PARKBURY HOUSE SURGERY

PARKBURY HOUSE SURGERY
ST PETERS ST
ST ALBANS HERTS AL1 3HD **www.parkburyhouse.nhs.uk**

Telephone: St Albans (01727) 851 589
Fax: St Albans (01727) 854372
e-mail: **parkburyhhouse.info@hnhs.net**

Confidentiality

In any health organisation, confidentiality is a high priority. Everyone at Parkbury House Surgery must respect all information held about others. Such personal information belongs first and foremost to the patients or employees it relates to. All members of staff at Parkbury House have signed confidentiality and IT security policy along with an induction covering confidentiality.

All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 1998 and, for health and other professionals, through their own professions Code/s of Practice. This means that employees are obliged to keep any personal identifiable e.g. patient and employee records information strictly confidential. It should be noted that employees also come into contact with non-person identifiable information which should also be treated with the same degree of care e.g. business in confidence information, financial reports.

Confidential information can be anything that relates to patients, staff, their family or friends, including attendances at appointments, staff qualifications, training, disciplinary records and information about volunteers, agency staff and contractors, however stored. For example, information may be held on paper, CD, USB sticks, computer file or printout, laptops, mobile phones, digital cameras, video, photograph or even heard by word of mouth. However person-identifiable information should not be stored on removable media unless it is encrypted to NHS standards. Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Disclosing information

Care must be taken to check that enquirers (such as insurance companies/solicitors) have a legitimate right to have access to the information that they ask for, so that information is only shared with the right people. Never give out information on patients or staff to persons who do not “need to know”. When a request comes in for

copy of medical records a signed declaration must be provided by the patient to confirm they are happy for their notes to be copied and sent to the relevant party. It is important to consider how much information is needed before disclosing it and only disclose the minimal amount necessary. It is best practice to phone the solicitors/insurance company to find exactly what information they need. On some occasions they have requested only a computer print out to be sufficient. Providing a whole medical file is generally needless and is likely to constitute a breach of confidence.

Information can be disclosed:

- With the patient's written consent for a particular purpose.
- On a need to know basis if the person receiving the information is involved in the patient's treatment and requires the information for clinical reasons.
- When the information is required by law or under a court order. In this situation staff must discuss with their manager staff before disclosing.
- In Child Protection proceedings if it is considered that the information required is in the public or child's interest.
- Where disclosure can be justified for another purpose. This is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime.
- All staff members have a duty of confidence and must take care to keep person-identifiable information private and not to divulge information accidentally.
- Do not give any results/information to anyone apart from the patient. Please ensure you have completed checks i.e. name, date of birth and address when giving out results or other information.
- For results and information on the under 16's the parents **only** are authorised to obtain this information. Ensure the parents can confirm their child's date of birth, name and address. Be extra cautious if giving sensitive information regarding contraception/sexual health information to parents. Please refer to the doctor if you are unsure.

Staff must not:

- Discuss patients in public places or where they can be overheard particularly in the reception area where there is a lot of patient traffic.
- When on the phone to a patient you should not give any personal identifiable information, ideally you should ask the patient to confirm this to you particularly when at the reception area. You must not disclose the patient's name or any other identifiable details.
- Leave any medical records or confidential information lying around unattended; this includes telephone messages, computer printouts, faxes and other documents.
- Leave a computer terminal logged onto a system where personal and sensitive information can be accessed, unattended. You must log off Vision when on a break or when ending your shift and remove your smart card.

- Passwords must be kept securely and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information.

- You must not provide any form of patient data via email unless to a secure email address (nhs.net). Patient information such as test results, NHS numbers and medical information is to be obtained by coming into the surgery or calling the surgery. Emailing information to patients personal email addresses is not considered secure and could breach confidentiality and security.

Confidentiality is an obligation for all staff. Any breach of confidentiality, inappropriate use of health or staff records or abuse of computer system is a disciplinary offence, which could result in dismissal or termination of your employment contract.
It is compulsory for all employees to sign a confidentiality agreement statement.

CONFIDENTIALITY AGREEMENT STATEMENT

You will not at any time during your attachment (except as so far as is necessary and proper in the course of your attachment) or afterwards disclose to any person any information as to the practice, business, dealings, accounts, finances, trading, software, know-how or affairs of the employer or any of the employer's clients, patients, prospective patients, distributors, suppliers or persons, firms or companies otherwise connected with the employer, patients or otherwise howsoever.

All notes, memoranda, records and other documents of Parkbury House and in your possession are and shall remain the property of Parkbury House and shall be handed over by you to Parkbury House from time to time on demand and, in any event on termination of your attachment. No data is to be removed or down loaded from the clinical system of Parkbury House without prior permission of the Practice Manager or his deputy in his absence.

You should understand that any breach of this agreement will constitute a very serious offence for which your attachment maybe terminated with immediate effect. Should you breach this agreement after your attachment has ended, the practice may take legal action against you.

Whilst this document is confidential the Practice may be obliged to disclose the document, or parts of it, to an applicant making a request under the Freedom of Information Act.

I have read and understood clearly the accompanying confidentiality document as well as the agreement statement and if there is any information I am unsure about I will seek further advice from My Line Manager.

Print Name _____

Date _____

Sign _____