Data Protection Act policy

professional standards authority

Document Control

Version Control

Version	Status	Description of Version	Date Completed
1.0	agreed	Data Protection Act Policy	24/11/08
1.1		Updated for changes from CHRE to Professional Standards Authority.	October 2012
1.1		Under review	2016

1. Purpose

1.1 This document sets out our policy for ensuring the Professional Standards Authority for Health and Social Care (the Authority) acts in accordance with the Data Protection Act 1998.

1.2 It is the Act in the UK that explains the rights and responsibilities of those dealing with personal data. All staff are contractually bound to comply with the Act and other relevant Authority policies.

1.3 This policy should be read in conjunction with:

- Removing documents and IT containing personal and sensitive data policy
- Protecting personal and sensitive data policy
- Data Protection Act – Subject Access Request policy.

2. Introduction

What is the DPA?

2.1 The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for specific and lawful purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the individuals' rights
- Secure
- Not transferred to other countries without adequate protection.

2.2 Secondly, it provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

Satisfaction of the principles

2.3 In order to meet the requirements of the eight principles, we will:

- Observe fully the conditions regarding the fair collection and use of personal data.
- Meet our obligations to specify the purpose for which data is used.
- Collect and process appropriate personal data only to the extent that it is needed for the Authority to exercise any of the functions conferred on it by or under any enactment. Where necessary we will to seek express consent to process the data.
- Ensure the quality of the personal data used. All staff are responsible for ensuring that personal data is kept up to date and accurate, as far as is reasonably practicable in compliance with the Authority's functions.
- Apply strict checks to determine the length of time personal data is held. We will need to keep some forms of information longer than others. All staff are responsible for ensuring that information is not kept for longer than necessary and we have record management policies to help staff manage their responsibilities.
- Ensure that the rights of individuals about whom personal data is held can be fully exercised under the Act. This includes ensuring that anyone who has a query about our data handling procedures or would like to make a subject access request knows how to do so and are dealt with courteously and appropriately.
- Take the appropriate technical and organisational security measures to safeguard personal data. These include ensuring that sensitive personal information is kept in locked filing cabinets or secure electronic drives with limited access rights and that everyone managing and handling sensitive and personal information understands their responsibilities for following good data protection practice. It also includes having secure processes for sending personal data internally and externally.
- Ensure that personal data is not transferred abroad without suitable safeguards.

Data Controller

2.4 The Authority is a designated data controller and we are registered with the Information Commissioner. The Governance and Compliance Manager is responsible for ensuring compliance with the Data Protection Act and implementation of this policy on behalf of the Chief Executive.

The Duty of Confidentiality

2.5 A duty of confidence arises when one person provides information to another in circumstances that brings in the obligation of confidence, for example, when a regulator passes on medical records to a member of staff.

2.6 The general principle by which staff should abide is that information which is held by the Authority relating to individuals should not be used or disclosed except in accordance with the Authority exercising any function conferred on it by or under an enactment or with the individual's consent. A lack of ability to understand the likely use and disclosure of information does not diminish the duty of confidence.

2.7 Staff should seek advice in cases of doubt and refer matters to a senior manager.

3. Information Sharing

General Position

3.1 Personal information will be obtained from regulators and other third parties in the course of the work which the Authority undertakes. Some of the information will be of an administrative nature and other information will be about a person's mental or physical health, or how they practise. Generally speaking, personal information which is obtained on an individual will be held in compliance with this and other relevant Authority policies.

3.2 Personal information should not be disclosed outside of the Authority unless:

- it is consistent with our policy on removal of documents and IT containing personal and sensitive data policy and the obligation of fair processing;
- it is necessary for the Authority to exercise any of the functions conferred on it by or under any enactment;
- it is otherwise lawful; or
- the data subject has given his/her consent to the disclosure.

3.3 When seeking consent from an individual, they must be informed of the extent of any disclosure and its implications. In all cases no more information will be disclosed than is necessary to achieve the purpose behind the disclosure. In any cases other than where the data subject has given his/her consent to the disclosure, the matter must be referred to a senior manager prior to disclosure of the data.

3.4 If a circumstance arises where any personal information is to be transferred outside the Authority in circumstances that are not covered by this part of the policy, then before any such transfer of information takes place a senior manager must be consulted. Under no circumstances is personal information to be transferred to a country or territory outside the European Economic Area without the authority of a senior manager so as to ensure that the relevant legal obligations have been met.

4. Enquires from the Media

4.1 Any requests for personal information by the media (press, television or radio) must be referred to a senior manager for consideration.

5. Breaches of confidentiality

5.1 Staff who identify possible breaches of confidentiality or risk of a breach must raise these concerns with their manager or other appropriate colleagues.

5.2 The Authority will treat breaches of confidentiality as very serious matters.

5.3 In any organisation, regardless of the size and nature of services there is the risk of loss due to fraud and corruption.

5.4 The Professional Standards Authority for Health and Social Care (the Authority) is committed to making sure that the opportunity for fraud and corruption is reduced to the lowest possible risk. Where there is the possibility of fraud, corruption bribery or other problems, we will deal with it in a robust and controlled manner.

5.5 An important part of this approach is having an anti-fraud and corruption strategy, which we will use to advise and guide Authority members and staff on our approach to the serious issues of fraud and corruption. This document provides an overview of our policy and includes a 'fraud response plan' which provides more detailed guidance on how to deal with fraud and corruption.

5.6 The main message is that the Authority expects all members, employees, consultants and contractors to be fair and honest, and to give us any help, information and support we need to deal with fraud and corruption.

5.7 The strategy set out in this document covers the following areas:

- our written rules
- how we expect our employees to behave
- preventing fraud and corruption
- detecting and investigating fraud and corruption
- training.