Peninsula Medical Practice

Confidentiality, information sharing and the use of Internet, mobile phones and electronic equipment

The Health Centre

GRANGE OVER SANDS

LA11 7DJ

Fairfield Surgery

FLOOKBURGH

LA11 7JY

Practice Policy Document No. 1

v1.2

March 2014

Contents

Confidentiality

All clinical staff are bound by their professional code of ethics issued by their relevant licensing body, such as the General Medical Council, The Nursing and Midwifery Council and the Royal Pharmaceutical Society.

All practice staff must respect the confidentiality of information acquired in the course of professional practice relating to a patient and the patient's family. Such information must not be disclosed to anyone without the consent of the patient or appropriate guardian unless the interest of the patient or the public requires such a disclosure.

Information concerning particular patients can be shared within a health care team unless a patient objects. Specific consent for information to be shared to allow treatment is not required as patients have implied consent by joining the practice list. However, it is good practice to make sure that patients are aware that personal information about them will be shared within the health care team, unless they object, and the reasons for this.

The partners also require that all staff maintain the confidentiality of any information concerning the management or business dealings of the practice and any personal information concerning their work colleagues.

Responsible person

The data protection custodian and Caldicott guardian for the practice is the Practice Manager.

Use of Anonymised Data

If information for the purposes of audit, research, public health purposes, teaching and training or to plan the delivery of healthcare is required, this information should be kept to the minimum necessary. It may only be passed to other organisations or agencies in anonymised form.

Patient Identifiable Information

You must adhere to the Caldicott principles which govern access to patient identifiable information. These are:

1. You must be able to justify the purpose of the information being shared
2. Only share such information when absolutely necessary
3. Share the minimum information that is required

Access to patient identifiable information is on a strict need to know basis.

You are responsible for personal information about patients and must make sure it is effectively protected against improper disclosure at all times both within and outside the practice.

Computer Systems

Wherever possible work should be prepared and stored on the practice's clinical system. Protection of this data will be covered by the practice's security policy.

If you need to work on a portable computer system, for example a laptop, or take any patient identifiable material away from the practice on a portable computer or memory device to work on, then that computer or memory device must be encrypted to a standard approved by the practice's data security manager.

If you need to take printouts of the patient record in order to visit patients away from the practice these must be returned promptly to the practice. They should be disposed of safely once they are no longer required.

Disclosing Patient Identifiable Information in the Public Interest

If you feel that you must disclose information in the public interest you must consult with the one of the practice's clinical partners.

Information sharing

The 'Seven Golden Rules' of information sharing are set out in the government guidance, Information Sharing: Pocket Guide . This guidance is applicable to all professionals charged with the responsibility of sharing information, including in child protection scenarios:

1. The Data Protection Act is not a barrier to sharing information but provides a framework to ensure personal information about living persons is shared appropriately.
2. Be open and honest with the person/family from the outset about why, what, how and with whom information will be shared and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice if you have any doubt, without disclosing the identity of the person if possible.
4. Share with consent where appropriate, and where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent, if, in your judgement, that lack of consent can be overridden by the public interest – you will need to base your judgement on the facts of the case.
5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.
6. Necessary, proportionate, relevant , accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely.
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Conversations with and referrals to outside agencies should be recorded under an appropriate Read code.

Email

The only email system that should be used for practice business is NHSmail. This is an accredited system meeting the Government's 'RESTRICTED' security standard meaning that the whole NHSmail service, not just the link between systems, is fully secure.

Local Government email systems are not guaranteed to have similar levels of security and confidential patient sensitive information (unless the address contains a .gsi.gov.uk suffix) and must not be sent to Social Service or other Local Authority Departments unless subjected to additional encryption.

Referral forms and confidential information can be sent by FAX to a designated Safe Haven number within a Social Services or Local Authority Department.

Use of electronic equipment and access to the internet

You must always act responsibly with regard to internet, electronic and telecommunications equipment (including use of mobile phones), and use them in a professional, lawful and ethical manner.

Inappropriate types of sites

Accessing or downloading data from inappropriate websites, (e.g., pornographic websites or emails, racist, sexist or gambling websites or emails, sites promoting violence and illegal software) at any time is forbidden and may lead to disciplinary proceedings.

Permitted personal use

Reasonable personal use of the internet by the partners and employees of the Peninsula Medical Practice is permitted, as long as it does not interfere with the performance of normal duties, and remains in accordance with the stated IT policies, including those on acceptable use of equipment and use of email. Such limited, personal use of the internet should only be conducted when it doesn't interfere with the user's ability to carry out their normal duties, e.g. outside normal working hours.

You should bear in mind that when visiting an internet site, information identifying your PC may be logged. Therefore any activity you engage in via the internet may affect the Practice Team. Practice employees are strongly discouraged from using their Practice email address when using public web sites for non-practice purposes. This must be kept to a minimum as it results in you, and the Practice, receiving large amounts of unwanted email (spam).

Breaches of Practice Policy

All breaches of practice policy will be considered on their merits and treated sympathetically if inadvertent. However, breaches of patient confidentiality will be taken very seriously, and if patient identifiable information is released deliberately or negligently then this will usually result in dismissal.

Review

This policy will be reviewed within three (3) years of its implementation, or sooner if any significant changes in best practice are advised by the Department of Health.

Declaration

This policy will be binding upon all employees of the Peninsula Medical Practice from the 1st October 2012.

We, the partners, have reviewed and accepted this policy.

Dr Diane Ruell
Dr Michael Bunter
Dr Nick Gent

1st October 2012

Reviewed and amended

1st March 2014

NG

Appendix (1): confidentiality declaration

Peninsula Medical Practice

Confidentiality, information sharing and the use of internet, mobile phones and electronic equipment

I confirm that I have received a copy of Peninsula Medical Practice policy concerning confidentiality, information sharing and the use of internet, mobile phones and electronic equipment.

I confirm that I have read and understood this policy document.

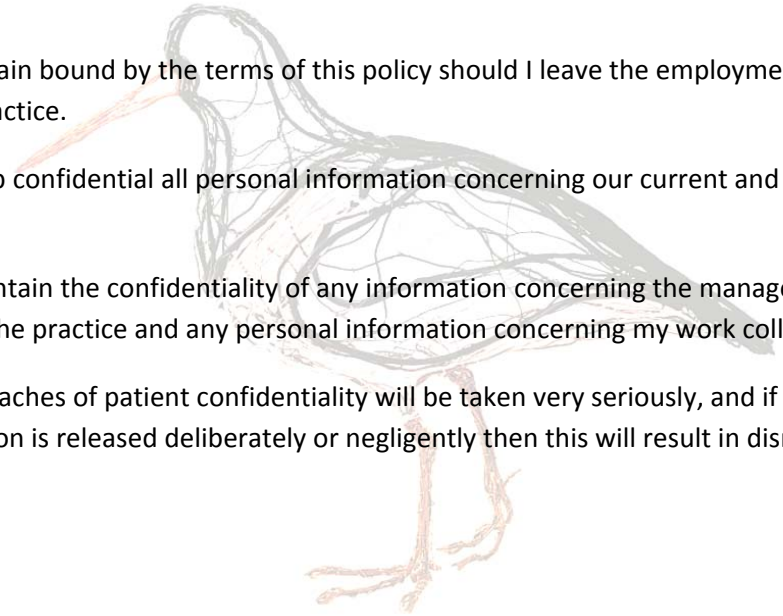
I agree to abide by the terms of this policy during my period of employment by the Peninsula Medical Practice.

I agree that I will remain bound by the terms of this policy should I leave the employment of the Peninsula Medical Practice.

I agree that I will keep confidential all personal information concerning our current and past patients.

I agree that I will maintain the confidentiality of any information concerning the management or business dealings of the practice and any personal information concerning my work colleagues.

I understand that breaches of patient confidentiality will be taken very seriously, and if patient identifiable information is released deliberately or negligently then this will result in dismissal.



Name _____

Signature _____

Date _____

Appendix (2): keyholder declaration

Peninsula Medical Practice

Keyholder declaration

As part of your duties with the Peninsula Medical Practice you are provided with a key to access the premises and codes to disable and enable the alarm systems.

I understand that the key and alarm codes are provided to me only for the purposes of accessing the premises of the Peninsula Medical Practice for those purposes agreed in my job description.

I agree to keep the key provided to me safe at all times and not to affix any label to that key that indicates that it gives access to the premises of Peninsula Medical Practice.

I agree not to allow any copies of the key to be made.

I agree not to make any record of the alarm codes provided to me, or to give these codes to any unauthorised persons.

I will report the loss of the key, or any disclosure of the alarm codes to a person who is not a member of the practice staff, to a senior member of the management team immediately I discover such a loss or disclosure.

I agree to return the key immediately should I leave the employment of Peninsula Medical Practice.

Name _____

Signature _____

Date _____