POLICY 21

POLICY ON INFORMATION GOVERANCE, DATA PROTECTION & CALDICOTT STANDARDS

WHO MUST ABIDE BY THIS POLICY?

A24Group – Locum Doctors

THE PURPOSE OF THIS POLICY:

In 1997 the Caldicott Committee, chaired by Dame Fiona Caldicott, issued a report on the protection of personally identifiable information within the health services. This report identified standards, which began to be implemented in the Health Service in 1998. In 2000, the government decided that these standards should be extended to "*Councils with Social Service Responsibilities",* and this process is now under way. This leaflet gives a summary of the Information Governance, Data Protection & Caldicott Principles and the responsibilities of all staff.

The Information Governance, Data Protection & Caldicott Standards are based on the Data Protection Act 1998 principles and again are set out in the form of Principles.

POLICY CONTENT:

Information Governance, Data Protection Caldicott Principles

1. Justify the purpose for which the information is needed.
2. Only use personally identifiable information when absolutely necessary.
3. Use the minimum personal identifiable information possible – if possible use an identifier number rather than a name.
4. Access to the information should be on a strict need to know basis.
5. Everyone should be aware of his/her responsibilities to respect client's confidentiality.
6. Understand and comply with the law. The most relevant legislation is the Data protection Act 1998, the Police & Criminal Evidence Act 1984 and the Human Rights Act 1998.

Some Do's and Don'ts of Data Protection

- **Do** be aware that any recorded information about an individual should be protected – this includes notes diaries and message books.
- **Don't** think that comments which you make will only be for your eyes only individuals have the right to access information kept about them by making a Subject Access Request.
- **Do** inform clients of their rights under the Data Protection Act 1998,
- **Don't** leave information unattended on your desk.
- **Do** only share information with your Team Manager.
- **Don't** share passwords and ensure passwords are used.
- **Do** make sure that you log out of your computer when you are not using it, even if you only leave your desk for a few minutes.
- **Don't** gossip about cases or individuals, if you do have to discuss cases openly, always ensure clients remain anonymous?
- **Do** take care when sending fax or email correspondence and where applicable retain a receipt.
- **NEVER** leave files or information in the car, on the bus or when working from home, ensure that information is not accessible to anyone other than **YOU**. You have a Personal Liability under the Data Protection Act 1998, you will only protect yourself if you protect clients information.

End of policy

