PelvicPhysio

Office 19139
182-184 High Street North
London E62JA
| info@pelvicphysiolondon.com | 07838 053 867

DATA BREACH RESPONSE PLAN

Version: 1.0 | Date: April 2026

1. What Is a Data Breach?

A personal data breach is any incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Examples include:

- Sending patient information to the wrong email recipient
- Paper consent forms lost, stolen, or seen by an unauthorised person
- A device containing patient data lost or stolen
- Google Workspace email account hacked or compromised
- Patient records accidentally destroyed before their retention period

2. Your 72-Hour Legal Obligation

Under UK GDPR Article 33, you must report certain breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of them. You must report if the breach is likely to result in a risk to individuals' rights and freedoms.

ICO breach reporting: ico.org.uk/for-organisations/report-a-breach | 0303 123 1113

3. Step-by-Step Response

Step 1: Contain the Breach

- Stop the breach from continuing or spreading immediately
- If a device is lost/stolen — change your Cliniko and Google Workspace passwords immediately and enable a remote wipe if possible
- If a Google Workspace email was sent to the wrong person — contact them immediately, ask them to delete it, and log the incident
- If paper consent forms are lost — retrace steps and inform anyone who may have found them

Step 2: Assess the Breach

- What data was involved? (Names, clinical notes, contact details?)
- How many patients are affected?
- What is the likely harm to those patients? (embarrassment, discrimination, identity theft?)

- Was the data encrypted or otherwise protected? (Cliniko data is encrypted at rest; Google Workspace emails are encrypted in transit)
- Has the data been recovered?

Step 3: Report to the ICO (if required within 72 hours)

- Report if: the breach involves sensitive health data, affects multiple people, or poses risk of harm
- You do NOT need to report if: the breach is unlikely to result in risk (e.g., encrypted device recovered quickly)
- When in doubt — report. Failure to report can result in larger fines than the breach itself
- ICO self-assessment tool: ico.org.uk/for-organisations/report-a-breach

Step 4: Notify Affected Patients (if high risk)

- If the breach is likely to result in HIGH risk to patients, you must notify them directly
- Do this without undue delay — aim within 72 hours
- Tell them: what happened, what data was involved, what you are doing about it, who they can contact

Step 5: Document Everything

- Complete the Breach Log below regardless of whether you report to the ICO
- Record: date/time breach discovered, nature of breach, data involved, likely consequences, actions taken
- Keep this record for at least 3 years

4. Breach Log

Date/Time Discovered:	
Date/Time Breach Occurred (if known):	
Nature of Breach:	
Data Involved:	
Number of Patients Affected:	
Likely Consequences:	
Actions Taken to Contain:	
Reported to ICO? (Yes/No/Not required):	
ICO Reference Number (if reported):	

Patients Notified? (Yes/No/Not required):	
Lessons Learned / Changes Made:	

5. Key Contacts

- ICO Report a Breach: ico.org.uk/for-organisations/report-a-breach
- ICO Helpline: 0303 123 1113
- Your professional insurer (notify them of any breach or ICO investigation)
- Your professional body (e.g., CSP, HCPC — check their breach notification requirements)