GENERAL PRACTICE SOLUTIONS
EXPERTLY NAVIGATING SUCCESS

71-75 Shelton Street, London, WC2H 9JQ | www.generalpracticesolutions.net
020 8865 1942 | enquiries@generalpracticesolutions.net

CONFIDENTIALITY CODE OF CONDUCT

INTRODUCTION
The aims of the policy are to ensure:

- All information held by GPS and client providers concerning service users is confidential, whether held electronically or in hard copy.
- Other information about the GPS (for example its financial matters, worker records) is confidential.
- All staff associates are aware of their responsibilities for safeguarding confidentiality and preserving information security.
- All workers understand their responsibilities when sharing information with both NHS and non-NHS organisations.

Staff will, by necessity, have access to such confidential information from time to time

APPLICABILITY
The policy applies to all employees and associates, and also applies to other people who work at GPS e.g. self-employed workers, temporary workers and contractors – collectively referred to herein as 'workers'.

POLICY

- All information about service users is confidential: from the most sensitive diagnosis to the fact of having visited a client provider or being registered at a client provider. This includes information about service users families or others associated with them.
- Confidential information may not be health related. It can include anything that is private and not public knowledge.
- Workers should limit any discussion about confidential information to only those who need to know within for GPS.
- Only the minimum amount of necessary information should be disclosed.
- The duty of confidentiality owed to a person under 16 is as great as the duty owed to any other person.
- Workers must not under any circumstances disclose patient information to anyone outside of the client provider, except to other health professionals on a need-to-know basis, or where the service user has provided written consent.
- Workers must not under any circumstances disclose other confidential information about the GPS to anyone outside the organisation unless with the express consent of your Customer Relations Manager (CRM).

- All service users can expect that their personal information will not be disclosed without their permission (except in the most exceptional circumstances when disclosure is required when a person is at grave risk of serious harm).
- Where disclosure of information is required which is non-routine in nature the patient will, where possible, be fully informed of the nature of the disclosure prior to this being released.
- Where the decision is made to disclose information, the decision to do so must be justified and documented.
- Person-identifiable information must not be used unless absolutely necessary – anonymised data should be used wherever possible.
- Workers must be aware of and conform to the requirements of the Caldicott recommendations.
- Electronic transfer of any confidential information, once approved by their CRM must be transmitted via the NHSnet. Workers must take particular care that confidential information is not transmitted in error by email or over the Internet.
- Workers must not take data from the client providers computer systems (e.g. on a memory stick or removable drive) off the premises unless authorised to do so by their CRM.
  Where this is the case, the information must be kept on the worker's person at all times while travelling and kept in a secure, lockable location when taken home or to another location. All information should be held on an encrypted disc, or pendrive.
- Workers who suspect a breach of confidentiality must inform their CRM.
- Any breach of confidentiality could be considered a serious disciplinary offence and will be investigated in line with the GPS disciplinary procedure.
- Workers remain bound by a requirement to keep information confidential even if they are no longer affiliated with GPS. Any breach, or suspected breach, of confidentiality after the worker has left the GPS employment will be passed to GPS lawyers for action.

RESPONSIBILITIES OF GPS WORKERS

All health professionals must follow their professional codes of practice and the law. This means that they must make every effort to protect confidentiality. It also means that no identifiable information about a service user is passed to anyone or any agency without the express permission of that service user, except when this is essential for providing care or necessary to protect somebody's health, safety or well-being.

All health professionals are individually accountable for their own actions. They should, however, also work together as a team to ensure that standards of confidentiality are upheld, and that improper disclosures are avoided.

Additionally, GPS as Employers:

- Are responsible for ensuring that everybody commissioned by the GPS understands the need for, and maintains, confidentiality.
- Have overall responsibility for ensuring that systems and mechanisms are in place to protect confidentiality.
- Have vicarious liability for the actions of those working for GPS – including health professionals and non-clinical staff.

Standards of confidentiality apply to all health professionals, administrative and ancillary staff - including receptionists, secretaries, managers, cleaners, and maintenance staff - who are bound by contract to maintain confidentiality.

They must not reveal personal information they learn in the course of their work to anybody outside of the client provider without the service user's consent. Nor will they discuss with colleagues any aspect of a service users' attendance at the client provider in a way that might allow identification of the service user, unless to do so is necessary for the service users care.

IF DISCLOSURE IS NECESSARY

If a service user or another person is at grave risk of serious harm that disclosure to an appropriate person would prevent, the relevant health professional can take advice from colleagues within GPS, of from a professional / regulatory / defence body, to decide whether disclosure without consent is justified to protect the service user or another person. If a decision is taken to disclose, the service should always be informed before disclosure is made, unless to do so could be dangerous. If possible, any such decisions should be shared with another member of the client providers team.

Any decision to disclose information to protect health, safety or well-being will be based on the degree of current or potential harm, not the age of the service user.

CONFIDENTIALITY GUIDELINES

- Be aware that careless talk can lead to a breach of confidentiality – discuss your work only with authorised personnel, preferably in private.
- Always keep confidential documents away from prying eyes.
- Verbal reporting should be carried out in private. If this is not possible, it should be delivered in a volume such that it can only be heard by those for whom it is intended.
- When asking for confidential information in circumstances where the conversation can be overheard by others, conduct the interview in as quiet and discreet a manner as possible and preferably find somewhere private for the discussion.
- There may be times when a young person attends on their own. On such occasions it may not be appropriate to enquire further as to the reason for the visit.
- Precautions should be taken to prevent telephone conversations being overheard.
- Information should be given over the telephone only to service user or, in the case of children, to their parent or guardian. However, care must be taken to ensure that the duty of confidentiality to a minor is not breached, even to a parent.
- The duty of confidentiality owed to a person under 16 is as great as the duty owed to any other person.
- When using computers, unauthorised access should be prevented by password protection and physical security such as locking the doors when offices are left unattended. Where possible, VDU screens should be positioned so they are visible only to the user. Unwanted paper records should be disposed of safely by shredding on site and computer files on hard

or floppy disks should be wiped clean when no longer required.

- If unsure about authorisation to disclose, or a person's authorisation to receive confidential information, always seek authorisation from your CRM before disclosing any personal health information.