Standard operating procedure (SOP) · DIG-SOP-002 · Version 1.1 · Approved by the ASF Expert Committee

Supports: 2D.1

At a glance

- Assess every digital care system before it is introduced: costs, benefits, interoperability and possible unintended effects.
- Record the assessment on DIG-FRM-002, signed by the clinical and IT leads.
- Do not adopt a system on vendor claims alone.
- 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 the facility
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

Term	Meaning
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

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	Responsibility	Competence
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. Materials and equipment

Item	Requirement	Condition
Digital tool assessment template (DIG-FRM-002)	Current	Available to project leads
Vendor information and evidence	From the vendor, dated	On file

7. Safety

- 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

Step 1. Define the need.

- Write the clinical problem the system will solve, the patients affected, and how success will be measured.

Key point: A system without a stated problem will be hard to evaluate later.

Step 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.

Key point: Cost and benefit must be compared with real figures, not the vendor brochure.

Step 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.

Key point: Two systems that do not talk create the most common data errors.

Step 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.

Key point: Ask the people who will use it, not only the people who buy it.

Step 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.

Key point: A fall-back plan is needed before go-live, not after the first failure.

Step 6. Review.

- Review the system after three months of use, and yearly after that.
- Record the findings and actions.

Key point: Systems change, and so do the risks.

10. 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.

11. Special situations

Situation	Action
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.

12. Escalation

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

13. Monitoring

Measure	Target	Frequency	Owner	If not met
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

14. Records

Record	Kept in	Retention

DIG-FRM-002 Digital Tool Assessment	IT governance file	the period set by the facility's records policy years after the system is retired

15. Training

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

16. Related documents

ID	Title	Use
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

17. Evidence

Reference	Note
E-006	ASF Policy Framework v1.2. Adapted.
E-009	ASF Expert Committee consensus. Assessment thresholds to be set by the committee.

18. Change history

Version	Date	What changed	Approval
1.0	the date of approval	First version	Approved by the ASF Expert Committee
1.1	the date of approval	Internal quality review: corrected cross-references, status wording and document control	Approved by the ASF Expert Committee

E-learning for this document

- **Technology Platform Reliability & Security** (TM-01)

Planned course: Digital care assessment and management process. New course planned.

References

- Accréditation Sans Frontières (2026). ASF Expert Committee consensus on Standard 1. (E-009)
- Accréditation Sans Frontières (2026). ASF Policy Framework v1.2. (E-006)

Download this document as PDF

Download this document as an editable Word file