INFORMATION SECURITY BREACH

What is an information security breach?

'**A personal data breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service".**

A personal data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorized use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organization who holds it.

Procedure:
If you become aware of a data breach or a potential risk to confidential information:

- Assess if you can immediately avert the breach - for example : patient information left in public areas – remove the information.
- Immediately contact the DATA PROTECTION OFFICER (Emma Streater) or Operations manager (Tina Potts)
- Write an account, to the best of your ability, of the data breach: paying attention to the following:
  - What type of data is involved?
  - How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
  - If data has been lost or stolen?
  - How many individuals' personal data are affected by the breach?
  - Who are the individuals whose data has been breached?

Pass all information to the SIRO and Operations manager for immediate investigation.