

Digital Care System Assessment and Management

Standard operating procedure (SOP) | DIG-SOP-002

Document type	Standard operating procedure (SOP)
Title	Digital Care System Assessment and Management
Document ID	{{facility.code}}-DIG-SOP-002
Version and status	1.1 Approved by the ASF Expert Committee
Prepared by	{{roles.quality_lead.name}}, Quality lead
Reviewed by	{{roles.clinical_director.name}}, Clinical director Date: _____
Approver and signature	{{roles.clinical_director.name}}, Clinical director Signature: _____ Date: _____
Effective date	{{document.effective_date}}
Next review	{{document.review_date}} (12 months, or sooner after any incident or change)
Replaces	None (new document)
Standards and criteria supported	Standard 2D, criterion 2D.1
Evidence basis	E-009
Status of this document	Recommended best-practice model. A hospital may adopt, adapt or replace it with an equivalent that meets the same criteria.

At a glance: what to do

1. Assess every digital care system before it is introduced: costs, benefits, interoperability and possible unintended effects.
2. Record the assessment on DIG-FRM-002, signed by the clinical and IT leads.
3. Do not adopt a system on vendor claims alone.
4. Review each system after go-live and at least yearly.

Stop and get help straight away if: a system is in clinical use with no completed assessment.

1. Purpose

To make sure every digital care system (telehealth, remote monitoring, patient-facing app, clinical software) is assessed, implemented and managed through a defined process, not adopted on a vendor pitch [EC].

2. Scope

Applies to	Clinical leads, IT lead, procurement lead, chief executive
Locations	All clinical and patient-facing digital systems at {{facility.legal_name}}
When	Before introduction, at go-live, and yearly
Does not apply to	Standard office software with no clinical use (covered by IT policy DIG-POL-001)

3. Definitions and abbreviations

Term	Meaning in this SOP
Digital care system	Any software or device that supports diagnosis, treatment, monitoring or communication with patients
Interoperability	The ability of two systems to exchange and use data correctly
Unintended consequence	An effect not planned, such as extra workload, duplicate records or missed alerts

4. Background and rationale

Digital tools can improve care but also create new risks: extra workload, data errors, failed links between systems and missed alerts. Criterion 2D.1 asks for an internal assessment and management, not reliance on a vendor's claims.

5. Responsibilities

Role	Duties in this SOP	Competence needed
Chief executive	Approves systems with a major clinical impact	Executive
Clinical lead for the area	Defines the clinical need; signs the assessment	Clinical
IT lead	Assesses interoperability and security	Health informatics (EC)
Procurement lead	Collects vendor information; keeps the contract	Procurement

6. Equipment, materials and resources

Item	Specification or standard	Check before use
Digital tool assessment template (DIG-FRM-002)	Current	Available to project leads
Vendor information and evidence	From the vendor, dated	On file

7. Safety and infection prevention

- No clinical system goes live without a tested interface to the systems it depends on.
- Patient data handling must meet the information security policy (DIG-POL-001).

8. Before you start

- Confirm the clinical need in writing before any vendor evaluation.

9. Procedure

Follow the steps in order. Where a step says "If", take the action for the case that applies. Do not skip a step. If a step cannot be done, use section 11 and section 12.

Step	Action	How to do it	Key point
1	Define the need.	Write the clinical problem the system will solve, the patients affected, and how success will be measured.	A system without a stated problem will be hard to evaluate later.
2	Assess costs and benefits.	- Estimate costs: purchase, training, support, interfaces, and staff time. - Estimate benefits and how they will be measured. - Record the comparison on DIG-FRM-002.	Cost and benefit must be compared with real figures, not the vendor brochure.
3	Assess interoperability.	- List every system the new tool must exchange data with. - Test each link in a non-live environment. - Record each risk from non-interoperability and its mitigation.	Two systems that do not talk create the most common data errors.
4	Assess unintended consequences.	- Ask the clinical lead and two front-line staff what could go wrong: extra workload, duplication, alert fatigue, data errors or delay. - Record each possible effect and how it will be prevented or checked.	Ask the people who will use it, not only the people who buy it.
5	Decide and manage implementation.	- The approver decides on the basis of the record. - Manage go-live with a named owner, training, a fall-back plan and a support route.	A fall-back plan is needed before go-live, not after the first failure.

Step	Action	How to do it	Key point
6	Review.	- Review the system after three months of use, and yearly after that. - Record the findings and actions.	Systems change, and so do the risks.

Decision points

- If the assessment shows a high clinical risk that cannot be mitigated, the system is not introduced until the chief executive decides otherwise, with reasons recorded.

10. Special situations

Situation	What to do
Urgent need (for example, during an outbreak)	Use a temporary, reviewed approval with a time limit set by the chief executive, then complete the assessment.

11. Problems and escalation

- System failures affecting patients go to the chief executive and INC-POL-001 at once.

12. Monitoring and compliance

What is checked	Target	How often	Who	If the target is missed
Systems in clinical use with completed assessment	100%	Yearly	IT lead	Stop use until assessed
Post-implementation reviews done at 3 months	100%	Each system	Clinical lead	Escalate to chief executive
Interface failures logged and reviewed	100%	Quarterly	IT lead	Escalate

13. Records

Record	Where it is kept	Kept for
DIG-FRM-002 Digital Tool Assessment	IT governance file	{{facility.records_retention_years}} years after the system is retired

14. Training and competence

- Project leads are trained in the assessment method at appointment (EC).

15. Related documents

ID	Title	Relationship
DIG-FRM-002	Digital Tool Assessment Template	Used in steps 2 to 4
DIG-POL-001	Information Security and Access Control Policy	Security rules
DIG-FRM-004	Digital System Test and Support Record	Test records

16. Evidence

ID	Source and status
E-006	ASF Policy Framework v1.2. Adapted.
E-009	ASF Expert Committee consensus. Assessment thresholds to be set by the committee.

EC = ASF Expert Committee consensus. Items marked EC are reviewed by the Committee each year.

17. Change history

Version	Date	What changed	Approver and signature
1.0	{{document.effective_date}}	First version	Approved by the ASF Expert Committee
1.1	{{document.effective_date}}	Internal quality review: corrected cross-references, status wording and document control	Approved by the ASF Expert Committee