Standard operating procedure (SOP) · DIG-SOP-001 · Version 1.1 · Approved by the ASF Expert Committee

Supports: 2A.4

At a glance

- Contain: stop the access or loss if it is safe to do so. Do not delete anything.
- Report to the data protection lead and your line manager at once.
- The data protection lead assesses the breach within 24 hours and records it.
- Decide, with the chief executive, whether the regulator and affected patients must be told.
- Review the cause and change the controls within 30 days.
- Stop and get help straight away if: the breach is still happening, or information is at risk of being sent further. Contain it first.

1. Purpose

To make sure any breach of patient information is contained, assessed, reported where required, and used to strengthen controls [EC].

2. Scope

Applies to	Everyone who discovers, reports or handles a suspected breach
Locations	All sites, systems and paper records
When	As soon as a breach or suspected breach is found
Does not apply to	Routine errors with no disclosure, which are handled under the incident policy but are also recorded here

3. Definitions

Term	Meaning
Breach	Unauthorised access, loss, disclosure or change of health information
Containment	Action to stop further harm, such as disabling a login or recovering a document

Breach team	The data protection lead, IT lead, the relevant service head and the chief executive or delegate

4. Background

Speed matters in a breach. Containment and early reporting limit the harm to patients. The law may require notification within set times, which must be confirmed for the country (EC).

5. Responsibilities

Role	Responsibility	Competence
Person who discovers the breach	Contains if safe; reports at once	Induction
Data protection lead	Leads the assessment; keeps the breach log; advises on notification	Data protection competence
IT lead	Secures systems; preserves logs; recovers data	IT security
Chief executive	Decides on notification to regulator and patients	Executive leadership

6. Materials and equipment

Item	Requirement	Condition
Breach report form	Date, time, what, who, how found	Complete
Breach log	Current	Updated for each breach

7. Safety

- Do not forward or copy the information to investigate.
- Do not contact the affected patient before the breach team has agreed the message.

8. Before you start

- Know who your data protection lead and IT lead are, and how to reach them out of hours.

9. Procedure

Step 1. Contain the breach.

- If safe, stop the access: log out, disable the account, or secure the paper record.
- Do not delete messages, files or logs.
- Note the time you found the breach and what you did.

Key point: Containment limits harm. Deletion destroys the evidence.

Step 2. Report at once.

- Tell your line manager and the data protection lead immediately, by phone if needed.
- Complete the breach report form within 24 hours.

Key point: The clock for notification starts when the facility knows. Early reporting protects the facility as well as patients.

Step 3. Assess the breach within 24 hours.

- The data protection lead records what information was involved, how many patients, what harm could result, and whether it was accidental or deliberate.
- Preserve system logs and emails.

Key point: The assessment decides what must be done next.

Step 4. Decide on notification.

- The breach team and chief executive decide whether the regulator and affected patients must be told, and by when.
- Record the decision and the reasons.

Key point: Notification decisions must be recorded, even when the decision is not to notify.

Step 5. Tell the affected people.

- Where notification is needed, give the patient a clear, honest account: what happened, what information, what they can do, and who to contact.
- Record the date and method.

Key point: Patients are owed the truth, given clearly and promptly.

Step 6. Learn from the breach.

- Carry out a root-cause review (INC-SOP-001) within 30 days.
- Change the controls, training or access that failed, and record the action.
- Record the closure on the breach log.

Key point: A breach that does not change anything will happen again.

10. Decision points

- If the breach involves a criminal act, report to the police through the chief executive, after the containment step.

11. Special situations

Situation	Action
Breach by a member of staff	Follow the disciplinary procedure after the assessment. Do not prejudge the outcome.

12. Escalation

- Serious breaches go to the chief executive and the governing body at the next meeting, or sooner if urgent.

13. Monitoring

Measure	Target	Frequency	Owner	If not met
Breaches reported within 24 hours	100%	Each breach	Data protection lead	Review of reporting delay
Breaches assessed within 24 hours	100%	Each breach	Data protection lead	Escalate to chief executive
Root-cause reviews completed within 30 days	100%	Monthly	Data protection lead	Escalate

14. Records

Record	Kept in	Retention
Breach report form	Data protection file	the period set by the facility’s records policy years
Breach log and root-cause review	Data protection file	the period set by the facility’s records policy years

15. Training

- Breach response is covered in induction and yearly training (EC).
- The breach team is exercised yearly through DIG-FRM-001 (EC).

16. Related documents

ID	Title	Use
DIG-POL-001	Information Security and Access Control Policy	Source of access rules
DIG-FRM-001	Breach Response Test Record	Yearly test
INC-POL-001	Incident Reporting and Management	Breach also logged as an incident

17. Evidence

Reference	Note
E-009	ASF Expert Committee consensus. Notification timing must be confirmed against national law before approval.

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

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

References

- 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