POLICY ON CONFIDENTIALITY OF PERSONAL HEALTH INFORMATION

Author (s): Clinical Policy Group
Version: 2.1 April 2018
Status: Final TECHNICAL UPDATE
Date of Authorisation: April 2018
Key Words: Confidentiality
Authorised by: Information Governance Sub Committee
Review Date: April 2021 Comments:

ELEMENT	DESCRIPTION
Key Messages	1. The confidentiality policy exists to ensure that all patient information is treated with complete confidentiality and MUST NOT be divulged to anyone who does not have right to access that information. 2. Access to information on patients is restricted to those that have been given permission by the patient, except in circumstances outlined in this policy. 3. This policy applies to all information where the patient can be identified, and applies to all types of media where patient identifiable data is processed. 4. This policy applies to all staff employed by NHS Lothian, including agency and bank staff, all students, volunteers and agency and contractors working on behalf of NHS Lothian. 5. The policy can be found on the Homepage>Healthcare>Clinical Guidance Site.
Minimum Implementation Standards	All staff must sign a confidentiality statement in their contract of employment prior to commencing work for NHS Lothian. Confidentiality training will be provided as part of the mandatory induction program for new NHS Lothian employees. All staff must complete the eLearning mandatory module updates every 24 months. Included in this is an information governance module which ALL staff must complete. All line managers of should have local dissemination and implementation plans in place to ensure all staff are familiar and adhere to all aspects of this policy. This includes non clinical areas and non clinical staff at all locations within NHS Lothian. Unauthorised breaches of confidentiality will be taken very seriously and will result in an investigation into the alleged breach, and may result in disciplinary action in accordance with Management of Employee Conduct - Disciplinary

1. INTRODUCTION

1.1 Confidentiality is central to the trust between all healthcare staff, the public and patients who use our services. Under normal circumstances, patients have a statutory right to expect that information about them will remain confidential and for staff, volunteers and external contractors this is a contractual obligation. Without assurances about confidentiality, patients may be reluctant to give health professionals the information required to provide the most effective care.

1.2 All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security. All patient information must be treated with complete confidentiality and MUST NOT be divulged to anyone who does not have the right to access. Information refers to ALL information including that held on paper, in manual form and electronically. Access to information on patients is restricted to those who have been given permission by the patient, except in specific circumstances laid out in this policy and its appendices.

2. AIM

2.1 To provide guidance on the principles of patients' right to confidentiality within the current statutory framework whilst ensuring NHS Lothian staff share patient information with informed consent and disclose information when required to do so by law.

2.2 Staff must also ensure that when complying with this policy that they do not obstruct or unnecessarily delay the provision of essential clinical care to patients.

3. SCOPE OF THE POLICY

3.1 This policy applies to all information where a patient can be identified, and applies to all types of media where patient-identifiable data is processed including, but not limited to:

- Paper, manual and electronic health records
- Administrative records that hold identifiable patient data e.g. clinica attendance lists
- Records held on machines
- Transport – physical and electronic
- Laboratory results
- Radiographic images
- Photographic images
- Digital images
- email

- Telephone conversations
- Text messages
- Social media

In addition, staff must store, analyse and process patient information in accordance with other NHS Lothian policies including the eHealth Security Policy and the NHS Lothian Social Media Policy

3.2 It is based on the principle that healthcare can be provided in a number of settings, including NHS Lothian premises, community settings and a patient's home. It may, therefore, be necessary to adjust practice and procedure, depending on location.

3.3 This policy applies to those listed below:

- All staff employed by NHS Lothian, including bank and agency staff.
- All students on placement within NHS Lothian premises, or under the mentorship of an NHS Lothian employee in other settings.
- Staff from partner agencies working in NHS Lothian premises.
- Volunteers in locations where healthcare is delivered, whether appointed by NHS Lothian or not.
- Agency and independent contractors working for, or on behalf of, NHS Lothian.

4 LEGAL/REGULATORY FRAMEWORK

Patient information is generally held under legal and ethical obligations of confidentiality within the healthcare team. Information provided in confidence should not be used or disclosed outwith the healthcare team in a form that might identify a patient without his or her consent.

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.

Further information on consent is available in the NHS Lothian policy and guidance for obtaining consent

There are a number of important exceptions to the above rule and these are explained in the NHS Scotland Code of Practice on Protection of Patient Confidentiality

4.1 It is important to note that the right of confidentiality in the healthcare environment is not absolute, and as well as there being a legal obligation to maintain confidentiality, there are occasions where breaching patient confidentiality is a legal requirement.

4.2 Data Protection Legislation is the primary legislation that requires NHS Lothian to process patient information in a confidential manner. NHS Lothian must process personal data in accordance with the eight Data Protection Principles.

4.3 Data Protection Legislation is supported by the Human Rights Act 1998 (HRA) and the Common Law on Confidentiality.

4.4 Article 8 of HRA gives citizens the qualified right of privacy. Any breach of this Article must be justified and proportionate to the purpose for which the Article is being interfered with.

4.5 The common law gives individuals an expectation of confidentiality in their relationship with healthcare professionals.

4.6 Staff must act in accordance with the six Caldicott Principles on best practice on the use of patient-identifiable information (see Appendix 1 – A guide to good practice and procedures).

4.7 The various Professional Codes of Conduct produced by regulatory authorities also place obligations on registered healthcare staff.

4.9 A list of relevant legislation and external guidance supporting NHS Lothian policies is listed in the Reference section of this policy.

4.10 All healthcare staff have a duty to ensure that patients understand their rights with regard to confidentiality and that if applicable Interpreters should be used to avoid any confusion. Further information is available from the Policy for Meeting the Needs of People with Limited English Proficiency

5 INFORMATION SHARING/DISCLOSURES

5.2 Appropriate information sharing is often required to avoid harm and provide the best quality healthcare a patient may need and can therefore be considered good practice.

5.3 NHS Lothian participates in clinical audit, research and teaching, where information sharing occurs at both the point of healthcare delivery and for secondary purposes.

5.4 Further guidance on these forms of information sharing is detailed in Appendices 1, 2, and 3 of this policy.

5.5 There are limited circumstances where information can be disclosed without a patient's consent. An example of appropriate disclosure without consent is for the prevention and detection of crime. Further guidance on good practice on such disclosures is detailed in Appendices 1, 2 and 3 of this policy. Other information is available from Information sharing between NHS Scotland and the police

6 CONFIDENTIALITY, CHILD PROTECTION AND PROTECTING VULNERABLE ADULTS

Sharing relevant information is an essential part of protecting children and vulnerable adults. Although those providing services to adults and children may be concerned about balancing their duty to protect children and vulnerable adults from harm and their general duty towards their patient or service user, the over-riding concern must always be the safety of the child or vulnerable adult. Whenever possible, consent should be obtained before sharing personal information with third parties but concerns about a child or vulnerable adult's safety will always take precedence over the 'public interest' in maintaining confidentiality. It should be borne in mind that an apparently minor concern raised by one agency may, when combined with information from other agencies, point to much more serious concerns.

For more information please see the National Guidance for Child Protection in Scotland (2014), NHS Lothian Child protection procedures (2012), Edinburgh and Lothian's interagency child protection procedures (2012) and Edinburgh Lothian & Borders Guidelines: Adult Support and Protection: Ensuring Rights and Preventing Harm January 2012

7 MANAGEMENT/COMPLIANCE OF THIS POLICY

7.1 NHS Lothian is committed to manage patient information in accordance with the standards set out in the NHS Scotland Information Governance Framework, in partnership with the recommendations and guidance issued by the UK Caldicott Guardians' Council.

7.2 Corporate responsibility for the standards set out in this, and supporting documentation detailed in the Reference section of this policy, lies with the Director of Public Health and health policy who is NHS Lothian's Caldicott Guardian.

7.3 All staff must sign a confidentiality statement in their contract of employment as a condition of employment with NHS Lothian. An extract of the contract is detailed in Appendix 4.

7.4 No staff member should be carrying a portable media device with patient identifiable information contained within it without the media device being encrypted. Further information relating to cameras and recording devices can be found in the Photography and Video Recording of patient policy.

7.5 Staff should only be carrying patient identifiable material on any device with the explicit permission of the Caldicott Guardian. This information should only be carried for an agreed purpose e.g. patient information from pathology at RIE to the multidisciplinary meeting in the Chancellors Building because there is no other means of sending it securely and in a timely fashion.

7.6 Any transfer of identifiable data must be carried out securely with an adequate level of protection given to the data in transit in accordance

with current NHS information security standards. In most circumstances this will require data transferred on portable media or electronically to be encrypted during transit.

7.6 Confidentiality training will be provided as part of the mandatory induction program for new NHS Lothian employees. All staff are expected to be aware of the following:

- Justify the purpose(s) for using confidential information
- Only use it when absolutely necessary
- Use the minimum that is required
- Access should be on a strict 'need to know' basis
- Everyone must understand his or her responsibilities
- Understand and comply with the law

7.7 All staff must attend mandatory updates every 24 months. Included in this is information governance module which ALL staff must complete.

7.8 In addition, managers must provide staff with an adequate support framework and ensure that appropriate training is provided to ensure they act in accordance with this policy.

7.9 Unauthorised breaches of confidentiality will be taken very seriously and will result in an investigation into the alleged breach, and may result in disciplinary action in accordance with Management of Employee Conduct - Disciplinary.

REFERENCES

There is a wealth of information on confidentiality and disclosure of information. The Data Protection Officer for NHS Lothian is always available for advice. The following therefore is not an exhaustive list:

Confidentiality and Security Advisory Group for Scotland (CSAGS) (2002) *Protecting Patient Confidentiality – Final Report* CSAGS Edinburgh

Department of Health (1997) The Caldicott Committee Report on the Review of Patient-Identifiable Information

National Guidence for Child Protection in Scotland (2014) available from http://www.gov.scot/Resource/0045/00450733.pdf last Accessed 19th March 2018

General Medical Council (2017) Confidentiality: Good Practice in Handling Patient Information Available from https://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp last accessed 19th March 2017

Lothian and Scottish Borders Interagency Guidelines for people working in health and social care settings (2013) *Protecting Vulnerable Adults: ensuring rights and preventing harm* available from http://www.nhslothian.scot.nhs.uk/Services/A-Z/LearningDisabilities/GuidelinesAndLegislation/ASPInformationLeaflet.pdf last accessed 19th March 2017

Lothian Health (2016) Child Protection Proceedures available from http://intranet.lothian.scot.nhs.uk/Directory/PublicProtection/ChildProtection/Documents/NHS%20Lothian%20Child%20Protection%20Procedures%202016.pdf last accessed 19th March 2017

Edinburgh & Lothian's Interagency Child Protection Procedures (2015) available from http://www.westlothianchcp.org.uk/media/9889/Child-Protection-Procedures-2015/pdf/Child_Protection_Procedures._2015.pdf Last Accessed 19th March 2017

Children and Young People (Information Sharing) (Scotland) Bill (2017) available from http://www.gov.scot/Topics/People/Young-People/gettingitright/information-sharing/cyp-information-sharing-bill-2017 last accessed 19th March 2017

NHS Executive (1999b) The Public Disclosure Act 1998: Whistle-blowing in the NHS. Health Service Circular 1999/198

Nursing and Midwifery Council (2015) The code: Standards of conduct, performance and ethics for nurses and midwives available from https://www.nmc.org.uk/standards/code/ last accessed 19th March 2017

Pan Lothian Partnership (2004) Individual Protocol governing the receipt and disclosure of personal information for the single shared assessment Edinburgh

Pan Lothian Partnership (2005) Data sharing agreement governing receipt and disclosure of personal information for children Edinburgh

Pan Lothian Partnership (2005) Pan Lothian General Protocol for Sharing Information Edinburgh

NHS Scotland (2003) NHS Code of Practice on Protecting Patient Confidentiality Edinburgh

Information Governance Alliance (2016) Record Management Code of Practice for Health and Social Care. Available from https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjao--FkPjZAhUSy6QKHaQDDmgQFggnMAA&url=https%3A%2F%2Fdigital.nhs.uk%2Fmedia%2F1158%2FRecords-Management-Code-of-Practice-for-Health-and-Social-Care-2016%2Fpdf%2FRecords-management-COP-HSC-2016&usg=AOvVaw1cjNaWw_fF5ij5pn58XQjZ Last accessed 19th March 2017

Children and Young People (Scotland Act) (2014) Available at http://www.legislation.gov.uk/asp/2014/8/contents/enacted Last accessed 19th March 2017

A GUIDE TO GOOD PRACTICE AND PROCEDURES (Appendix 1)

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.

CONFIDENTIALITY AND DISCLOSURE OF INFORMATION (Appendix 2)

INTRODUCTION

Accurate and secure personal health information is an essential part of patient care. The NHS Code of Practice on Protecting Patient Confidentiality (Scottish Executive 2003) states that NHS Scotland's goal is for a service that:

- Protects the confidentiality of patient information
- Commands the support and confidence of public, patients and all staff, students, volunteers and contractors working in or with NHS Scotland
- Complies with best practice
- Conforms with the law
- Promotes patient care, the running of care organisations and the improvement of health and care through new knowledge
- Works in partnership with other organisations and has clearly established and communicated protocols for sharing information

This goal is set within the context of the following legal framework:

- Statute law e.g. Data Protection Legislation, Human Rights Act 1998 Adults with Incapacity (Scotland) Act 2000
- The common law in Scotland on privacy and confidentiality
- Professional standards e.g. NMC code of professional conduct (2008)
- National and local policies and organisational standards Data Protection Policy

PRINCIPLES OF GOOD PRACTICE

A key document to refer to is the Data Protection Legislation (General data Protection Regulation), which describes seven principles for 'good information handling'. These seven principles and what this may mean in practice are detailed below:

Principle	What does this mean?
1. Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
2. Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Accuracy	Personal data shall be accurate and, where necessary, kept up to date

5. Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
6. Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
7. Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

This table was extracted from an example protocol for confidentiality, which can be viewed on www.show.scot.nhs.uk

THE USE OF ANONYMISED CASE STUDIES WITHIN NHS LOTHIAN FOR EDUCATIONAL PURPOSES (Appendix 3)

INTRODUCTION

As a result of a specific incident within NHS Lothian where a clinician delivering a teaching session to a group of healthcare students within an HEI inadvertently provided the cohort with enough relevant information for them to identify the patient in a case study, there was a need to review the practices related to the use of patient information for the purposes of education.

The issue and ethics of confidentiality go to the heart of the healthcare system in the Western world and is an immensely complex and detailed one. This paper will however maintain a focus on the specific aspects of confidentiality relating to the incident described providing advice to practitioners to ensure that patient confidentiality is not breached during educational events.

CURRENT HEI POLICIES IN RELATION TO THE USE OF PATIENT INFORMATION IN EDUCATION

An exploration of policies relating to the use of patient information within educational events in the three local Higher Educational Institutes (HEIs) relating to the involvement of clinicians in undergraduate medicine, nursing and midwifery programmes suggested that policies varied somewhat. It was established however that each HEI requires that the clinician satisfy local requirements to show that they are the appropriate level professionally to undertake a particular educational session. This may be in the form of a Curriculum Vitae, formal appointment as a visiting lecturer (or equivalent role) or recommendation from a trusted clinical source. As such the clinician would also be subject to their employer's confidentiality policies and their respective professional bodies code of professional conduct regarding confidentiality.

In terms of vicarious accountability of the HEI, should for example, a serious factual or procedural error be disseminated, there is a consensus within the HEIs that the programme leaders are ultimately responsible for content. This responsibility to ensure that any education provided upholds patient confidentiality is subsequently devolved to module leader (or equivalent role) colleagues engaging the clinician to contribute to the educational event. Where staff, have duel employment the use of any NHS live system to support lecture delivery can pose a breach of confidentiality. Where staff are unclear, advice should be sought from the relevant departments i.e. eHealth.

ENSURING ANONYMITY OF PATIENT INFORMATION

Whilst all the health and indeed other professions have clauses in their codes of conduct, most of them refer, understandably, to issues of confidentiality in terms of provision of care; communication within the care team; ethical considerations and so on. There is little in these documents however addressing use of confidential information relating to education or teaching situations.

The British Medical Association (2011) makes the following assertion around sharing of confidential information with other health professionals in an anonymised form: *'Information may be used more freely if the subject of the information is not identifiable in any way. Usually, data can be considered to be anonymous where clinical or administrative information is separated from details that may permit the individual to be identified such as name, date of birth and postcode. Even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification.*

When anonymised data will serve the purpose, health professionals must anonymise data to this extent and, if necessary, take technical advice about anonymisation before releasing data. Whilst it is not ethically necessary to seek consent for the use of anonymised data, general information about when their data will be anonymised should be available to patients.'

Taken from Confidentiality and disclosure of health information tool kit

Throughout this guidance the BMA emphasises that disclosures of information should involve the minimum necessary to achieve the objective.
Thus wherever possible, anonymous or aggregated data should be used in preference to identifiable information.'

NHS Scotland (2003) within the Code on Protecting Patient Confidentiality gives the following guidance:

' Data are said to be anonymised when items such as name, address, full postcode, date of birth and any other detail that might identify a patient are removed; the data about a patient cannot be identified by the recipient of the information; and the theoretical probability of the patient's identity being discovered is extremely small.' (p13)

CONSENT TO USE ANONYMISED PERSONAL INFORMATION

Within all professional codes of conduct the importance of maintaining confidentiality at all times is highlighted. However, in an educational environment, there is also the implicit expectation that case studies based around real patients and situations, are used in order to promote learning for the profession. A patient has the right to expect that their individual details are not identifiable. NHS Scotland (2003) also highlight the need fro the patient to be informed that their information will be used for disease registries, medical research, education and training in an anonymised format. The patient must consent to the use of this information in these circumstances and that their choice as to whether they agree to their information being used in this manner respected.
Again there is little if any literature referring specifically to this aspect, understandably focussing on consent within the realms of 'care'. The BMA (1999) notes that: 'It cannot be assumed that identifiable health information can be automatically shared with any other health professional or health service employee. Care must be taken to ensure that disclosures are not made inadvertently, that those receiving the information in a professional capacity also have obligations

(professional, contractual and/or legal) to maintain confidentiality, that only information necessary to achieve the objective is disclosed and it is understood that the information should only be used for the purpose for which it is disclosed.'

Transposing this to the educational environment, the professional who intends to use patient information for educational purposes has two obligations:-

i) the responsibility to inform the patient that their details (relevant to pathology) may be used in the future in order to assist in Continuing Professional Development and/or Practice Education. They must gain their consent for information to be used in this manner.

ii)) the responsibility to ensure that all identifiable personal information will be changed or deleted in order to maintain confidentiality

USE OF CASE STUDIES IN EDUCATION

Case studies by their nature are often used to highlight 'typical' or indeed atypical cases of pathology. They are commonly used in both undergraduate and postgraduate education as tools in assessment in clinical practice. Invariably, under these conditions the learner will need to gain consent from the patient/client/carer in order to use patient details, and also ensure that as far as possible, these details are kept confidential.

Most of the health professions in the United Kingdom have adopted a problem based learning (PBL) approach within the Universities and colleges to help engage students, provide a 'real' scenarios and to enable cross-boundary clinical and theoretical education. The essence of PBL is that the student addresses a scenario designed to mimic (to a greater or lesser extent) a clinical situation, and hence gain experience of dealing with real issues without the risk to the patient.

Case studies whilst not exclusively within the domain of PBL, can help illustrate a complex medical scenario very effectively. They also have a considerable benefit to both teacher and student of providing extra information or challenge that either requires, simply by definition, to be based on true events. In other words the reality of the situation provides a richness of experience where a purely fictional scenario probably could not.

It is therefore not surprising that clinicians will frequently refer to anonymised case studies to illustrate particularly interesting, representative or complex cases.

ENSURING ANONYMITY WHEN USING CASE STUDIES

Prior to preparing a session that will include information about real patients/clients/carers, it is suggested that the clinician should go through the following checklist:

• Is case study the best way to approach this topic – would another way be as effective?
• Could the case study be completely fictional instead?

• Could the case study be as effective if aggregated from a number of patients?
• What information is pertinent to the learning required for this particular cohort of students?
• What information, if any, has been retained, that may jeopardize a patient/client/carer's anonymity? Specifically:
1. Image (or part of an image), body morphology, tattoo or birth mark, presence of any readily recognisable feature including voice in the case of video or audio tape.
2. Demographic information on sex, date of birth, race, address, religion, profession.
3. Any form of identification easily or *potentially* 'decoded' by the audience such as initials, DoB, CHI or patient number.
4. Does the patient fall into the category of 'rare' in terms of diagnosis, drug therapy regime or very specific populous.
• Can further information relating to one, *or a combination of*, pieces of information that may jeopardize anonymity be omitted?
The professional also requires to be aware that it may be the supplementary information that the teacher provides, as 'background' to the case study, that may be the most hazardous in terms of breaking confidentiality and needs to be avoided. The issue of consent also needs to be addressed. Clearly if an individual clinician is undertaking development of a case study based on an individual patient event.

CONCLUSION

The dearth of literature around this topic would suggest that this incident is a rare one, with the temptation therefore to dismiss the possibility of it happening again as infinitesimal. Whilst recognising this to be the case, this particular incident has had widespread consequences both personal and professional for all those involved. When undertaking educational events, all professionals must take cognisance their professional bodies codes of conduct in relation to patient confidentiality and adhere to the NHS Lothian and HEI policies related to patient confidentiality and the use of patient information for educational purposes.

Information Governance guidance in education

The following guidance is intended for NHS Lothian Staff, Module Leaders and Module Teams developing and delivering modules / courses delivered by NHS Lothian or modules within the Collaborative Agreements between NHS Lothian and Queen Margaret and Edinburgh Napier Universities.

Guidance on the use of anonymised information

It is recognised that information from the practice arena may be used in an educational environment to promote professional learning. In such circumstances information must be anonymised. Anonymised information is information that does not identify a specific individual and all patient, staff, relative or carer information used in course / module material must be anonymised. If a patient, staff member, relative or carer could identify specific individuals or specific practice areas in any educational material used in then it is not anonymous. It is therefore recommended that all training materials use composite information to ensure teaching materials are truly anonymised. NHS Lothian policy on Confidentiality of Personal Health Information (2011) states that consent must be obtained to use anonymised personal information (P.18).

To ensure that the confidentiality of patients, staff, relatives and carers is preserved, the following guidelines must be followed when using any practice based material in the educational environment:

A. Names, addresses and any other identifiable personal details of patients, staff, relatives or carers should not be used in any circumstances.

B. Identifiable work areas such as NHS directorates, hospitals or wards should not be used.

C. Identifiable information relating to critical incidents or fatal accident enquires should not be used.

D. Where there is an uncommon diagnosis or other distinctive circumstances that could potentially lead to identification of a patient, member of staff, relative or carer this information should not be used without significant adjustment to ensure anonymity is maintained.

E. In circumstances such as D above, aggregation of data or information from a number of patients or the use of composite information from multiple sources may be used to ensure anonymity.

NHS LOTHIAN
INFORMATION GOVERNANCE GUIDANCE FOR ACADEMIC ASSESSMENT

The following guidance is intended for students undertaking modules / courses delivered by NHS Lothian or modules in the Collaborative Agreements between NHS Lothian and Queen Margaret and Edinburgh Napier Universities.

Guidance on the use of anonymised information

Some modules / courses require students to submit assignments using information based on clinical practice. In such circumstances information must be anonymised. Anonymised information does not identify a specific individual and all patient, staff, relative or carer information used in course / module assignments must be anonymised. If a patient, staff member, relative or carer could identify specific individuals in a piece of written work then it is not anonymous. It is therefore recommended that students use composite information to ensure assignments are truly anonymised.

NHS Lothian policy on Confidentiality of Personal Health Information (2011) states that consent must be obtained to use anonymised personal information (P.18).
To ensure that the confidentiality of patients, staff, relatives and carers is preserved, the following guidelines must be followed when submitting any module / course assignments or work:

A. Names, addresses and any other identifiable personal details of patients, staff, relatives or carers should not be used in any circumstances.

B. Identifiable work areas such as NHS directorates, hospitals or wards should not be used.

C. Identifiable information relating to critical incidents or fatal accident enquires should not be used.

D. Where there is an uncommon diagnosis or other distinctive circumstances that could potentially lead to identification of a patient, member of staff, relative or carer this information should not be used without significant adjustment to ensure anonymity is maintained.

E. In circumstances such as D above, aggregation of data or information from a number of patients or the use of composite information from multiple sources may be used to ensure anonymity.

EXTRACT FROM CONTRACT OF EMPLOYMENT (Appendix 4)

Confidentiality

Obligations Arising from Data Protection Legislation

Particular regard should be given to your responsibility to abide by the principles of Data Protection Legislation and any subsequent legislation or formal guidance issued by the Scottish Executive. Further information is available from the Data Protection Officer.

General Obligations

Patients
In the course of your duties you may have access to confidential material about patients. On no account must information relating to patients be divulged to anyone other than authorised persons - for example medical, nursing or other professional staff, as appropriate who are concerned directly with the care, diagnosis and/or treatment of the patient.

Staff
Similarly no information of a personal or confidential nature concerning individual members of staff should be divulged to anyone without the proper authority having first been given.

Health Service Business
You may also have access to confidential material on Health Service business that should not be divulged to anyone without the proper authority having first been given.
If you are in any doubt whatsoever as to the authority of a person or body asking for information on patients, staff or Health Service business you must seek advice from your manager. The Scottish Office Home and Health Department code of practice on confidentiality of personal health information is available from your local HR Department.

Information Technology
You are required to comply with NHS Lothian policies on information technology security, use of e-mail and Internet access. Copies of these policies may be obtained through your line manager.

Failure to Comply with Obligations

Failure to observe these obligations will be regarded by your employer as serious misconduct that could result in disciplinary action being taken against you including dismissal. You may also be liable to prosecution for an offence under the data protection legislation or an action for civil damages.

References:

Draper, H and Rogers, W (2005) Re-evaluating confidentiality **Advances in Psychiatric Treatment vol. 11, 115–124**

NHS Code of Practice on Protecting Patient Confidentiality (2003) Available at http://www.elib.scot.nhs.uk/SharedSpace/ig/Uploads/2008/Oct/20081002150659_6074NHSCode.pdf last accessed 22nd September 2011

The Confidentiality & Security Advisory Group for Scotland: Protecting patient confidentiality Available from: http://www.sehd.scot.nhs.uk/publications/ppcr/ppcr.pdf last accessed 22nd September 2011

BMA Confidentiality and disclosure of health information tool kit Available from http://www.bma.org.uk/images/confidentialitytoolkitdec2009_tcm41-193140.pdf last accessed 22nd September 2011