NHS Fife

Appendix 4

CONFIDENTIALITY PROCEDURE
GOOD PRACTICE GUIDE

DOCUMENT CONTROL		POLICY NO.	GP/C9-4
Policy Manual/System General, e.g. Clinical		General	
Author (original policy)	Una Hill	Version No.	V1
Reviewer (policy review)	Una Hill	Implementation Date	July 2012
Signed by Responsible Director	C. Bowring	Next Review Date	01072013

GOOD PRACTICE GUIDE

Privacy Markings

1. Privacy markings are used to protect information which might lead to a breach of confidentiality, administrative or personal embarrassment if it were disclosed without authorisation.

2. Where information being transmitted **internally** relates to an identifiable person or contains other confidential information, it should be placed in a buff envelope. The envelope must be marked with an appropriate privacy marker such as "Private and Confidential" or "Medical – In Confidence". The envelope must be sealed and show the full name, title and address of the intended recipient.

3. An exception is made for departments (such as NHS Fife Laboratories) who use specially designed envelopes clearly alerting the privacy status.

4. Where the information being sent internally is particularly sensitive, the sender may exercise discretion and double envelope.

5. Where information is being sent **externally** it will be at the Line Manager's discretion to apply a privacy marking. It is unlikely that such correspondence will require to be double enveloped.

.

6. The category. **"MANAGEMENT IN CONFIDENCE"** also relates to Freedom of Information legislation. This must not be used routinely, but must be applied if the "public interest " test as set out in the FOI(S)A is applicable. Staff must seek advice from the FOI Lead (Head of Corporate Services) on the designation of documents in this way: it is anticipated that this will be rarely applied.

The following also relate to privacy markings:

(a) The information protected by a privacy marking must be conveyed only to those who need to know it.
(b) Files and papers for internal transfer which are not passed directly by hand must be sent under cover showing the privacy marker. Transit envelopes must not be used for this purpose.
(c) Files and papers bearing privacy markers must be kept under lock and key when not in use.

(d) Papers no longer required and not meriting preservation as permanent records must be destroyed by shredding or other agreed disposal method. Staff must refer to the Guidance for Retention and Destruction of Health Records (H5).

Confidential Communications Opened in Error

7. Where a confidential communication is opened in error by someone other than the addressee,
contact must be made with the addressee and an explanation given. The Line Manager must also be informed. Where such information is confidential, staff must uphold confidentiality in accordance with their contract of employment. An incident form (IR1) must be completed.

8. Where an email is opened in error by someone other than the intended recipient, contact must
be made with the intended recipient and an explanation given. The Line Manager of the person who opened the email must also be informed. An Incident Form (IR1) must be completed.

Postal Arrangements

9. Whether being sent by internal or external mail, staff must ensure that a named recipient is stated on the envelope along with the correct, full address with postcode where appropriate. This will apply to both confidential and routine information.

10. The Royal Mail Recorded Delivery service may be used when sending original items such as patient casenotes, business contracts and other confidential business or patient information. This will not apply to routine correspondence with patients.

11. Where appropriate, confidential information such as letters to patients from Health Care Professionals and personal communications to staff must be sent in sealed envelopes marked “Private and Confidential” or have these words visible as part of the template.

Faxing of Confidential information

12. Faxes of confidential information are particularly vulnerable to interception, and in principle confidential, clinical or personal information must not be sent by fax. As NHSmail provides national email and fax facilities and is the only service endorsed for email communications, it is recommended this mode of transmission is used where possible. If this is not possible then NHS Fife Safe Haven Policy GP/S4 (Procedure for operating fax machines) must be referred to.

Record Storage

13. Personal information as defined under the Data Protection Act, 1998 must be held securely and access limited solely to those who require access to perform their duties.

14. Sensitive information as defined under the Data Protection Act 1998 may not be shared in most circumstances without the person’s consent.

Confidential Conversations

15. Within the constraints of the clinical environment, all staff must make every effort to maintain confidentiality and utilise the facilities provided when possible. In clinical areas conversations must be held as discreetly as possible.

16. Within the public area, whether or not on NHS Fife premises, staff must maintain patient, client and staff confidentiality at all times.

17. NHS Fife is committed to promoting equality and diversity. Staff must therefore take steps to ensure confidentiality when communicating with someone with a sensory loss, such as hearing or visual impairment. Advice may be sought locally on Equality and Diversity and external agencies may be contacted when seeking advice about communicating confidential information with individuals with specific needs, e.g. individuals who are deaf or blind.

Sharing Information with Police

18. Staff must make themselves familiar with the NHS Fife Guidance for staff on Information Sharing with Police.

Requests for information over the telephone

19. Staff are professionally responsible for the information they divulge by telephone. Where the caller cannot be positively identified by answering security questions, or there is any doubt as to the validity of the request, the information should not be released. The caller's contact telephone number should be noted and further advice sought from the line manager.

Accessing Information

20. Staff must not:
    a. Access any patient, staff or management record (manual or electronic) whether confidential or routine when they have no authority to do so in the course of their duties.

    b. Access any records for their personal interest.

    c. Access their own health or personnel records without authorisation. Staff may apply to access such information under the Data Protection Act (1998)

    d. Remove confidential information from the workplace. In circumstances where staff are working on confidential information external to their workplace, express consent must be sought from the Line Manager. The relevant IT policies must be referred to.

Transportation of Health Records

21. Where staff need to transport healthcare records it is their responsibility to ensure this is done safely. The records must be securely packaged in sealed/lockable containers and transported in the boot of the vehicle. Confidential records must not remain in the vehicle when it is unattended. The staff member is responsible for ensuring no unauthorised access occurs whilst the records are in his/her possession.

An Equality & Diversity Rapid Impact Assessment has been completed for this procedure. No negative impacts have been identified.