A GUIDE TO GOOD PRACTICE AND PROCEDURES

This guide has been produced to support the policy by citing some examples of good practice in order that the provisions of the Policy can be translated into personal and departmental procedures. Common sense governs most daily activity, however risks might not always be identifiable when priority is placed on getting the job done. Remember ignorance is not an acceptable excuse for not respecting patient confidentiality.

CONFIDENTIALITY AT SOURCE

Thought should be given to all circumstances by which patient information is obtained:

By Telephone

It is common, when verifying information by telephone, to repeat details. Where this occurs in a public area, efforts should be made to anonymise any information being relayed back and limit the amount of detailed reference. It is therefore considered good practice to ask that the information be repeated to ensure that it was received correctly rather than the staff member personally repeating back within earshot of unauthorised personnel. What must be borne in mind is that, where patients/visitors/members of the public hear details of other patients, it can immediately undermine their trust in our standards of confidentiality and this, in itself, can be harmful to the delivery of care.

Leaving Messages

In order to ensure that the patient's right to confidentiality is maintained, messages should not be left on answer machines of shared telephones for example a landline at the patient's house. Messages can be left on the patient's mobile number if this is known.

Any messages should be clear and contain a name and phone number for the patient to contact if they have any questions.

If a patient has clearly asked for a message to be left then this should be recorded in the patient's record either electronic or paper.

In person

The best opportunity to confirm information is speaking directly with the patient, wherever practical staff seeking to approach patients with a set of questions should attempt to identify a facility for discreet interview. As well as this demonstrating our interest in protecting confidentiality, much more information can be obtained in the appropriate environment.

Reception staff will often find themselves unable to ask questions or escort patients to an interview room through their responsibility to be present on the reception desk. Where this is the case, the information being checked should be kept to a minimum. Reception staff should, if possible use an appointment card, or other document which has the patient details recorded on it, to confirm the patients identification by showing the card to the patient and asking them to confirm the details on the document. If this is not available then reception staff should ask the patient questions which can be answered by a 'yes' or 'no'. For example, checking the accuracy of address, the receptionist would ask 'Are you still at...?' then quote the street name without the number. This should be adequate to establish accuracy or otherwise.

In writing

Documents containing patient specific information should be considered confidential / legal documents and should be handled with this in mind. Where envelopes are marked 'Confidential' they should only be opened by the individual to whom they are addressed or by those carrying the appropriate authority to do so. Confidential documents should be stored securely when not in use and access to the documents restricted.

Fax

FAX CAN ONLY BE USED AS A BUSINESS CONTINUITY TOOL AND MUST NO BE USED AS A REGULAR MEANS OF TRANSFERING INDENTIFIABLE DATA.

If permitted to be used ensure –

When receiving fax transmissions of confidential information it is preferred that this is by prior arrangement and that the intended recipient be anticipating its arrival in order that the information does not fall into unauthorised hands and that receipt is confirmed. This is not necessary in designated fax 'safe havens' where restricted access to the area is normally operation. NHS Lothian has one 'safe haven' which is based here at Waverly Gate. Safe Haven fax machines need to have a degree of security, locked door and someone responsible for the information arriving and being dispatched. If any further Safe Havens are proposed they will have to be reviewed fully.. Where a fax is received without warning, a member of staff of appropriate authority should contact the sender advising of the future requirement to telephone with advance warning. It is in the sender's best interests to do this.

Email/Internet

We need to remember that the Internet is not secure. Some parts of the Internet are able to maintain the confidentiality and security required by the NHS, and expected of us from patients. Within the reference section of this document is a list of email addresses where it is safe to include patient identifiable

information. If you do send an email to an address, not on the list, e.g. AOL, Hotmail etc and all other commercial providers then this is not secure and cannot be regarded as confidential. You must remember that the NHS Code of Confidentiality requires that patient identifiable data should only be processed on NHS owned IT equipment. Taking patient identifiable information from one computer to a different computer i.e. to work at it on your home computer, is not authorised, and is a breach of patient confidentiality. It is therefore a breach of NHS Board policy and therefore subject to disciplinary action. Further information can be obtained in the Safe Email Transmission Standard operating procedure

The NHS Lothian Social Media Policy has been developed to provide clarification and remind all NHS Lothian employees of their responsibilities and accountability as an employee with regard to social media websites such as Facebook, Bebo, Twitter and Myspace.

For guidance on social media please see Using Social Media: Practical and ethical guidance for doctors and medical students.

The NMC also offer guidance for nursing staff on the use of social networks. It can be accessed at http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Social-networking-sites/

Advice for staff that is registered with the Health Professions Council can be found here http://www.hpc-uk.org/Assets/documents/100035B7Social_media_guidance.pdf

Managers can also access information from the Code of Conduct for NHS Managers.

Display equipment use – Best Practice

As part of NHS Lothian's Data Protection Policy it was agreed that NHS Lothian will ensure that:

"Methods of processing personal data are clearly defined and reviewed regularly to ensure best practice guidance is followed within the organisation"

This document relates to the use of display equipment in business or ward environments where patients or their visitors may have access.

1. Do not write personal information relating to treatment, race, age, sex, condition drug prescribing, address, other contact details or any other information which can be deemed 'personal', on any medium or visual aid which is on open view to the public or in a prominent position.

2. Only identify patients using surname and initial. In no circumstances use condition, visual appearance, dress or details which may be misunderstood as an identifier.

3. Consider carefully when placing wall mounted flat-screen televisions, whiteboards, display screens or notice boards, which may be used to hold sensitive information.
Encourage a 'safe haven' principle for these visual aids. A safe haven should be identified and clearly marked as 'staff only'. Computer monitors should face "in" to staff and not "out" meaning they could be viewed by patients or their visitors.

4. Where sensitive information is required to be held temporarily, such as messages to patients or employees, shift change information, managers should ensure procedures are in place to prevent disclosure to unauthorised persons.

STORAGE AND ACCESS

The primary tool for protecting the confidentiality of patient information is the healthcare record folder. Adherence to the filing requirements of the folder not only improves its confidential status but also, makes it easier to use. Healthcare records, which are not immediately required, should be returned to the appropriate records library/site where they can be easily located. Where documents are in isolation of the healthcare record, efforts should be made to locate the folder and make arrangements for the documents to be filed.

Storage Storing confidential information in general offices requires vigilance on the part of the occupants. Where possible, offices should be locked when unoccupied. As much consideration should be afforded to confidential information as to accessibility to personal belongings. Since many offices are subject to much coming and going, it might be beneficial to install keypad security. Risks would have to be assessed against cost, however healthcare record libraries should be fitted with a keypad entry system, which include self-closing hinges in addition to formal locks to be used when the department is closed.

Access Since 1991 legislation has existed that has provided for patients to view their records or to nominate someone to view them on their behalf. This provision requires careful monitoring in terms of validity, content of the record and guaranteed timescales for response. All requests for information should be referred to the Medical Records Manager who will process the required information within the terms of Data Protection Legislation. Further information is available from Access to health records policy

Research Purposes Requests for access to healthcare records for research purposes would normally require both the patients' and consultants' consent and those requesting records should be questioned to this effect where they do not provide any evidence of authorisation. Further information can be found in the Request for Case notes research and audit policy Research access to healthcare records held by Lothian Health Services Archive is governed by local policy under the Caldicott Guardian. Further information can be found at www.lhsa.lib.ed.ac.uk

Police Requests .The vast majority of patient contacts do not raise issues about public safety or the investigation of a crime. However, many health professionals, including those in the A&E Departments, minor injury clinics, and GP surgeries, may have contact with individuals involved in - or injured as a consequence of - crimes. While health professionals have a legal duty to provide confidential health care, the statutory provisions which govern this allow the sharing of information in appropriate circumstances to prevent or detect crime. Professional codes of

practice also recognise this kind of co-operation is of key importance, and is an expected part of the health professional's role. Further information is available from Information sharing between NHS Scotland and the police

Caldicott Guardian Each NHS organisation must have in post a senior person responsible for safeguarding the confidentiality of patient information. This person is known as the Caldicott Guardian. The Caldicott Review proposed 6 general principles that health and social care organisations should adopt when reviewing their use of client information:

1. Justify the purpose. Every proposed use or transfer of personally identifiable information within or from an organisation should be clearly defined and scrutinised, within continuing uses regularly reviewed by the appropriate guardian.
2. Do not use personally identifiable information unless it is absolutely necessary. Personally identified items should not be used unless there is no alternative.
3. Use the minimum personally identifiable information – where the use of personally identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identification.
4. Access to personally identifiable information should be in a strict need to know basis. Only those individuals who need access to personally identifiable information should have access to it.
5. Everyone should be aware of, their responsibilities. Action should be taken to ensure that, those using personally identifiable information are aware of the responsibilities and obligations to respect patient confidentiality.
6. Understand and comply with the Law. Every use of personally identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements (The Caldicott Guardian). Further information is available on the Information Governance pages of the intranet

Ethical Dilemma Issues associated with confidentiality are complex and health care professionals may face tensions between the requirement of patient confidentiality and facilitating patient care. Difficulties may arise where practitioners are faced with conflicting obligations within their ethical code. The NMC Code of Professional Conduct, Standards for Conduct, Performance and Ethics (NMC 2008) provides that each Registered Nurse, Midwife or Health Visitor must report to an appropriate person in the care environment, circumstances that could jeopardise safe standards of practice or circumstances in which safe and appropriate care for patients cannot be provided. See also General Medical Council (2009) Confidentiality: Protecting and Providing Information. Staff registered with HPC may find

additional information in Confidentiality – guidance for registrants (2008)

THE LEGAL/ETHICAL FRAMEWORK

There are three main areas of law that need to be observed within the scope of this Policy: The Human Rights Act 1998 (HRA); Data Protection Legislation and The Common Law on confidentiality (Common Law).

As a public authority, NHS Lothian is required to act in a manner compatible with the qualified rights conferred to citizens under the Human Rights Act.

Article 8, which states, "Everyone has a right to respect for his private and family life, his home and correspondence," is of particular relevance. Under this article, NHS Lothian must maintain the confidentiality of patient information and can only interfere with an individual's right to privacy under very limited circumstances.

Article 10 states that "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers," and is often used as a 'balancing act' against Article 8 rights. However, individuals cannot exercise their right of freedom of expression if the information they wish to express is received on the expectation that it will remain confidential.

Data Protection Legislation refers to processing personal data relating to living individuals, places a requirement on NHS Lothian and its employees to have appropriate technological and organisational measures in place to ensure that information is managed to ensure a patient's right of confidentiality. Data Protection Legislation also enables information to be appropriately passed onto partner agencies in cases of cause for concern such as Child Protection, and for the investigation of incidents and complaints by regulatory and law enforcement authorities.

The Common Law is not an Act of Parliament like HRA and Data Protection Legislation above; it has been built up from previous rulings and judgements made by the courts. As with HRA, the Common Law supports that the right to confidentiality is not absolute, but if breached without good reason is an offence. The Common Law treats information relating to both living and deceased patients in the same manner.

DISCLOSURE AND TRANSIT

Where requests for information are validated there are further measures to be taken to ensure the safe delivery and appropriate receipt of the information.

The golden rule concerning provision of access would dictate that disclosure should only be made in respect of facilitating the provision of health care to those who would be unable to provide effective treatment and care without that information.

Disclosure by Telephone

Staff will be requested to provide patient information over the telephone frequently and from a number of different sources. These may include fellow healthcare workers seeking information on a new admission or transfer and relatives enquiring about a patient. Information should be shared with another member of the healthcare team that is required by that member to carry out their duties, for example a handover to another clinical area or profession. It is not appropriate to divulge confidential information to members of the healthcare team that are not directly involved in that patients care. For example all members of the healthcare team should be aware that infection control measures are in place for specific patients, but they do not need to know a patient's past medical history or reason for admission.

The healthcare team will mainly consist of registered and unregistered nursing staff, medical staff and allied health professionals. However it may also include, but not be limited to, estate staff, administrative staff, portering staff, corporate staff and domestic staff.

Queries from friends and relatives can cause confusion for healthcare staff and steps should be taken to confirm the identity of the person on the phone. This can be done by asking the caller for details of the patient, including full name, date of birth and address. This will help to clarify that the caller is close to the patient. If possible staff should then obtain consent from the patient before giving out any information and ideally should allow the patient to talk to the caller. Staff should also request that only one member of the family phones the clinical area for information. This can reduce interruption for healthcare staff and reduce the risk of healthcare workers inadvertently breaching confidentiality.

In situations where a person telephones NHS Lothian seeking confidential information about an out patient, e.g. the date of an appointment or clarification of a medical query, NHS Lothian staff should phone the patient on the number that is recorded in either the Healthcare Records, or the Patient Administration System (e.g. Trak). This will allow the staff member to obtain consent from the patient and avoid any confusion. NHS Lothian staff should not telephone back on a number given by the caller or give out information without consent.

Healthcare staff should be aware that some patients may not want family members to know any details regarding their care and therefore should avoid giving out information. Even transferring a caller to the

patient's clinical area could be breach of confidentiality. Healthcare staff should check with the clinical area before transferring any calls through.

Disclosure Staff should attempt to limit the amount of information provided to that which was specifically requested. It is also worth considering information, which might not technically constitute health record information, e.g. medical reports, details of legal proceedings, these may not constitute part of the patient's record are still patient identifiable information. If an individual other than the patient is identifiable from the information, e.g. a member of the family, this person's right to confidentiality must be respected and any references should, therefore, be removed from view.

There are few circumstances where there is a specific need for the principal record to be provided and photocopies should be used where possible. Where records are required to transfer with patients from one hospital to another (out with NHS Lothian) it is preferred that the appropriate copied extract accompany the referring documentation rather than the entire healthcare record.

Transit Where confidential information is being transported by both internal and external mail, it is important to ensure that it is securely packaged and that the word 'Confidential' is clearly displayed. Where information is being sent to locations outwith those covered by the van service, recorded delivery should be utilised. Lockable, traceable, tamper proof bags should be used. Faxing information should only be done where there are guarantees that it is being received confidentially and this might require an advance telephone call.

Staff carrying records in cars It is acknowledged that staff are often required to transport patient information in their cars or on their person. Staff required to do this must use lockable cases/boxes for all records. Every other reasonable precaution should be taken when the person is in the car. At the end of the working day, all patient information must be returned to the practitioner's base or where the records are normally stored. In exceptional circumstances, which must be justifiable, where patient information cannot be returned to the practitioner's base or to where the record is normally stored, the practitioner must ensure that every reasonable precaution is taken to protect the information.

DISPOSAL

Items disposed of through general waste will eventually arrive at local landfill sites. It is possible therefore that confidential information discarded as general waste could become unintentional public information. There is, therefore, provision for confidential disposal of information.

Confidential Waste Paper

Opaque bags available for this located in almost every room or department. Bags to be secured by staff and uplifted by Facilities. Items sent for disposal and recycling with certificate of destruction provided for all loads sent.

Further information is available in the waste disposal policy.

Confidential IT Hardware All IT hardware should be disposed via eHealth.