

# Staff Confidentiality Policy and Agreement

## Introduction

The aims of the policy are to ensure:

- all information held at the practice about patients is confidential, whether held electronically or in hard copy
- other information about the practice (for example its financial matters, staff records) is highly confidential
- staff will, by necessity, have access to confidential information as required to perform their expected roles.

## Applicability

The policy applies to all employees and partners, and also applies in principle\* to other people who work at the practice e.g. self-employed staff, temporary staff and contractors – collectively referred to herein as ‘workers’.

\*Practices should ensure that workers who are not employees are aware of and agree to abide by this policy in principle. In cases calling for action, and if the worker is an employee of another organisation (e.g. an agency), the worker's employer should also be involved

## Policy

- Staff must not under any circumstances disclose patient information to anyone outside the practice, except to other health professionals on a ‘need to know’ basis, or where the patient has provided (written or recorded) consent.
- All information about patients is confidential; including being registered at or having visited the practice. This includes information about patients’ families or others associated with them.
- Staff must not under any circumstances disclose other confidential information about the practice to anyone outside the practice unless with the express consent of Dr Sarah Hawxwell or Mr Sunil Gupta. Staff must limit any discussion about confidential information only to those who need to know within the practice.
- The duty of confidentiality owed to a person under 16 is as great as the duty owed to any other person.
- Staff must be aware of and conform to the requirements of the Caldicott recommendations.
- All patients 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.
- Electronic transfer of any confidential information, once approved by Mr Sunil Gupta, must be transmitted via the NHSnet or another agreed secure transfer of

patient identifiable data. Staff must take particular care that confidential information is not transmitted in error by email or over the Internet.

- Staff must not take data from the practice's computer systems (e.g. on a memory stick or removable drive) off the premises unless authorised to do so Mr Sunil Gupta.
- Staff who suspect a breach of confidentiality must inform their line manager immediately.
- Any breach of confidentiality will be considered as a serious disciplinary offence and may lead to dismissal.
- Staff remain bound by a requirement to keep information confidential even if they are no longer employed at the practice. Any breach, or suspected breach, of confidentiality after the staff member has left the practice's employment will be passed to the practice's lawyers for action

## Responsibilities of Practice Staff

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 patient is passed to anyone or any agency without the express permission of that patient, 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, Penrose Health as Employers:

- are responsible for ensuring that everybody employed by the practice 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 in the practice – including health professionals and non-clinical staff (i.e. those not employed directly by the practice but who work in the surgery).

Standards of confidentiality apply to all health professionals, administrative and external staff - receptionists, secretaries, cleaners and maintenance staff are bound by contracts of employment to maintain confidentiality. They must not reveal personal information they learn in the course of their work, or due to their presence in the surgery, to anybody outside the practice without the patient's consent. Nor will they discuss with colleagues any aspect of a patient's attendance at the surgery in a way that might allow identification of the patient unless to do so is necessary for the patient's care.

## If Disclosure is Necessary

If a patient 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 the practice, or from a professional / regulatory / defence body, in order to decide whether disclosure without consent is justified to protect the patient or another person. If a decision is taken to disclose, the patient should always be informed before

disclosure is made, unless to do so could be dangerous. If at all possible, any such decisions should be shared with another member of the practice 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 patient.

## Gender Recognition Act 2004

The 2004 Gender Recognition Act (GRA) makes it a criminal offence to disclose an individual's transgender history to a third party without their written consent if that individual holds a Gender Recognition Certificate (GRC).

Patients do not need to show a GRC or birth certificate in order for the GRA 2004 to be in effect, so it is best practice to act as though every trans patient has one. This means always obtaining a trans patient's written consent before sharing details about their social or medical transition, sometimes also called gender reassignment, with other services or individuals.

This includes information such as whether a patient is currently taking hormones or whether they have had any genital surgery, as well as information about previous names or the gender they were given at birth. Consent should always be obtained before information relating to the patient being trans is shared in referrals and this information should only be shared where it is clinically relevant, e.g. it would be appropriate when referring a trans man for a pelvic ultrasound but not when referring him to ENT.

## Staff Confidentiality Agreement

(Must be signed by every staff member)

### Declaration

I understand that all information about patients held by Penrose Health is strictly confidential, including the fact of a particular patient having visited the surgery.

I will abide by the confidentiality guidelines set out above.

I have read the Staff Confidentiality Policy above and fully understand my obligations and the consequences of any breach of confidentiality. I understand that a breach of these obligations may result in dismissal.

I understand that any breach, or suspected breach, of confidentiality by me after I have left the practice's employment will be passed to the practice's lawyers for action.

If I hold a professional qualification and my right to practice depends on that qualification being registered with a governing body, it is my responsibility to have read and understood their advice on confidentiality.

Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

## Confidentiality guidelines:

- Careless talk can lead to a breach of confidentiality – discuss only with colleagues as needed, ideally in private.
- Always keep confidential documents in locked drawers/cupboards when not in use
- Verbal reporting should be carried out in private. If this is not possible, it should be discussed at a volume such that it cannot be heard by other parties
- 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.
- Precautions should be taken to prevent telephone conversations being overheard.
- Information should be given over the telephone only to the patient 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.
- Duty of confidentiality to a person under 16 is as great as the duty to any other person.
- When using computers, unauthorised access should be prevented by password protection and physical security such as locking the door when an office is left unattended. Where possible, VDU screens should be positioned so they are visible only to the user. Paper records should be disposed of safely by confidential waste shredding and computer files to be wiped clean when no longer required.