8(1)."

312. The Data Act states in Article 30(1): "The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements: (d) access control: a smart contract shall be protected through rigorous access control mechanisms at the governance and smart contract layers."

313. NEN 7510-2 states in Article 12.4.2 Protecting information in log files: "Log facilities and information contained in log files should be protected against forgery and unauthorized access."

Authorized access

314. The Wet op de geneeskundige behandelingsovereenkomst states in Article 458(1): "Contrary to the provisions of Article 457, paragraph 1, information about the patient or access to the data from the file may be provided to another person on request without the patient's consent for the purpose of statistics or scientific research in the field of public health, if: a) requesting permission is not reasonably possible and with regard to the conduct of the research such

guarantees have been provided that the privacy of the patient is not disproportionately harmed, or

315. The Wet op de geneeskundige behandelingsovereenkomst states in Article 458(1): "Contrary to the provisions of Article 457, paragraph 1, information about the patient or access to the data from the file may be provided to another person on request without the patient's consent for the purpose of statistics or scientific research in the field of public health, if: b) requesting permission, given the nature and purpose of the research, cannot reasonably be required and the care provider has ensured that the data is provided in such a form that it can reasonably be prevented that it can be traced back to individual natural persons.""

316. The Wet elektronische gegevensuitwisseling zorg states in Article 4.1(3): "The officials referred to in the first paragraph are, insofar as this is necessary for the performance of their duties, authorized to inspect data, including health data, to make copies thereof and if this cannot be done on site, the data for that purpose for a short period of time against written evidence to be issued by them, and to demand information in this regard from the relevant care provider or care provider."

317. The European Health Data Space states in Article 44(1): "The health data access body shall ensure that access is only provided to requested electronic health data relevant for the purpose of processing indicated in the data access application by the data user and in line with the data permit granted."

318. The European Health Data Space states in Article 46(7): "Data users shall have the right to access and process the electronic health data in accordance with the data permit delivered to them on the basis of this Regulation."

319. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (c) limit the input of electronic health data and the inspection, modification or deletion of electronic health data hosted in the secure processing environment to a limited number of authorised identifiable individuals;

320. The European Health Data Space states in Article 50(2): "The health data access bodies shall ensure that electronic health data can be uploaded by data holders and can be accessed by the data user in a secure processing environment. The data users shall only be able to download non-personal electronic health data from the secure processing environment."

Data transfer

321. The General Data Protection Regulation states in Article 14: ""1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: f) where applicable, that the controller intends to transfer the personal data to a recipient in a third country or to an international organisation; whether or not there is an adequacy decision by the Commission; or, in the case of transfers referred to in Article 46, Article 47 or the second subparagraph of Article 49(1), what are the appropriate or suitable safeguards, how a copy of them can be obtained or where they can be consulted.

322. The General Data Protection Regulation states in Article 15: "2. When personal data are transferred to a third country or an international organisation, the data subject shall have the right to be informed of the appropriate safeguards in accordance with Article 46 on the transfer.

323. The General Data Protection Regulation states in Article 30: "2. The processor and, where applicable, the processor's representative, shall keep records of all categories of processing activities they have carried out on behalf of a controller. This register contains the following

information: (c) where applicable, transfers of personal data to a third country or an international organisation, specifying that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documents concerning the appropriate safeguards;

324. The European Health Data Space states in Article 3(8): "Natural persons shall have the right that, where the data holder and the data recipient are located in different Member States and such electronic health data belongs to the categories referred to in Article 5, the data holder shall transmit the data in the European electronic health record exchange format referred to in Article 6 and the data recipient shall read and accept it.

325. The General Data Protection Regulation states in Article 30: "1. Each controller and, where applicable, the controller's representative, shall keep a record of the processing activities under their responsibility. That record shall contain all of the following information: (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documents regarding the appropriate safeguards;

326. ISO 27701 states in Article 6.11.1.2 Toepassingen op openbare netwerken beveiligen: "The organization should ensure that PII transferred over untrusted data transfer networks is encrypted prior to transfer."

Integrity

327. The Wet elektronische gegevensuitwisseling zorg states in Article 1.4(2): ""A data exchange is only designated if the data is secured along the entire path between sender and receiver and is exchanged based on: a. a quality standard as referred to in Article 1, first paragraph, of the Healthcare Quality, Complaints and Disputes Act; or b. legislation or regulations that specify which data are necessary for the provision of good care or with a view to it.""

328. The General Data Protection Regulation states in Article 5(1): ""1. Personal data must: (f) processed, by taking appropriate technical or organizational measures, in such a way that their appropriate security is ensured, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage (‘integrity and confidentiality ”).""

329. The General Data Protection Regulation states in Article 32: "1. Taking into account the state of the art, the costs of implementation, as well as the nature, scope, context and purposes of the processing and the varying likelihood and severity of risks to the rights and freedoms of individuals, the controller and the processor shall appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, where appropriate, the following: b) the ability to ensure on an ongoing basis the confidentiality, integrity, availability and resilience of the processing systems and services;

330. ISO 27701 states in Article 6.11.1.2 Toepassingen op openbare netwerken beveiligen: "The organization should ensure that PII transferred over untrusted data transfer networks is encrypted prior to transfer."

331. NEN 7510-2 states in Article 12.4.2 Protecting information in log files: "Log facilities and information contained in log files should be protected against forgery and unauthorized access."

Encryption

332. The AI Act states in Article 10(5): "To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article

9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued."

333. ISO 27701 states in Article 6.7.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen: "The organization should inform the customer of the circumstances in which it uses cryptography to protect the PII it processes."

334. ISO 27701 states in Article 6.11.1.2 Toepassingen op openbare netwerken beveiligen: "The organization should ensure that PII transferred over untrusted data transfer networks is encrypted prior to transfer."

335. NEN 7512 states in Article 6.2.5 Encryption: "1) Exchange must be done securely as follows by means of layered security ('defence in depth'), recognizing the following security layers: secure network, encrypted message and encrypted channel. The required layering of security is as follows:

Safeguards

336. The General Data Protection Regulation states in Article 14: "5. Paragraphs 1 to 4 shall not apply if and insofar as: c) the collection or disclosure of the data is expressly provided for by Union or Member State law to which the controller is subject and which provides for appropriate measures to safeguard the data subject's legitimate interests; or

337. The General Data Protection Regulation states in Article 25: "1. Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of risks to the rights and freedoms of natural persons subject to the processing, the controller shall implement, both in determining the means of processing and in the processing itself, appropriate technical and organizational measures, such as pseudonymization, designed with the aim of effectively implementing data protection principles, such as data minimization and to include necessary safeguards in the processing to comply with the requirements of this Regulation and to protect the rights of the data subjects.

338. The European Health Data Space states in Article 45(2): "The data access application shall include: (f) a description of the safeguards planned to protect the rights and interests of the data holder and of the natural persons concerned;

Pseudonymization

339. The General Data Protection Regulation states in Article 25: "1. Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of risks to the rights and freedoms of natural persons subject to the processing, the controller shall implement, both in determining the means of processing and in the processing itself, appropriate technical and organizational measures, such as pseudonymization, designed with the aim of effectively implementing data protection principles, such as data minimization and to include necessary safeguards in the processing to comply with the requirements of this Regulation and to protect the rights of the data subjects.

340. The European Health Data Space states in Article 44(3): "Where the purpose of the data user's processing cannot be achieved with anonymised data, taking into account the information provided by the data user, the health data access bodies shall provide access to electronic health

data in pseudonymised format. The information necessary to reverse the pseudonymisation shall be available only to the health data access body. Data users shall not re-identify the electronic health data provided to them in pseudonymised format. The data user's failure to respect the health data access body's measures ensuring pseudonymisation shall be subject to appropriate penalties. "

341. The AI Act states in Article 10(5): "To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued."

Logging

342. NEN 7510-2 states in Article 12.4.2 Protecting information in log files: "Log facilities and information contained in log files should be protected against forgery and unauthorized access."

343. NEN 7512 states in Article 6.2.9 Logging : "De communicatiepartijen moeten ervoor zorgen dat logging plaatsvindt volgens NEN 7513 voor zowel de gebeurtenis verzending als ontvangst.

344. NEN 7510-2 states in Article 12.4.1 Logging actions: "Event logs that log user activity, exceptions, and information security events should be created, retained, and reviewed regularly."

Robustness

345. The Data Act states in Article 30(1): "The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements: (a) robustness: ensure that the smart contract has been designed to offer a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;

346. The AI Act states in Article 15(1): "High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle."

Availability

347. The General Data Protection Regulation states in Article 32: "1. Taking into account the state of the art, the costs of implementation, as well as the nature, scope, context and purposes of the processing and the varying likelihood and severity of risks to the rights and freedoms of individuals, the controller and the processor shall appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, where appropriate, the following: b) the ability to ensure on an ongoing basis the confidentiality, integrity, availability and resilience of the processing systems and services;

Automated Processing

Smart contracts

348. The Data Act states in Article 11(1): "The data holder may apply appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and to ensure compliance with Articles 5, 6, 9 and 10, as well as with the agreed contractual terms for making data available. Such technical protection measures shall not be used as a means to hinder the user's right to effectively provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation implementing Union law as referred to in Article 8(1)."

349. The Data Act states in Article 30(1): "The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements: (a) robustness: ensure that the smart contract has been designed to offer a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;

350. The Data Act states in Article 30(1): "The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements: (b) safe termination and interruption: ensure that a mechanism exists to terminate the continued execution of transactions: the smart contract shall include internal functions which can reset or instruct the contract to stop or interrupt the operation to avoid future (accidental) executions;

351. The Data Act states in Article 30(1): "The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements: (c) data archiving and continuity: foresee, if a smart contract must be terminated or deactivated, a possibility to archive transactional data, the smart contract logic and code to keep the record of the operations performed on the data in the past (auditability); and

352. The Data Act states in Article 30(1): "The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements: (d) access control: a smart contract shall be protected through rigorous access control mechanisms at the governance and smart contract layers."

353. The Data Act states in Article 28(1): "Operators of data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services: (d) the means to enable the interoperability of smart contracts within their services and activities shall be provided."

AI risks

354. The AI Act states in Article 9(2): "The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise the following steps: (a) identification and analysis of the known and foreseeable risks associated with each high-risk AI system;

355. The AI Act states in Article 9(2): "The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular

systematic updating. It shall comprise the following steps: (b) estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse;

356. The AI Act states in Article 9(2): "The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise the following steps: (c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;

357. The AI Act states in Article 9(4): "The risk management measures referred to in paragraph 2, point (d) shall be such that any residual risk associated with each hazard as well as the overall residual risk of the high-risk AI systems is judged acceptable, provided that the high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. Those residual risks shall be communicated to the user.

Automated decision-making

358. The General Data Protection Regulation states in Article 14: "2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information in order to ensure fair and transparent processing vis-à-vis the data subject: (g) the existence of automated decision-making, including profiling referred to in Article 22(1) and (4), and, at least in those cases, useful information about the underlying logic, as well as the importance and expected consequences of that processing for the data subject.

359. The General Data Protection Regulation states in Article 15: "1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, to obtain access to those personal data and to the following information: (h) the existence of automated decision-making, including profiling referred to in Article 22(1) and (4), and, at least in those cases, useful information about the underlying logic, as well as the importance and expected consequences of that processing for the data subject.

360. The General Data Protection Regulation states in Article 21: "1. The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to processing of personal data concerning him/her which is based on point (e) or (f) of Article 6(1), including profiling on the basis of those provisions. The controller shall cease processing the personal data unless he can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims .

361. The General Data Protection Regulation states in Article 21: "2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing, including profiling related to direct marketing.

Safe termination and interruption

362. The Data Act states in Article 30(1): "The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements: (b) safe termination and interruption: ensure that a mechanism exists to terminate the continued execution of transactions: the smart contract shall

include internal functions which can reset or instruct the contract to stop or interrupt the operation to avoid future (accidental) executions;

363. The AI Act states in Article 14(4): "The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (e)be able to intervene on the operation of the high-risk AI system or interrupt the system through a “stop” button or a similar procedure."

364. The AI Act states in Article 29(4): "Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor when they have identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis."

Overrule

365. The European Health Data Space states in Article 4(4): "Where access to electronic health data has been restricted by the natural person, the healthcare provider or health professionals shall not be informed of the content of the electronic health data without prior authorisation by the natural person, including where the provider or professional is informed of the existence and nature of the restricted electronic health data. In cases where processing is necessary in order to protect the vital interests of the data subject or of another natural person, the healthcare provider or health professional may get access to the restricted electronic health data. Following such access, the healthcare provider or health professional shall inform the data holder and the natural person concerned or his/her guardians that access to electronic health data had been granted. Member States’ law may add additional safeguards."

366. The AI Act states in Article 14(4): "The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (d)be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system;

AI bias

367. The AI Act states in Article 10(2): "Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular, (a) the relevant design choices; (b) data collection; (c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation; (d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent; (e) a prior assessment of the availability, quantity and suitability of the data sets that are needed; (f) examination in view of possible biases; (g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed."

368. The AI Act states in Article 10(5): "To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-

art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued."

AI vulnerabilities

369. The AI Act states in Article 15(4): "High-risk AI systems shall be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities. The technical solutions aimed at ensuring the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks. The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws

Automated Processing

AI Monitoring

370. The AI Act states in Article 12(3): "In particular, logging capabilities shall enable the monitoring of the operation of the high-risk AI system with respect to the occurrence of situations that may result in the AI system presenting a risk within the meaning of Article 65(1) or lead to a substantial modification, and facilitate the post-market monitoring referred to in Article 61."

371. The AI Act states in Article 14(4): "The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (a)fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible;

372. The AI Act states in Article 20(1): "Providers of high-risk AI systems shall keep the logs automatically generated by their high-risk AI systems, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law. The logs shall be kept for a period that is appropriate in the light of the intended purpose of high-risk AI system and applicable legal obligations under Union or national law."

373. The AI Act states in Article 9(2): "The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise the following steps: (c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;

374. The AI Act states in Article 29(4): "Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor when they have identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis."

Oversight

375. The AI Act states in Article 14(1): "High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use."

376. The AI Act states in Article 14(4): "The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (a)fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible;

377. The AI Act states in Article 14(4): "The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (b)remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;

378. The AI Act states in Article 14(4): "The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (c)be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available;

Healthcare and Ethics

Electronic Health Record

379. The Wet op de geneeskundige behandelingsovereenkomst states in Article 454(1): "The care provider sets up a file regarding the treatment of the patient. He keeps a record in the file of the data concerning the health of the patient and the procedures performed with regard to him and includes other data in it, all this insofar as this is necessary for proper care of the patient."

380. The Wet op de geneeskundige behandelingsovereenkomst states in Article 458(3): "In the case of a provision in accordance with paragraph 1, this shall be noted in the file."

381. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 4: "A healthcare provider uses a client's citizen service number with the aim of guaranteeing that the personal data to be processed in the context of the provision of healthcare relate to that client."

382. The Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 8: "The healthcare provider includes the citizen service number of the client in its administration when recording personal data with regard to the provision of healthcare."

383. The Wet elektronische gegevensuitwisseling zorg states in Article 4.1(3): "The officials referred to in the first paragraph are, insofar as this is necessary for the performance of their duties, authorized to inspect data, including health data, to make copies thereof and if this cannot be done on site, the data for that purpose for a short period of time against written evidence to be issued by them, and to demand information in this regard from the relevant care provider or care provider."

384. The European Health Data Space states in Article 3(6): "Natural persons may insert their electronic health data in their own EHR or in that of natural persons whose health information they can access, through electronic health data access services or applications linked to these

services. That information shall be marked as inserted by the natural person or by his or her representative."

385. The European Health Data Space states in Article 3(8): "Natural persons shall have the right to give access to or request a data holder from the health or social security sector to transmit their electronic health data to a data recipient of their choice from the health or social security sector, immediately, free of charge and without hindrance from the data holder or from the manufacturers of the systems used by that holder.

386. The European Health Data Space states in Article 4(3): "Member States shall ensure that access to at least the priority categories of electronic health data referred to in Article 5 is made available to health professionals through health professional access services. Health professionals who are in possession of recognised electronic identification means shall have the right to use those health professional access services, free of charge."

387. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (a) restrict access to the secure processing environment to authorised persons listed in the respective data permit;

388. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (b) minimise the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the secure processing environment through state-of-the-art technological means;

389. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (c) limit the input of electronic health data and the inspection, modification or deletion of electronic health data hosted in the secure processing environment to a limited number of authorised identifiable individuals;

390. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (d) ensure that data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only;

391. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (e) keep identifiable logs of access to the secure processing environment for the period of time necessary to verify and audit all processing operations in that environment;

392. The European Health Data Space states in Article 50(1): "The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures: (f) ensure compliance and monitor the security measures referred to in this Article to mitigate potential security threats."

393. The European Health Data Space states in Article 50(2): "The health data access bodies shall ensure that electronic health data can be uploaded by data holders and can be accessed by the data user in a secure processing environment. The data users shall only be able to download non-personal electronic health data from the secure processing environment."

Ethical conduct

394. The Wet op de geneeskundige behandelingsovereenkomst states in Article 448(2): "In carrying out the obligation laid down in paragraph 1, the care provider is guided by what the patient should reasonably know with regard to: b. the expected consequences and risks to the health of the patient in the case of the proposed examination, the proposed treatment, the procedures to be performed and in the event of non-treatment;

395. The Wet op de geneeskundige behandelingsovereenkomst states in Article 448(4): "The care provider may only withhold such information from the patient insofar as providing it would clearly cause serious harm to the patient. If the interest of the patient so requires, the care provider must provide the relevant information to someone other than the patient. The information will be given to the patient as soon as the said disadvantage can no longer be feared. The care provider will not make use of his power referred to in the first sentence until he has consulted another care provider about this."

396. The Wet op de geneeskundige behandelingsovereenkomst states in Article 458(1): "Contrary to the provisions of Article 457, paragraph 1, information about the patient or access to the data from the file may be provided to another person on request without the patient's consent for the purpose of statistics or scientific research in the field of public health, if: a) requesting permission is not reasonably possible and with regard to the conduct of the research such guarantees have been provided that the privacy of the patient is not disproportionately harmed, or

397. The Medical Devices states in Article 64(1): "In the case of incapacitated subjects who have not given, or have not refused to give, informed consent before the onset of their incapacity, a clinical investigation may be conducted only where, in addition to the conditions set out in Article 62(4), all of the following conditions are met: (d) no incentives or financial inducements are given to subjects or their legally designated representatives, except for compensation for expenses and loss of earnings directly related to the participation in the clinical investigation;

398. The Medical Devices states in Article 64(1): "In the case of incapacitated subjects who have not given, or have not refused to give, informed consent before the onset of their incapacity, a clinical investigation may be conducted only where, in addition to the conditions set out in Article 62(4), all of the following conditions are met: (e) the clinical investigation is essential with respect to incapacitated subjects and data of comparable validity cannot be obtained in clinical investigations on persons able to give informed consent, or by other research methods;

399. The Medical Devices states in Article 65(1): "A clinical investigation on minors may be conducted only where, in addition to the conditions set out in Article 62(4), all of the following conditions are met: (d) no incentives or financial inducements are given to the subject or his or her legally designated representative except for compensation for expenses and loss of earnings directly related to the participation in the clinical investigation;

400. The Medical Devices states in Article 65(1): "A clinical investigation on minors may be conducted only where, in addition to the conditions set out in Article 62(4), all of the following conditions are met: (e) the clinical investigation is intended to investigate treatments for a medical condition that only occurs in minors or the clinical investigation is essential with respect

to minors to validate data obtained in clinical investigations on persons able to give informed consent or by other research methods;

401. The Wet op de geneeskundige behandelingsovereenkomst states in Article 448(2): "In carrying out the obligation laid down in paragraph 1, the care provider is guided by what the patient should reasonably know with regard to: a. the nature and purpose of the intended examination, the proposed treatment or the procedures to be performed;

Accessibility

402. The European Health Data Space states in Article 4(1): "Where they process data in an electronic format, health professionals shall: (a) have access to the electronic health data of natural persons under their treatment, irrespective of the Member State of affiliation and the Member State of treatment;

403. The European Health Data Space states in Article 4(3): "Member States shall ensure that access to at least the priority categories of electronic health data referred to in Article 5 is made available to health professionals through health professional access services. Health professionals who are in possession of recognised electronic identification means shall have the right to use those health professional access services, free of charge."

Doctor patient confidentiality

404. The Wet elektronische gegevensuitwisseling zorg states in Article 4.1(4): "Insofar as the healthcare provider or healthcare provider in question is obliged to keep data confidential by virtue of his office, profession or agreement, he cannot invoke this obligation, contrary to Article 5:20, second paragraph, of the General Administrative Law Act against officials referred to in paragraph 1. The officials referred to in the first paragraph are subject to the same duty of confidentiality as the relevant healthcare provider or healthcare provider."

405. The General Data Protection Regulation states in Article 14: "5. Paragraphs 1 to 4 shall not apply if and insofar as: d) the personal data must be kept confidential for reasons of professional secrecy under Union or Member State law, w"

Protection of vital interests

406. The General Data Protection Regulation states in Article 6(1): "1. The processing is lawful only if and to the extent that at least one of the following conditions is met: d) the processing is necessary to protect the vital interests of the data subject or of another natural person;