DATA PROTECTION POLICY

Summary

NHS 24 is fully committed to compliance with the requirements of the Data Protection Act 1998, which came into force on the 1st March 2000. NHS 24 will therefore follow procedures that aim to ensure that all employees, contractors, agents, consultants, partners and other trusted third parties who have access to any personal data held by or on behalf of NHS 24, are fully aware of and abide by their duties and responsibilities under the Act.

DOCUMENT CONTROL			
Owner:	Associate Medical Director/Information Governance Manager		
Document Control:	Version 1.0		
Date Live From:	Final		
Review/Approval Group:	IGSG/NCGG		
Last Reviewed:	January 2011		
Review Due/Cycle:	2 Years		
DOCUMENT CHANGE LOG			
Version	**Author**	**Date**	**Comment**
V0.1	A Morton	Dec '10	Draft
V1.0	A Morton	Jan '11	Final approved by IGSG 18.01.11

1. Statement of policy

1.1. In order to operate efficiently, NHS 24 collects and uses information about the people with whom it works. These may include members of the public, current, past and prospective employees, patients, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

1.2. NHS 24 regards the lawful and correct treatment of personal information as mandatory to its successful operations and to maintaining confidence between the organisation and those with whom it carries out business. NHS 24 will ensure that it treats personal information lawfully and correctly.

1.3. To this end NHS 24 fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

2. The principles of data protection

2.1. The Act stipulates that anyone processing personal data must comply with Eight Principles of good practice. These Principles are legally enforceable.

2.2. The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

2.3. The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and ”sensitive” personal data.

2.4. Personal data is defined as, data relating to a living individual who can be identified from:

2.4.1. that data, or
2.4.2. that data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

2.5. Sensitive personal data is defined as personal data consisting of information as to:

2.5.1. Racial or ethnic origin;
2.5.2. Political opinion;
2.5.3. Religious or other beliefs;
2.5.4. Trade union membership;
2.5.5. Physical or mental health or condition;
2.5.6. Sexual life;
2.5.7. Criminal proceedings or convictions.

3. Handling of personal/sensitive information

3.1. NHS 24 will, through appropriate management and the use of strict criteria and controls:-
3.1.1. Observe fully conditions regarding the fair collection and use of personal information;
3.1.2. Meet its legal obligations to specify the purpose for which information is used;
3.1.3. Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
3.1.4. Ensure the quality of information used;
3.1.5. Develop a retention policy to determine the length of time information is held;
3.1.6. Take appropriate technical and organisational security measures to safeguard personal information;
3.1.7. Ensure that personal information is not transferred abroad without suitable safeguards;
3.1.8. Ensure that the rights of people about whom the information is held can be fully exercised under the Act. These include:

3.1.8.1. The right to be informed that processing is being undertaken;

3.1.8.2. The right of access to one's personal information within the statutory 40 calendar days;
3.1.8.3. The right to prevent processing in certain circumstances;
3.1.8.4. The right to correct, rectify, block or erase information regarded as wrong information.

3.2. In addition, NHS 24 will ensure that:

3.2.1. There is someone with specific responsibility for data protection in the organisation;
3.2.2. Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
3.2.3. Everyone managing and handling personal information is appropriately trained to do so;
3.2.4. Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
3.2.5. Queries about handling personal information are promptly and courteously dealt with;
3.2.6. Methods of handling personal information are regularly assessed and evaluated;
3.2.7. Performance with handling personal information is regularly assessed and evaluated;
3.2.8. Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

3.3. All staff including Board Members are to be made fully aware of this policy and of their duties and responsibilities under the Act.

3.4. All managers and staff within NHS 24's directorates will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

3.4.1. Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
3.4.2. Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
3.4.3. Individual passwords should be such that they are not easily compromised.

3.5. All contractors, consultants, partners or other trusted third parties will:

3.5.1. Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of NHS 24, are aware of this policy and are fully trained in and are aware of their

duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between NHS 24 and that individual, company, partner or firm;

3.5.2. Allow data protection audits by NHS 24 of data held on its behalf (if requested);

3.5.3. Indemnify NHS 24 against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

3.6. All contractors who are users of personal information supplied by NHS 24 will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by NHS 24.

4. Implementation

4.1. NHS 24 has a Caldicott Guardian who is the Clinical Director with corporate responsibility for Information Governance. The Clinical Director/Caldicott Guardian has designated responsibility for Information Governance to the Associate Medical Director and day to day management for data protection lies with the Information Governance Manager. The Information Governance Manager in conjunction with the Information Security Manager will also have overall responsibility for:

4.1.1. The provision of cascade data protection training, for staff within NHS 24.

4.1.2. For the development of best practice guidelines.

4.1.3. For carrying out compliance checks to ensure adherence, throughout the organisation, with the Data Protection Act.

5. Notification to the Information Commissioner

5.1. The Information Commissioner maintains a public register of data controllers. NHS 24 is registered as such.

5.2. The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

5.3. To this end the Information Governance Manager will be responsible for notifying and updating the Information Commissioner of the processing of personal data.

5.4. Any changes to the register must be brought to the attention of the Information Governance Manager immediately and notified to the Information Commissioner within 28 days.