

CONFIDENTIALITY AND DISCLOSURE OF INFORMATION

INTRODUCTION

Accurate and secure personal health information is an essential part of patient care. The NHS Code of Practice on Protecting Patient Confidentiality (Scottish Executive 2003) states that NHS Scotland's goal is for a service that:

- Protects the confidentiality of patient information
- Commands the support and confidence of public, patients and all staff, students, volunteers and contractors working in or with NHS Scotland
- Complies with best practice
- Conforms with the law
- Promotes patient care, the running of care organisations and the improvement of health and care through new knowledge
- Works in partnership with other organisations and has clearly established and communicated protocols for sharing information

This goal is set within the context of the following legal framework:

- Statute law e.g. Data Protection Legislation, Human Rights Act 1998 Adults with Incapacity (Scotland) Act 2000
- The common law in Scotland on privacy and confidentiality
- Professional standards e.g. NMC code of professional conduct (2008)
- National and local policies and organisational standards Data Protection Policy

PRINCIPLES OF GOOD PRACTICE

A key document to refer to is the Data Protection Legislation (General data Protection Regulation), which describes seven principles for 'good information handling'. These seven principles and what this may mean in practice are detailed below:

Principle	What does this mean?
1. Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
2. Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Accuracy	Personal data shall be accurate and, where necessary, kept up to date

5. Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
6. Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
7. Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

This table was extracted from an example protocol for confidentiality, which can be viewed on www.show.scot.nhs.uk