Graduate Certificate in AI for Medical Device Regulation

Data Protection and Privacy in AI for Medical Devices

Data Protection and Privacy in AI for Medical Devices are critical aspects of the Graduate Certificate in AI for Medical Device Regulation. Below are key terms and vocabulary that learners should understand:

1. Personal Data: Any information relating to an identified or identifiable natural person.
2. Data Controller: The entity that determines the purposes, conditions, and means of the processing of personal data.
3. Data Processor: The entity that processes personal data on behalf of the data controller.
4. Data Protection Impact Assessment (DPIA): A process to help identify and minimize the data protection risks of a project.
5. General Data Protection Regulation (GDPR): The European Union's regulation on data protection and privacy in the European Economic Area.
6. Health Insurance Portability and Accountability Act (HIPAA): A US law that provides data privacy and security provisions for safeguarding medical information.
7. Artificial Intelligence (AI): The simulation of human intelligence processes by machines, especially computer systems.
8. Machine Learning (ML): A subset of AI that enables systems to learn and improve from experience without being explicitly programmed.
9. Deep Learning (DL): A subset of ML that uses neural networks with many layers to learn and represent data.
10. Natural Language Processing (NLP): A field of AI that focuses on the interaction between computers and human language.
11. Computer Vision: A field of AI that trains computers to interpret and understand the visual world.
12. Data Mining: The process of discovering patterns and knowledge from large amounts of data.
13. Data Privacy: The protection of personal data and the preservation of an individual's right to control their information.
14. Data Security: The protection of data from unauthorized access, use, disclosure, disruption, modification, or destruction.
15. Anonymization: The process of removing personally identifiable information from data.
16. Pseudonymization: The process of replacing personally identifiable information with pseudonyms to prevent identification.
17. Consent: A freely given, specific, informed, and unambiguous indication of the data subject's wishes.
18. Data Subject Access Rights: The rights of individuals to access their personal data and to know how it is being used.

19. Data Breach: The unauthorized access, use, disclosure, disruption, modification, or destruction of personal data.
20. Privacy by Design: The approach to designing systems and processes that protect privacy and data protection from the outset.
21. Privacy by Default: The approach to setting privacy-friendly defaults in systems and processes.
22. Accountability: The obligation of data controllers to implement appropriate technical and organizational measures to ensure and demonstrate compliance with data protection laws and regulations.
23. Transparency: The obligation of data controllers to provide clear and concise information about the processing of personal data.
24. Profiling: The automated processing of personal data to evaluate certain personal aspects relating to a natural person.
25. Right to Erasure: The right of individuals to request the deletion of their personal data.
26. Right to Object: The right of individuals to object to the processing of their personal data.
27. Data Protection Officer (DPO): A person responsible for ensuring that an organization complies with data protection laws and regulations.
28. Cross-Border Data Transfers: The transfer of personal data between different countries or jurisdictions.
29. Standard Contractual Clauses (SCCs): A set of contractual terms and conditions that ensure the protection of personal data in cross-border data transfers.
30. Binding Corporate Rules (BCRs): A set of internal rules that ensure the protection of personal data in cross-border data transfers within a multinational corporation.
31. Encryption: The process of converting plaintext into ciphertext to prevent unauthorized access.
32. Access Control: The process of granting or denying access to personal data based on the user's role or permissions.
33. Incident Response: The process of responding to and managing a data breach or other security incident.
34. Vendor Management: The process of selecting, monitoring, and managing third-party vendors that process personal data on behalf of the data controller.
35. Privacy Shield: A framework for protecting personal data in cross-border data transfers between the European Union and the United States.
36. Cloud Computing: The delivery of computing services over the internet, including software, storage, and processing power.
37. Internet of Things (IoT): The network of physical devices, vehicles, buildings, and other items embedded with sensors, software, and network connectivity.
38. Edge Computing: The processing of data at the edge of the network, near the source of the data, rather than in a centralized data center.
39. Federated Learning: A ML approach that allows models to be trained on decentralized data without sharing the data itself.
40. Explainability: The ability to understand and interpret the decisions made by AI systems.
41. Fairness: The absence of bias and discrimination in AI systems.
42. Accountability: The ability to trace the decisions made by AI systems back to the underlying data and

algorithms.
43. Robustness: The ability of AI systems to withstand adversarial attacks and other forms of disruption.
44. Privacy-Preserving Data Mining: The process of extracting knowledge from data while preserving privacy and data protection.
45. Differential Privacy: A mathematical approach to data privacy that adds noise to data to prevent identification while preserving utility.
46. Homomorphic Encryption: An encryption method that allows computations to be performed on encrypted data without decrypting it.
47. Secure Multi-Party Computation: A cryptographic technique that allows multiple parties to perform computations on shared data without revealing the data itself.
48. Federated Learning: A ML approach that allows models to be trained on decentralized data without sharing the data itself.
49. Synthetic Data: Artificially generated data that can be used for training AI systems without revealing sensitive information.
50. Transfer Learning: The process of using a pre-trained model as a starting point for training a new model on a different dataset.
51. Adversarial Attacks: Maliciously crafted inputs that are designed to cause AI systems to make incorrect decisions.
52. Model Inversion: An attack that attempts to reconstruct the original data used to train an AI model.
53. Membership Inference: An attack that attempts to determine whether a particular data sample was used to train an AI model.
54. Data Poisoning: An attack that manipulates the training data used to train an AI model.
55. Model Stealing: An attack that attempts to replicate a proprietary AI model without access to the original code or data.
56. Explainable AI (XAI): The development of AI systems that can provide clear and understandable explanations for their decisions.
57. Interpretable AI: The development of AI systems that use simple and transparent algorithms that can be easily understood by humans.
58. Trustworthy AI: The development of AI systems that are transparent, explainable, fair, robust, and accountable.
59. Ethical AI: The development of AI systems that respect human rights, promote social welfare, and avoid harm.
60. Responsible AI: The development of AI systems that are designed and used with consideration for their social and ethical implications.

In conclusion, understanding the key terms and vocabulary related to data protection and privacy in AI for medical devices is essential for learners in the Graduate Certificate in AI for Medical Device Regulation. These terms cover a wide range of concepts, from personal data and data protection laws to AI technologies and ethical considerations. By mastering these terms, learners will be better equipped to navigate the complex regulatory landscape of AI for medical devices and ensure the protection of patient

data and privacy.