Policies and Procedures

Staff should refer to their organisation's policies and procedures around information sharing, security, and confidentiality, of patient or service user information, and if in doubt speak to their manager or supervisor or relevant contact printed on this leaflet.

For further information please contact:

Tameside Hospital NHS Foundation Trust

Information Governance Team - Tel: 0161 331 6681/6936 or email:foi@tgh.nhs.uk

Tameside & Glossop Primary Care Trust

If you are a patient and would like to know more about how we use your information, please speak to the health professionals *(for example, your doctor)* concerned with your care. Staff should contact the IT Service Desk.

Pennine Care NHS Trust

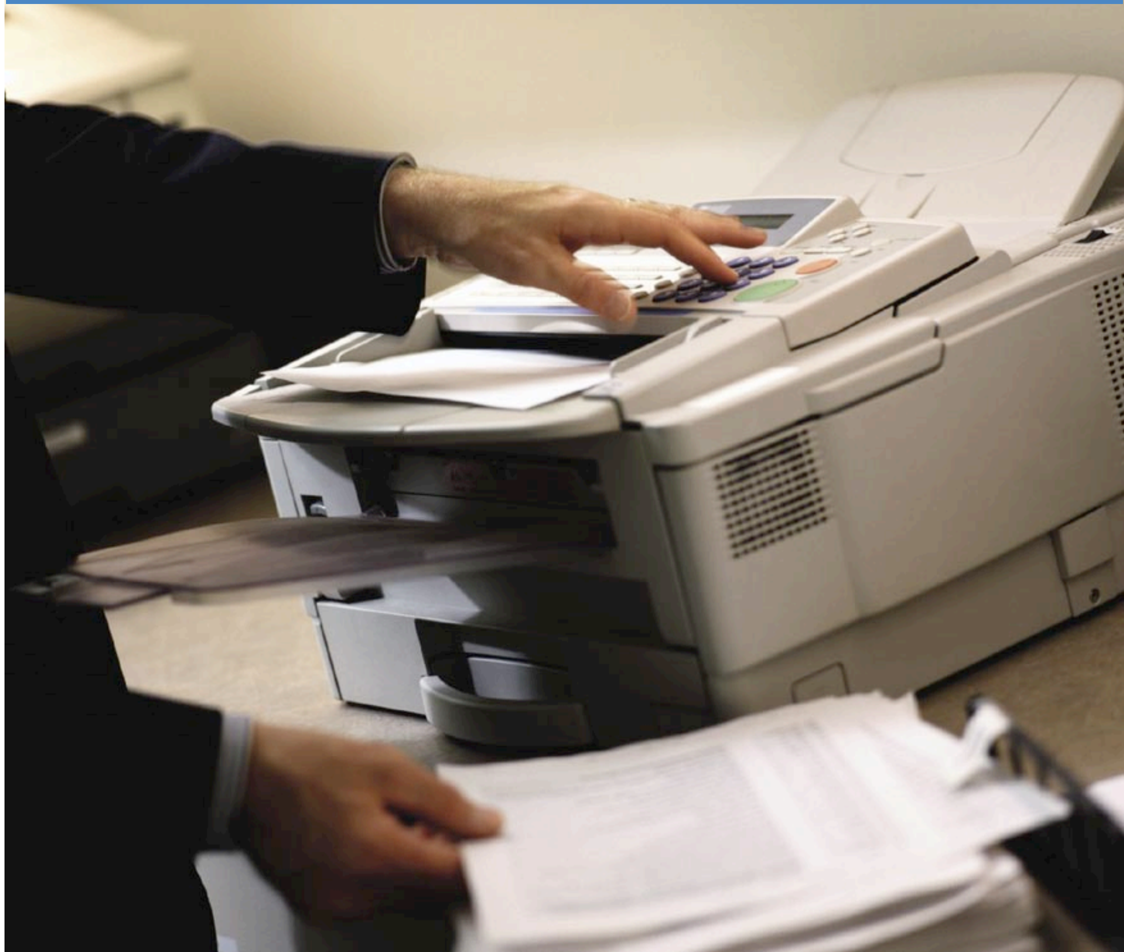
Tel: 0161 604 3000 or email:foi@penninecare.nhs.uk

Developed by the Tameside & Glossop Local Care Records Development Board.

Revision date: July 2009

Tameside Hospital NHS Foundation Trust
Tameside & Glossop Primary Care Trust
Pennine Care NHS Trust

General guidelines on sharing and taking care of personal information



General guidelines on sharing and taking care of personal information

These guidelines have been commissioned by the Tameside & Glossop Local Care Records Development Board for use jointly by the local NHS and Tameside Metropolitan Borough Council Social Care Departments. The guidelines complement, and do not conflict with existing policies, procedures and guidance around sharing and managing personal information within participating organisations. They serve to ensure consistency and to reinforce the standards around the sharing and use of personal information.

All of the following rules apply to the sharing of personal information about patients or service users with any individual or organisation and apply equally to computer and paper records. They also cover communication of information by all methods, including verbal.

Top Ten Principles – Patient/Service User perspective

1. *Personal information has to be recorded in some written form to help others in the team know what's already been done*
2. *Information may be passed on to others to help provide care*
3. *Information will only be passed to others who need to know it to do their job*
4. *Only personal information that is needed will be passed on*
5. *Individuals have a right to restrict who gets their information, but this may affect the safety of the care provided*
6. *Patients/service users can always ask questions and share their concerns about what is recorded and shared*
7. *Individuals have a right of access to their information – each organisation has procedures and forms to fill in to ask for it*
8. *Personal information is treated by all health and social care agencies in strictest confidence*
9. *Personal information can be used to support audit and checking the quality of care, without your consent*
10. *Personal information will not be shared for other purposes, except where required by law, without your consent*

Top Ten Principles – Staff perspective

1. *Store all personal information securely when not being used, not leaving information open or accessible to view by unauthorised persons*
2. *Limit access to personal information to those staff who need to know to do their job, ensuring that the person to whom you are giving the information has a legitimate right to receive that information*
3. *Never deliberately access or change information if you do not have legitimate right of access to that information in the course of your job*
4. *Respect the patient's wishes about restricting access to their information*
5. *Take care to ensure that information forwarded by you to another person is as secure as possible, and that it is addressed correctly*
6. *Dispose of all personal information in a secure manner – see your local policies*
7. *Take care not to access the records of members of your family or friends (or indeed yourself) even if you are the legal guardian or next of kin, unless you need to do this as part of your job*
8. *Keep passwords to computers and systems confidential, never letting anyone else know them, e.g. by writing them down and leaving them where others can see.*
9. *Never use another person's password or user ID to access a system, and always log off computerised systems at the end of your user session so that other people cannot use your password to access that system*
10. *You should also refer to your professional codes of conduct, and the "Joint guidance on use of IT equipment and access to patient data" issued by the Department of Health, General Medical Council and Information Commissioner. Although directed at the NHS, the principles are generally applicable.*