Policy · DIG-POL-001 · Version 1.1 · Approved by the ASF Expert Committee

Supports: 2A.4

At a glance

- Give each person access only to the health information they need for their job.
- Use a unique login and a strong password. Never share your login.
- Lock your screen when you leave the workstation.
- Report any suspected breach at once through the breach procedure.
- Review who has access every quarter and remove access when a person leaves.
- Stop and get help straight away if: you suspect patient information has been seen, copied or sent to the wrong person. Stop, and report it at once.

1. Purpose

To protect patient health information from unauthorised access, loss, change or disclosure, using practical security measures [E-006, EC].

2. Scope

Applies to	All staff, students, contractors and anyone with access to the facility's systems or paper records
Locations	All sites, systems, devices and paper records
When	At all times
Does not apply to	Clinical decisions on the use of information, which are covered by the confidentiality and records policies

3. Definitions

Term	Meaning
Health information	Any information that identifies a patient and relates to their care

Access control	Rules and tools that decide who can see, change or share information
Breach	Any unauthorised access, loss, disclosure or change of health information

4. Background

Patients share their health information on the basis that it will be kept private. A breach can cause harm, distress and loss of trust. Criterion 2A.4 asks for access controls and a breach response plan that the facility can actually carry out with its resources.

5. Responsibilities

Role	Responsibility	Competence
IT lead	Sets access controls; runs the access review; manages security tools	IT security competence
Data protection lead	Advises on the law; leads breach assessment; keeps the breach log	Data protection competence
Line managers	Request and approve access; tell IT when a person changes role or leaves	Management training
Every user	Protect login and device; report breaches; follow the rules	Induction and annual training

6. Materials and equipment

Item	Requirement	Condition
Access rules (role-based list)	Written per role	Reviewed quarterly
Strong password standard	Length and rules set by the IT lead (EC)	Enforced by system
Screen lock	Set to lock after a short period of inactivity (EC)	On all workstations
Breach response plan (DIG-SOP-001)	Current	Available to the breach team

7. Safety

- Do not write passwords on paper near a workstation.
- Do not email health information to personal accounts or unapproved services.
- Do not leave paper records unattended. Use locked storage.

8. Before you start

- Check your access is correct for your role.
- Check your device is locked when unattended.

9. Procedure

Step 1. Set access by role.

- Write an access list for each role: what information, what systems, what actions (view, change, export).
- Give access on the basis of the role, not the person.
- Use a unique login for each user.

Key point: Role-based access limits what a person can see to what their job needs.

Step 2. Protect logins and devices.

- Use a strong password and multi-factor login where the system allows.
- Lock the screen when you leave. Log out of shared devices.
- Keep devices encrypted where the hospital can do so (EC).

Key point: Most breaches start with a stolen or shared login.

Step 3. Review access every quarter.

- The IT lead and line managers review the list of users and their access.
- Remove access that is no longer needed. Remove access the same day a person leaves.
- Record the review date and the changes.

Key point: Access that is never reviewed grows until no one knows who can see the records.

Step 4. Monitor and log access.

- Keep logs of access to electronic records where the system allows.
- Check unusual access (for example, records of patients not under the person's care) each month.

Key point: Logs show who looked at a record, which is essential when a breach is suspected.

Step 5. Keep paper records secure.

- Store paper records in locked cabinets with controlled keys.
- Track removal of records from the store.
- Destroy paper records only through the approved disposal process.

Key point: Paper breaches happen through records left on desks and in cars.

Step 6. Report any breach at once.

- Report to your line manager and the data protection lead immediately, using DIG-SOP-001.
- Do not try to investigate alone or delete anything.

Key point: Early reporting limits harm and is required by the breach procedure.

10. Decision points

- If a breach is confirmed to affect many patients, the chief executive decides on notification to the regulator and to patients, as the law requires (EC).

11. Special situations

Situation	Action
Remote working	Use only approved devices and connections. No health information on personal devices unless the IT lead approves it (EC).
Third-party systems	Contracts must set security duties and breach notice periods (EC).

12. Escalation

- Breaches go to the data protection lead at once, and to the chief executive the same day.

13. Monitoring

Measure	Target	Frequency	Owner	If not met
Access reviews completed each quarter	100%	Quarterly	IT lead	Escalate to chief executive
Access removed the same day a person leaves	100%	Monthly sample	HR lead	Review and correct
Breaches reported within 24 hours of discovery	100%	Monthly	Data protection lead	Review of reporting delay

14. Records

Record	Kept in	Retention
Access review record	IT file	the period set by the facility’s records policy years
Breach log	Data protection file	the period set by the facility’s records policy years

15. Training

- All staff are trained in information security at induction and yearly (EC).
- IT and data protection staff receive specialist training (EC).

16. Related documents

ID	Title	Use
DIG-SOP-001	Patient Data Breach Response Procedure	Used when a breach occurs
DIG-FRM-001	Breach Response Test Record	Test record
REC-POL-001	Records Management and Retention	Retention and disposal
SOP-087	Confidentiality Policy (generic)	Confidentiality duties
SOP-108	Privacy Standard (generic)	Privacy duties

17. Evidence

Reference	Note
E-006	ASF Policy Framework v1.2. Adapted.
E-009	ASF Expert Committee consensus. Password, encryption and logging rules to be set by the IT lead and checked against national data protection law.

18. Change history

Version	Date	What changed	Approval
1.0	the date of approval	First version adapted from ASF Policy 37 and 71	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

- **Records, Confidentiality and Data Protection** (T-11)
- Security Protocols & Incident Response (SEC-01)

References

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

Download this document as PDF

Download this document as an editable Word file