Lockwood Surgery

Confidentiality & Consent Policy

A. Confidentiality Notice

This document and the information contained therein is the property of Lockwood Surgery.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Lockwood Surgery.

C. Document Revision and Approval History

The purpose of the protocol is to set out the obligations for all working at Lockwood Surgery either staff or contractors concerning the confidentiality of information held about patients and Lockwood Surgery.

This protocol will be reviewed annually to ensure that it remains effective and relevant.

CONFIDENTIALITY is the cornerstone of good practice, in the surgery or in any other location. Patients have the right to expect that information learned during the course of professional duties will not be disclosed.

All staff and contractors are obligated to:

- Always endeavour to maintain patient confidentiality
- Not discuss confidential information with colleagues without patient consent (unless it is part of the provision of care)
- Not discuss confidential information in a location or manner that allows it to be overhead
- Handle patient information received from another provider sensitively and confidentially
- Not allow confidential information to be visible in public places
- Store and dispose of confidential information in accordance with the GDPR Action May 2018, Data Protection Act 1998 and the Department of Health's Records Management Code of Practice (Part 2). In short anything with patient information should be shredded.
- Not access confidential information about a patient unless it is necessary as part of their work
- Not remove confidential information from the premises unless it is necessary to do so to provide treatment to a patient, the appropriate technical safeguards are in place and there is agreement from the information governance lead (Practice Manager) or Caldicott Guardian.
- Contact the PM immediately if there are barriers to maintaining confidentiality
- Report any loss, inappropriate storage or incorrect disclosure of confidential information to the PM

Casey Hancock
Practice Manager
June 2018

It is expected that members of staff or visitors (either contractors or external healthcare workers) will comply with the law and guidance/codes of conduct laid down by their respective regulatory and professional bodies.

In the General Practice environment every possible action should be taken to stop the possibility of confidential information about a patient being overheard by anyone for whom it is not intended. Patients in the waiting area should not be able to deduce name or circumstances of call being received or made. Likewise patients making a call to us should not be able to hear confidential information from staff and patients at the desk. Information of any kind must not be given out over the telephone to any one other than the patient, including their close family members. Schools, Insurance Companies, Social Services etc. should be referred to the Practice Manager. If there is any doubt about the identity of a caller, ask for date of birth, or check the telephone number and ring the patient back asking to speak to them in person. If there is any doubt, check with afore mentioned staff.

If a patient at Reception indicates they would like to speak privately, an empty room should be found for them. Also to afford privacy at the desk for a patient, other waiting patients will be asked to queue behind a barrier with notice asking for co-operation. Receptionists should be discreet and ensure surgery lists, visit books, patient records and computer screens are out of sight of the waiting room.

Doctors wishing to communicate with reception during surgery should be mindful of patients at Reception Desk and if the situation required discussion of a confidential nature ask the receptionist to ring them back or use patients' computer numbers. A doctors computer screen should be cleared of the previous patients records before the next patient enters the consulting room.

For computer confidentiality each member of staff has their own password, which should not be divulged to anyone else either in or out of the practice. For security reasons, staff should not keep a written record of their password. Staff is allowed different levels of access to the computer system according to their positions in the organisation. Any breach of these access levels without authorisation from the Practice Manager will be treated as a breach of confidentiality.

All information kept on computer and in manual records is covered by the GDPR Act 2018. Full policies covering this particular Act can be found under S/Practice Policies/GDPR

This gives the patient the right to see computer held information pertaining to them and have the ability to challenge and claim compensation in some cases if the information is found to be incorrect. Patients requesting a copy of information held on computer about them should be given a medical summary printout after confirming with one of the doctors that this will be acceptable. If a patient wishes to see their medical records, this can be arranged after the practice manager has examined all contents of record and confirmed the appropriateness of allowing patient to read the consultant's letter to the doctor. The request should be in writing from the patient and given 28 days for the PM to examine all contents.

Every member of staff or contractor/visitor is entirely under the same constraints of confidentiality.

Young Persons

The duty of confidentiality owed to a person under the age of 16 is as great as the duty owed to any other person. To this effect, doctors and nurses are asked to record when a young person under the age of 16 attends the surgery alone; and to make arrangements for discreet follow up on results etc where relevant. Reception staffs will double check for young persons 16 or under before disclosing information to parents etc.

Improper Disclosure

Such confidential information should be protected from improper disclosure when received, stored, transmitted or disposed of. If information is not kept confidential:

- Patients may be reluctant to or refuse to disclose any information. This may impede diagnosis or management.
- Patients may refuse to attend at all
- The patient has the freedom to decide which personal information should be made public or semi-public.

Doctors are responsible for breaches of confidentiality by those staff whom they employ and that a breach of such confidentiality is a serious disciplinary matter and could lead to dismissal.

Information Disclosures

When a decision is taken to disclose information about a patient to a third party due to safeguarding concerns/public interest, the patient should always be told and asked for consent before the disclosure unless it would be unsafe or not practical to do so (for safeguarding issues please refer to safeguarding policy).

In the circumstances that consent can not be sought then there must be clear reasons and necessity for sharing the information.

Disclosures of confidential information about patients to a third party must be made to the appropriate person or organisation and in accordance with the principles of the Data Protection Act 1998 the NHS Confidentiality Code of Practice and the GMCs Good medical practice.

Exceptions to Confidentiality

Essentially all information should be kept confidential. There are some exceptions that a doctor may observe:

- In the public interest - to avoid someone being exposed to serious harm or death
- Where the duty of care to an individual overrides the duty of confidentiality to another
- Where there is a legal obligation to do so e.g. notification of infectious disease.

A doctor must reveal to the police:

A suspected terrorist - and can reveal on enquiry the identity of a driver in an incident where there has been personal injury.

The police do not have access to clinical records or appointment books. If the police

require other information they should seek a judicial order under the Police and Criminal Act 1984

Consequences to breaching confidentiality

The potential consequences of breaching confidentiality:

- An NHS complaint
- A complaint to the G.M.C. –serious professional misconduct
- A civil action
- For staff-possible instant dismissal for gross misconduct

It seems it is usually easier to defend a failure to inform than it is to defend an inappropriate breach of information.

This protocol is subject to the provisions set out in the legislation and guidance listed below.

GDPR Action May 2018
Data Protection Act 1998; The Information Commissioners' Office guide to data protection
The Department's Code of Practice for Records Management (Part 2)
Human Rights Act 1998
The Common Law Duty of Confidence
Access to Health Records Act 1990
Confidentiality: NHS Code of Practice 2003
NHS Care Record Guarantee 2009

Any updates to the above original legislation will be found on the website.

Casey Hancock
Practice Manager
June 2018

All Staff and Suppliers will be required to sign the Practices Confidentiality Statement, as detailed below.

Staff Confidentiality Agreement in line with GDPR May 2018

I understand that all information about patients held by Lockwood Surgery is strictly confidential.

I shall never disclose any information about a patient to anybody other than Lockwood employees, the patient's consented person or next of kin (again only if authorised by the patient). Any other disclosure will only be on the request of the Partners or Practice Manager

I will abide by the terms of the Confidentiality Policy and GDPR Privacy Policy.

I have read the Confidentiality Policy 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 premises 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: _____

I also agree to undertake all training on Information Governance and GDPR on Bluestream within the next 2 months.

Casey Hancock
Practice Manager
June 2018