

ALL GENERAL PRACTITIONERS

Date 28th November 2008
Your ref
Our Ref AL/LK
Enquiries to Lynn Kennedy
Direct Line 01698 245014
Fax 01698 245008
E-mail Alan.Lawrie@lanarkshire.scot.nhs.uk
Lynn.kennedy@lanarkshire.scot.nhs.uk

Dear Colleague

**Information Governance and Data Protection
Statement of policy, actions to be taken and recommendations for General Practice**

You will be aware of recent Scottish Government Guidance on the use of removable media – particularly where this is used for the storage and distribution of person identifiable data.

The Caldicott Guardian in NHS Lanarkshire, then Dr Dorothy Moir, recently corresponded with all directly employed staff setting out a revised set of procedures in response to that guidance. Essentially this involved the ‘locking down’ of USB Ports for the purposes of writing data to memory sticks and the reinforcement of good practice in the use of other transportable data media and devices.

Whilst the different status of Independent Contractors with regard to data protection is recognised, we would wish to make practices aware of their obligations under the Data Protection Act 1998 and to advise that a recent change in the Law states that in certain circumstances, data misuse and/or reckless disregard for the Act is a criminal offence with a maximum fine of £1 million.

NHS Lanarkshire in collaboration with other NHS Boards is currently reviewing its policies and has taken the opportunity over recent months to provide guidance through the communication of ‘top tips’ on security and confidentiality in the staff bulletin and other media. Anyone not familiar with this guidance should contact Alistair Stewart, Information Governance Manager (alistair.stewart@lanarkshire.scot.nhs.uk, Telephone 01698 245219) who will be happy to provide advice to practices.

In light of the recent guidance, there are a number of specific issues that we would wish to bring to your attention. These recommendations have been implemented for NHS Lanarkshire staff, and I would propose that they be adopted as best practice and policy for independent practitioners also.

-2-

These are:

- 1) Patient identifiable information must never be routinely transmitted by email other than between NHS mail users – if used in emergencies or contingencies, such data should be secured within a password protected file
- 2) Everyone who has been issued with Laptop Computers must have NHS Lanarkshire encryption software installed on these laptops.
- 3) New guidance and policy on the use of mobile/portable computing devices has come into effect and requires that;
 - a. The electronic transmission of person identifiable data to external agencies, home or personal computers and email accounts is prohibited – this includes the transfer of data on USB memory sticks, compact discs, MP3 Players and mobile phones with data storage capacity.
 - b. If it is genuinely necessary to hold NHS Lanarkshire or practice information on a portable device then such use must be risk assessed and approved and recorded by the Data Controller in the practice

In addressing these issues, NHS Lanarkshire will undertake a number of specific actions on behalf of practices:

1. All memory sticks should be securely encrypted in accordance with the recent guidance. In this regard, NHS Lanarkshire will provide practices with the facilities to securely encrypt all memory sticks. This work will be programmed during December and all practices are encouraged to participate in this work. Practices who do not wish to adopt the NHS Lanarkshire corporate approach will be required to provide details of how they will otherwise comply with the extant guidance.
2. Anyone who uses a laptop computer must contact the IT Helpdesk to have them encrypted. This has been an ongoing programme of work. . Practice staff who require their laptop encrypted must contact the IT Helpdesk immediately to have the necessary software loaded. Users who are not asked to install a username and password on a blue screen when they switch on their computer do not have the necessary level of encryption
3. Unencrypted data media must be securely destroyed. Practices wishing to avail themselves of the secure destruction service that is in place should contact the IT Helpdesk

-3-

4. NHS Lanarkshire is currently assessing the risks associated with the use of handheld computers and will issue guidance in due course. In the meantime, practices are advised to ensure that such devices are securely stored and use password protection facilities
5. Blackberry devices supplied by the NHS Lanarkshire IM&T Department are encrypted to the appropriate level and are password protected.

Whilst practices operate beyond the jurisdiction of the Caldicott Guardian and NHS Lanarkshire Information Governance Committee, the Board would wish to be assured that all practices are operating securely and with reference to prevailing NHS Scotland policies and guidance. In this regard GPs, through the Local Medical Committee, will become members of the Information Governance Committee and to participate fully in the development work that is underway to enhance levels of information security across all areas of activity.

I trust that you will recognise the benefits of participation in this essential work so that we can assure the public that the data that they entrust us with is securely and appropriately managed.

Yours sincerely



Alan Lawrie
Director
South Lanarkshire CHP



Dr Bill Martin
General Practitioner
eHealth Clinical Lead



Dr Colette Maule
Lanarkshire Local
Medical Committee