Data Breach under GDPR

Definition

1) Destruction – when personal data no longer exists in a form that can be used by the controller – Availability breach
2) Loss – when data still exists but the Data Controller has lost access to it or control of it – Availability breach
3) Damage – where personal data has been altered, corrupted or is not complete - Integrity breach
4) Unauthorised processing – any processing that is not lawful under GDPR – Confidentiality Breach
5) Unauthorised disclosure or sharing of personal data – Confidentiality Breach

n.b. a breach under GDPR involves personal data that prevents the controller processing under Article 5 of the GDPR

Process

1) All data breaches will be assessed individually to determine the possible consequences of the breach. If they involve any of the following they should be reported to the ICO and possibly the patient
   a) Loss of control of the data
   b) Limitation of their rights
   c) Identity theft or fraud
   d) Damage to reputation
   e) Loss of confidentiality of data
   f) Financial loss
   g) Unauthorised reversal of pseudonymisation
   h) Economic or social disadvantage

2) If the breach is assessed NOT to have affected an individuals rights and freedoms it should not be recorded but should be logged and actioned appropriately
3) A breach that needs to be reported to the ICO should be completed within 72 hours by the Data Controller after having implemented appropriate measures to assess the nature of the breach
4) It is the responsibility of every data processor to report a breach (all staff are data processors) under Article 33(2) immediately
5) If the breach is highly likely to affect the rights and freedoms of an individual it needn't be reported to the data subject

   A copy of the reporting form for the ICO is available shared drive/GDPR/Data breaches