Summary of Minimum Requirements Safety and Governance for Digital Health Solutions

Self-Assessment Checklist

Criteria	Response
1. Digital Health Implementation project leads must know: What is being introduced, why is it being introduced, when and where will it be introduced and for whom?	
2. Each new digital health initiative must have one or two local clinical sponsors who have the authority to prevent movement to next stage gate until risks are mitigated.	
3. Define performance and value indicators and a checkpoint schedule to audit progress and implement improvements, especially to mitigate patient safety risks as necessary.	
4. A Safety Case must be documented before implementation of a new digital health solution. All unacceptable risks must be mitigated before commencement.	
5. If possible include patient/citizen representation in the design of the new approach. At a minimum seek patient feedback within 2 months of solution implementation. Include this feedback in the Audit and Review process.	
6. Quality training must be provided by the vendor to clinical users, administrative support staff and technical staff as necessary. Staff should confirm their satisfaction with the training to the Clinical Sponsor.	
7. There must be published, evidence-based support for algorithms used for the provision of clinical decision support.	
8. Satisfactory evidence of clinical effectiveness must be provided.	
9. Information Governance procedures must be followed (Security, DPA and DPIA requirements must be met).	
10. Staff (clinical, technical, business/operational) must be available to implement, manage and sustain the new digital health service.	
11. A business case (detail required depend on cost and scale of the solution) outlining costs and benefits, providing assurance of the ability to deliver must be documented.	
12. There must be agreement from local IT that the infrastructure to support the solution is in place. The vendor and IT Department must agree on network access, cyber-security requirements, storage requirements, and responsibility for managing software updates and security patches.	

13. The HSE Rapid Digital Assessment Tool must be satisfactorily completed prior to implementation of the digital health solution, where the solution represents a new way to deliver health. Conformance with safety standards, Medical Device Directive/Regulations and local technical and cleaning/disinfection should be reviewed prior to purchase.	
14. The patient must consent to Telehealth & Remote Health Monitoring and consent must be recorded in the patient chart or on-boarding documentation.	
15. Every Digital Health project should have a business continuity plan, and a disaster recovery plan.	
16. If possible, digital solutions should make the patient interface available in a number of languages, recognising the diversity of the population.	
17. The manufacturer/vendor is required to submit a Safety Case and Hazard Log.	
18. The supplier of a Digital Health solution must be able to demonstrate that their product or service has a defined process for assessing third-party products and evidence that any third-party products have been assessed against all relevant standards, in particular ISO 14971:2019 Application of Risk Management to Medical Devices, where relevant.	
19. The supplier can provide evidence that the organisation holds a current Cyber Essentials certificate from an accredited certification body (as a minimum). Ideally, the organisation holds a current Cyber Essentials Plus (CE+) certificate.	
20. The supplier must assist the tenderer in completing the DPIA.	
21. There must be an SLA between the Supplier and Purchasing Organisation and this must be reviewed annually.	
22. The HSE's requirements for cyber security must be met.	
23. An MDS2 Form should be completed and submitted by the manufacturer (this is a formalised approach to a Software Bill of Materials).	
24. Medical devices, including Software which has a health function must conform either to the Medical Devices Directive or Medical Device Regulations depending on when they went on the market.	
25. All Digital Health Solutions should use SNOMED Clinical Terminology.	
26. All those implementing digital health solutions should be aware that healthcare activity is counted using ICD-10.	
27. Technical assessments of medical devices should be documented and should be carried out by	

personnel with the appropriate education and training.	
28. Processes must be put in place to track and maintain medical devices, ensure training and education resources are available, processes must be in place to follow up on Field Safety Notices. Consumables and accessories should be available and safe battery and charging management processes must be implemented.	
29. Pre-Acquisition Questionnaires should be used prior to the purchase of Medical Devices.	
30. New digital health solutions generally require their own Data Privacy Impact Assessment (DPIA).	
31. Data Processing Agreements and Data Processing Agreements may also be required as well as a DPIA where data is processed by a third-party.	
32. Retention of Medical Records should be in compliance with the Data Protection Acts: “Personal data must be 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”.	
32. Procurement regulations must be followed.	
33. Clinical Decision Support Systems which may or may not include Artificial Intelligence must undergo a thorough Clinical Risk Management process because there will be many unknowns.	
34. Those implementing new digital health solutions should highlight to manufacturers and vendors the importance of designing for those with disabilities.	
35. Health Apps and Digital Therapeutics, whether medical devices or not, require assurance of effectiveness, privacy & security, quality design and build, developer quality. Examples are Orcha Base Line Review or Label2Enable (ISO 82304 Part 2) assurance.	
36. If physiological data from consumer wearables is used clinically, there should be confirmation that the device is CE-marked to measure the relevant physiological parameter.	
37. Measurements from patient wearables which influence clinical care must form part of the patient record.	
38. Patients should only send measurements from wearables to healthcare professionals when healthcare professionals have invited them to do so, and have agreed to review them.	
39. Quality of consumer purchased app-based diagnostics will be variable and an actionable report will lead to accessing health services in the normal way.	

40. Assess the Digital Capability of the workforce required to implement a digital health solution and ensure staff are educated and trained to the appropriate standard. The Digital Capability Framework may support this process.	
41. Any adverse incidents arising from the use of a digital health solution should be reported on the National Incident Management System. If they involve or possibly involve a medical device (including software which is a medical device), the incident MUST be reported to the supplier and MAY be reported to the HPRA. Support from the Digital Health Clinical Safety lead is available in this regard.	