Lothian NHS Board

Lothian NHS Board
Mainpoint
102 Westport
Edinburgh
EH3 9DN
Main Switchboard: 0131 242 100

www.nhslothian.scot

Date 02/04/2025
Your Ref
Our Ref 9832

Enquiries to Richard Mutch
Extension 35687
Direct Line 0131 465 5687
loth.freedomofinformation@nhs.scot
richard.mutch@nhs.scot

Dear

FREEDOM OF INFORMATION – DATA PROTECTION AND PATIENT CONFIDENTIALITY

I write in response to your request for information in relation to data protection and patient confidentiality.

Question:

1. A copy of the Organisation's governance guidance document(s) regarding training of all employees in data protection and patient confidentiality. I understand this may have changed over time, please provide any documents showing changes or updates in the last 10 years, where that date range is not possible please provide what you can and clarify reasons why unable to provide more historical data (for example if this is due to a data retention policy then please include a copy of that data retention policy).

Answer:

Information Governance Policy notes Training from 2015 – 2018. Confidentiality Policy notes training from 2017 – 2020. Training then covered in NHS Lothian Training Strategy attached from 2021 & 2022 (to be updated 2025).

Question:

2. Information from the Organisation detailing the titles of roles (both clinical and non-clinical) and the data protection training and patient confidentiality training. For each role can you detail: a) expectations on candidates for employment and b) the frequency of renewal/refresh of such training for that title/role. If you do not have specific data, could you provide information on the general areas of roles... such as 'Nurses', 'Consultants', 'Surgeons', 'Secretary non-clinical', 'Payroll', etc, etc. This may have changed from year to year, over time - if this has changed significantly in the last 10 years, please advise of the date when changes were brought in and any associated documents regarding the change.

Answer:

TNA from 2016 – 2024, enclosed.

Question:

3. Information from the Organisation detailing the total number of staff and the percentage of adherence to completion of regular (annual?) renewal of data protection and patient confidentiality training. Please show as a trend over a number of years (annual aggregation is acceptable which shows the total staff and adherence/compliance data), Please provide data for the last 10 years, if unable to satisfy then provide it as far back as you can with a note on why additional historical data is not held (retention policy - then please quote the retention policy document).

Answer:

All staff complete mandatory online learning every 2 years.

	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Average Compliance Figure	55%	76%	89%	85%	77%	Not recorded as move to new system	71%	74%	78%	78%

Question:

4. Information from the Organisation regarding the number of data breaches. Grouped by those reported to the ICO (Information Commissioners Office) and those not reported to the ICO but reported internally to the organisation. If you could also provide within that data the severity that a breach was considered to be (e.g. Low, Medium, High). Additionally if any financial fines needed to be paid by the organisation, or other sanctions/enforcement actions made by the ICO or other regulatory body as a result of the breach. Please provide data for the last 10 years, if unable to satisfy then provide it as far back as you can with a note on why additional historical data is not held (retention policy - then please quote the retention policy document)

Answer:

	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Number of breaches Reported to ICO	5	<5	7	5	9	5	6	8	8	14
Number of breaches Reported internally but not accepted on review.	88	134	170	224	197	198	203	209	228	311

Question:

5. Please advise if your Organisation is asked to report on compliance with data protection training / patient confidentiality to a parent body or other organisation.

Answer:

Reported internally to NHS Lothian Board.

I hope the information provided helps with your request.

If you are unhappy with our response to your request, you do have the right to request us to review it. Your request should be made within 40 working days of receipt of this letter, and we will reply within 20 working days of receipt. If our decision is unchanged following a review and you remain dissatisfied with this, you then have the right to make a formal complaint to the Scottish Information Commissioner within 6 months of receipt of our review response. You can do this by using the Scottish Information Commissioner's Office online appeals service at www.itspublicknowledge.info/Appeal. If you remain dissatisfied with the Commissioner's response you then have the option to appeal to the Court of Session on a point of law.

If you require a review of our decision to be carried out, please write to the FOI Reviewer at the email address at the head of this letter. The review will be undertaken by a Reviewer who was not involved in the original decision-making process.

FOI responses (subject to redaction of personal information) may appear on NHS Lothian's Freedom of Information website at: https://org.nhslothian.scot/FOI/Pages/default.aspx

Yours sincerely

ALISON MACDONALD
Executive Director, Nursing
Cc: Chief Executive
Enc.

POLICY ON CONFIDENTIALITY OF PERSONAL HEALTH INFORMATION

Author (s): Clinical policy Advisor
Version: 1.2
Status: Final
Date of Authorisation: 2017
Key Words: Confidentiality
Page 1 of 29

Authorised by: Clinical Policy Group
Review Date: 2020
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 attend mandatory 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 The Data Protection Act 1998 (DPA) 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 DPA 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

Scottish Government National Guidance for Child Protection in Scotland available from http://www.scotland.gov.uk/Publications/2010/12/09134441/0 last Accessed 24th January 2012

General Medical Council (2009) Confidentiality Available from http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp last accessed 26th January 2012

Lothian and Scottish Borders Interagency Guidelines for people working in health and social care settings (2003) *Protecting Vulnerable Adults: ensuring rights and preventing abuse* available from http://intranet.lothian.scot.nhs.uk/NHSLothian/Corporate/A-Z/ASAP/Pages/ELBEGGuidelines.aspx last accessed 26th January 2012

Lothian Health (2007) Child Protection Policy available from http://intranet.lothian.scot.nhs.uk/NHSLothian/Corporate/A-Z/Clinical%20and%20Corporate%20Learning/CorpLearningDev/PublicProtection/ChildProtection/Pages/NHSLothianChildProtectionProcedures.aspx last accessed 26th January 2012

Edinburgh & Lothian's Interagency Child Protection Procedures (2007) available from http://intranet.lothian.scot.nhs.uk/NHSLothian/Corporate/A-Z/Clinical%20and%20Corporate%20Learning/CorpLearningDev/PublicProtection/ChildProtection/Pages/Inter-agencyProcedures.aspx Last Accessed 26th January 2012

Scottish Government Information sharing between NHS Scotland and the police available from http://intranet.lothian.scot.nhs.uk/NHSLothian/Corporate/A-Z/ASAP/Pages/ELBEGGuidelines.aspx last accessed 26th January 2012

Scottish Executive (2004) Sharing Information about Children at Risk: A Brief Guide to Good Practice

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 http://www.nmc-uk.org/Nurses-and-midwives/The-code/The-code-in-full/ last accessed 26th January 2012

Nursing and Midwifery Council (2009) Confidentiality available from http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Confidentiality/ last accessed 26th January 2012

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

Pan Lothian Partnership (2005) The Edinburgh and Lothian information sharing agreement for access to information on child protection register

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

Children's Scotland Act (1995) 2003

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

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. No other health boards in Scotland use fax to send patient identifiable information and other routes for sharing information should be explored, e.g. Email.

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 the Access to Health Records Act and Data Protection Act 1998. 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

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); The Data Protection Act 1998 (DPA) 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.

The Data Protection Act, which legislates for 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. DPA 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 DPA 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 Act 1998, 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 LPCT Data Protection Act 1998 Policy

PRINCIPLES OF GOOD PRACTICE

A key document to refer to is the Data Protection Act 1998, which describes eight principles for 'good information handling'. These eight principles and what this may mean in practice are detailed below:

Principle	What does this mean?
1. Fairly and lawfully processed	When obtaining the information from patients, relatives, users etc. you should ensure they are aware of the purpose of the data collection and to whom the data may be disclosed. Consent should be obtained and in the case of sensitive data (date of birth, Trade Union membership, ethnic origin etc) explicit consent should be obtained.
2. Processed for one or more lawful purpose and not in any manner incompatible with those purposes	Once data has been obtained for a specific purpose it cannot be used for any other purpose without the consent of the individual or a reassessment of the situation.
3. Adequate, relevant and not	You should only collect information for your

excessive	stated purpose, but this information should be sufficient for that purpose. You should only hold information that is required to enable you to treat the patient effectively. Where possible, use anonymised data.
4. Accurate and up to date	You should always try to ensure that any data is accurate. Any discrepancies should be amended as soon as possible after they have been pointed out. You should also try to ensure that data is kept up to date.
5. Not kept for longer than is necessary	Do not hold data longer than is necessary. Follow guidelines to help with this. Not all person identifiable data is held as part of the patient's record.
6. Processed in line with the data subject's rights	See below
7. Secure	You must ensure that appropriate security is in place for all processing i.e. from collection through to destruction.
8. Not transferred to countries outside the European Economic Area (EEA) without adequate protection.	You must not transfer personal data in whatever form to a country outside the EEA, which does not have an adequate level of protection.

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 the Data Protection Act 1998 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

A Quick Guide to Essential Data Sharing Training

NHS Lothian

Staff Group	Training Required	Training to be Provided
• Senior Managers • Information Asset Owners • Information Asset Administrators • IG Project Officers	• Data Sharing Training • DPIA Guidance • Project Management Guidance • ICO Guidance and Code of Practice	**Essential training-** Core skills e-learning Specialist Data Sharing Training by IG Team **Desirable training** ICO Guidance and online tools as outlined by the Data Protection Manager IG Intranet page and Project manager Guidance
• SAR Team • IG IT Security Staff • Projects Team • Innovation Team • R&D staff • Patient Experience Team (PET)	• Data Sharing Training • DPIA Guidance • Project Management Guidance • ICO Guidance and Code of Practice • SAR Team internal Processes (available to all on intranet)	**Essential training-** Core skills e-learning Specialist Data Sharing Training by IG team **Desirable training** IG Roadshow IG Intranet page Tailored training to core groups Bites size training videos on IG intranet. SAR Team Internal Process Newsletter
• All NHS Lothian Staff	• IG Intranet site • SAR Team internal Processes (available to all on intranet)	**Essential training-** Core skills e-learning **Desirable training** IG Roadshow IG Intranet page SAR Team Internal Process Newsletter

INFORMATION GOVERNANCE: A Quick Guide to Essential Training

NHS Lothian

ALL STAFF

2 YEARLY

Core Mandatory Information Governance e-learning module

STAFF WHO DEAL WITH SUBJECT ACCESS REQUESTS [SAR]

- Medical Legal Staff
- Dental Administrators
- Prison Staff
- NHSL GP Practice Manager

Attend the Specialist SAR Workshop, bookable via Empower

[Training content: Recognising; processing; handling; redacting; providing; follow-up & escalating]

STAFF WORKING IN THE PATIENT EXPERIENCE TEAM

Attend the Specialist SAR PET Presentation, bookable via Empower

[Presentation content: Recognising; processing; providing; follow-up & escalating]

All staff are encouraged to attend Information Governance Roadshows when available and regularly refer to the Information Governance documents available on the Intranet.

INFORMATION GOVERNANCE POLICY

Unique ID: NHSL.
Category/Level/Type:
Status:
Date of Authorisation:
Date added to Intranet:
Key Words: Information Governance Policy

Author (s): TMcKinley
Version: July 2015
Authorised by: Director of Public Health and Health Policy
Review Date: July 2018

Comments:

KEY POLICY ISSUES:

Principles of Information Governance

- Openness
- Confidentiality and Legal Compliance
- Information Security
- Quality Assurance
- Legal and Related Policies and Guidance
- Information Governance Management

Table of Contents

1. Purpose

1.1 The purpose of this policy is to set out the key principles which apply to the management of information stored and used by NHS Lothian.

1.2 The document will set out the high level framework within which the Board can monitor NHS Lothian performance and compliance in Information Governance and to provide an overview of responsibilities and sources of guidance for staff.

1.3 Information is a vital asset both in terms of the clinical management of the individual patient and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

1.4 It is, therefore, of paramount importance to ensure that all information is efficiently managed and those appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

2. Scope

2.1 This policy covers all types of information within NHS Lothian, including but not limited to:

- Patient/service user information
- Personnel information
- Financial information
- Estates information
- Organisational information

2.2 The policy covers all aspects of handling information, including but not limited to:

- Structured record systems – both paper and electronic
- Unstructured documents held on computer network drives, hard drives or removable media such as CD s and USB memory sticks (where use is authorised)
- Information published on the intranet
- Working documents regardless of format
- Information held outside NHS Lothian premises or systems on our behalf

The transmission of information – via electronic means, email, post, telephone and face to face.

2.3 The policy applies to and must be adhered to by all NHS Lothian staff. The policy is commended to independent sub-contractors.

3. Principles

3.1 NHS Lothian recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. NHS Lothian fully supports the principles of corporate governance and recognises its' public accountability but equally places importance on the confidentiality and security of personal information regarding patients and staff and commercially sensitive information.

3.2 NHS Lothian also recognises the need to share patient information with other healthcare organisations and outside agencies in a controlled manner which is consistent with the interest of individual patients, the health of the people of Lothian and, in some circumstances, the public interest.

3.3 NHS Lothian believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

3.4 There are four key inter-linked strands to the Information Governance Policy:

- Openness
- Confidentiality
- Information Security
- Quality assurance

4. Openness

4.1 Non-confidential information about NHS Lothian and its' services will be made available to the public through a variety of media, including an internet based Publication Scheme.

4.2 NHS Lothian will establish and maintain policies to ensure compliance with the Freedom of Information (Scotland) Act 2002.

4.3 NHS Lothian will undertake or commission annual assessments and audits of its policies and arrangements for openness.

4.4 Patients will have access to information relating to their own health care, options for treatment and rights as individuals.

4.5 NHS Lothian has clear procedures and arrangements for liaison with the press and broadcasting media.

4.6 NHS Lothian has clear procedures and arrangements for handling queries and complaints from patients and the public.

5. Confidentiality and Legal Compliance

5.1 NHS Lothian regards all identifiable personal information relating to patients as confidential.

5.2 NHS Lothian regards all identifiable information relating to staff as confidential, except where national policy on accountability and openness requires otherwise.

5.3 NHS Lothian will establish and maintain policies to ensure compliance with the Data Protection Act 1998, Human Rights Act 1998, Freedom of Information (Scotland) Act 2002 and the Public records Act 2011.

5.4 NHS Lothian will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies taking account of relevant legislation

5.5 NHS Lothian will undertake or commission annual assessments and audits of its compliance with legal requirements.

5.6 Staff responsibilities are set out in employment contracts, staff handbooks, etc. Alleged breaches of confidentiality will be dealt with in accordance with the Board's disciplinary policies. Awareness and understanding of staff, with regard to their specific responsibilities, will be regularly assessed and appropriate training and awareness will be provided

5.7 The Information Governance will provide regular workshops and yearly Information Governance Roadshows throughout the organisation. Iit is the responsibility of line managers to ensure all staff attend one of these events along with the completion of the IG LearnPro module on a bi yearly basis.

5.8 Risk assessment in conjunction with overall priority planning or organisational activity will be undertaken to determine if appropriate, effective and efficient information governance controls are in place.

6. Information Security

6.1 NHS Lothian will establish and maintain policies for the effective and secure management of its information assets and resources.

6.2 Audits will be undertaken or commissioned to assess information and IT Security arrangements.

6.3 NHS Lothian promotes effective confidentiality and security practice to its staff through policies, procedures and training.

6.4 NHS Lothian has agreed robust incident reporting procedures which will be maintained and monitored. All reported instances of actual or potential breaches of confidentiality and security will be investigated.

7. Information Quality Assurance

7.1 NHS Lothian will establish and maintain policies for information quality assurance and the effective management of records.

7.2 Audits will be undertaken or commissioned of NHS Lothian's quality of data and records management arrangements.

7.3 Managers will be expected to take ownership of, and seek to improve the quality of data, within their services.

7.4 Information quality will be assured at the point of collection by use of consistent agreed technical and data standards

7.5 Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

7.6 NHS Lothian will promote information quality and effective records management through policies, procedures/user manuals and appropriate training.

7.7 Internal and external audit and other quality assurance review processes including those requested by NHS Lothian Healthcare Governance and Clinical Risk management committees, Information Governance Toolkit standards and Quality Improvement Scotland (QIS) Information Governance Standards, along with NHS Scotland Information Governance toolkit standards will underpin this policy.

8. Legal and NHS Lothian Related Policies and Guidance

8.1 NHS Lothian has a comprehensive range of policies supporting the Information Governance agenda; reference must be made to these alongside this overarching policy (see Appendix 1 for related policies and Legal Acts).

8.2 Professional and legal guidance should also be considered where appropriate. All enquiries should be directed to NHS Lothian's Information Governance Working Group.
Contact: Info.Governance@nhs.lothian.scot.nhs.uk Enquiries will then be appropriately redirected.

9. Implementing the Policy – Information Governance Management

9.1 The strategic direction for Information Management and Information Governance will be set out in NHS Lothian's Information Strategy.

9.2 The Healthcare Governance and Risk Management Committee, accountable to NHS Lothian Board will have overarching responsibility for monitoring the strategy and for ensuring that NHS Lothian has effective policies and management arrangements in place which cover all aspects of information governance.

9.3 Assessments of compliance with relevant information governance standards (particularly the requirements of the Information Governance Toolkit) will be undertaken each year, and an appropriate information governance improvement plan will be produced as a result.

9.4 Delegated responsibility for overseeing the Information Governance Strategy, Policy and Implementation plan sits with the NHS Lothian Information Governance Assurance Board chaired by an Executive Director of the Board. This group will secure the necessary resources to implement the Information governance action plan and will monitor activities and periodically report progress to HCGRM. Full terms of reference will be available on NHS Lothian Intranet

9.5 The Director of Public Health is the named executive director on the Board with responsibility for Information Governance. The Director of Public Health is also the Caldicott Guardian for NHS Lothian.

9.6 Delegated responsibility for implementation and monitoring of the Information Governance Action plan sits with the Director of Clinical Information. A working group is in place and membership includes a wide range of healthcare and interagency staff.

9.7 The Information Governance working group led by the Director of Clinical Information and on behalf of the Information Governance Assurance Board will have operational responsibility for coordinating and monitoring information governance activities across NHS Lothian. The working group will provide expertise and advice to organisational departments on compliance with relevant standards and the management of health records.

9.8 The Information Governance Working Group has membership representation from within appropriate organisational departments who will be central to the delivery of the information governance improvement plan. This group will act

as a first point of contact for disseminating information and will assist with local training and staff induction.

9.9 In addition, managers across NHS Lothian will be expected to ensure their staff are aware of their responsibilities with regard to information governance and to identify appropriate training and support through the PDP/appraisal process.

10. Public Records (Scotland) Act

Under the Public Records (Scotland) Act 2011 Scottish public authorities must produce and submit a records management plan setting out proper arrangements for the management of the organisations records to the Keeper of the Records of Scotland for his agreement under Section 1 of the Public Records (Scotland) Act 2011.

NHS Lothian will submit its Records Management Plan (RMP) (during 2016?), and it will set out the overarching framework for ensuring that NHS Lothian's records are managed and controlled effectively, and commensurate with the legal, operational and information needs of the organisation. The RMP will consider 14 elements as advised in the Keeper's Model RMP and supporting guidance material. The 14 elements are:

- Senior management responsibility
- Records manager responsibility
- Records management policy statement
- Business classification
- Retention schedules
- Destruction arrangements
- Archiving and transfer arrangements
- Information security
- Data protection
- Business continuity and vital records

- Audit trail
- Competency framework for records management staff
- Assessment and review
- Shared information

The RMP will define NHS Lothian's Action Plan for improving the quality, availability and effective use of records in NHS Lothian and will provide a strategic framework for all records management activities.

This page will be regularly updated with information and progress as available, and the final RMP and supporting evidence will all be published on this page in due course

Appendix 1 – Related Policies and Legal Acts
Information Governance Related Policies and Strategies
Legal Acts

Legal acts relating to the Information Governance agenda include, but are not limited to:

- Data Protection Act 1998
- Freedom of Information (Scotland) Act 2002
- Human Rights Act 1998
- Public Records Act 2011
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998)
- Computer Misuse Act 1990
- Criminal Justice (Scotland) Act 2003
- Electronic Communications Act 2000
- Electronic Communications (Scotland) Order 2006
- Regulations of Investigatory Powers (Scotland) Act 2000
- NHS Lothian Confidentiality Policy
- NHS Lothian IT Security Policy
- NHS Lothian Safe Emailing Guidelines
- NHS Lothian Social Media Policy

INFORMATION GOVERNANCE INFRASTRUCTURE

Initiative/Work Area	Executive Lead	Responsible Person	Co-ordinator
Caldicott	Director of Public Health and Health Policy	Information Governance Manager	Specialist in Public Health & Health Policy
Confidentiality (Non-Clinical)	Director of Public Health and Health Policy	Director of Clinical Information	Information Governance Manager
Data Protection	Medical Director	Director of Clinical Information	Information Governance Manager
Freedom of Information	Director of Finance	Freedom of Information Officer	Freedom of Information Officer
Administrative Records	Director of Finance	Corporate Governance & VFM Manager	Corporate Governance & VFM Manager
Health Records (Electronic)	Medical Director	Head of Health Records	Health Records Managers
Health Records (Paper)	Medical Director	Head of Health Records	Health Records Managers
IG Policy & Planning	Director of Public Health and Health Policy	Director of Clinical Information	Information Governance Manager
IG Toolkit	Director of Public Health and Health Policy	Director of Clinical Information	Information Governance Manager
Information Quality Assurance (Clinical)	Medical Director	Head of Health Records	Health Records Managers
Information Quality Assurance (Non-clinical)	Director of Finance	Corporate Governance & VFM Manager	Corporate Governance & VFM Manager
IT Security	Director of eHealth	Head of Operations & Infrastructure	Systems Admin/Security Manager, ISO

DOCUMENT TITLE: INFORMATION GOVERNANCE POLICY

Version No.	Review Date	Signature	Date
1.0	2 March 2010	Alison McCallum Director of Public Health and Health Policy	19/02/2009
2.0	July 20120	Alison McCallum Director of Public Health and Health Policy	

Recognising a Subject Access Requests: A Quick Guide to Essential Training

NHS Lothian

Staff Group	Training Required	Training to be Provided
Staff who deal with Subject Access Requests Medical Legal Staff Dental Administrators Prison Staff NHSL GP Practice Managers	Legal Backgroud Subject Access Request: • Recognising • Processing • Handling • Redacting • Providing • Follow-up • Escalating	**Essential training-** Core skills e-learning Specialist SAR Workshop **Desirable training** IG Roadshow Documents on IG Intranet page
Staff working in the Patient Experience Team	Legal Backgroud Subject Access Request: • Recognising • Processing • Providing • Follow-up • Escalating	**Essential training-** Core skills e-learning Specialist SAR PET Presentation **Desirable training** IG Roadshow Documents on IG Intranet page
All Staff	Subject Access Request: • Recognising • Escalating	**Essential training-** Core skills e-learning **Desirable training** IG Roadshow Documents on IG Intranet page

A Quick Guide to Essential Information Governance Training

Staff Group	Training Required	Training to be Provided
Information Governance Managers and Project Officers	Mandatory IG Training ICO Guidance Peer Support – NHSS IG Forum Specialist Data Protection Training/Qualification (external provider)	**Essential training-** Core skills e-learning Specialist Data Protection Training by Data Protection Manager **Desirable training** ICO Guidance and online tools Specialist Data Protection Training (external provider)
Information Governance IT Security Staff Senior Managers eHealth Senior Management Tea eHealth Training staff HR Managers Executive Team	Mandatory IG Training Regular Updates via IG Intranet/IG Newsletter Bespoke training to core groups	**Essential training-** Core skills e-learning Specialist Data Protection Training by Data Protection Manager **Desirable training** IG Tailored training to core groups Documents on IG Intranet page
All NHSL Staff	Mandatory IG Training Regular Updates via IG Intranet/IG Newsletter	**Essential training-** Core skills e-learning **Desirable training** IG Roadshow Documents on IG Intranet page

Training Strategy
Information Governance

Contents

What is Training/Learning Needs Analysis (TNA)

A training/learning needs analysis (TNA) is a review of learning and development needs for staff, volunteers and trustees within in your organisation. It considers the skills, knowledge and behaviours that your people need, and how to develop them effectively.

Organisational TNA should ideally be undertaken at 3 levels:

- Organisational level
- Team/departmental level
- Individual level

These three levels are inter-linked and using this structure will help ensure a balanced analysis that takes into account the big picture as well as the specific needs of individuals.

Methods that can be used to identify learning needs include:

- Analysis of existing strategies and plan to identify what skills are needed for delivery
- Questionnaires – paper based or online
- One-to-one interviews
- Focus groups - facilitated small group discussions with a representative sample of people

The outcome of your TNA should be a robust learning and development plan, based on research and linked to organisational, team and individual objectives.

Some of the questions that you might like to ask before undertaking an analysis of learning needs are:

1. Do we have a strategic and organisational plan?
2. Do we have an appraisal system in place?
3. Do all staff have an up-to-date job description?
4. Do all staff have written objectives?
5. Do we have a competency framework in place?
6. Do we have a training strategy and/or a stated commitment to the value of learning and development for our staff/volunteers and trustees?
7. Do we have processes (formal and informal) in place for effective consultation across the organisation?

The more questions that you can answer yes to, the easier it will be to undertake training needs analysis. The information in this section and the diagnostic template (see Appendix 1) will help you in accessing resources to support your TNA process.

Organisational Level

Training/learning needs analysis at this level should start with a review of the organisation's strategic and operational plans.

If you do not already have a strategic planning process in place, it is recommended that you carry out one using a tool such as a **SWOT analysis** (see Appendix 2). This looks at the strengths, weaknesses, opportunities and threats facing your organisation.

The more people that you can involve in identifying this data the better: trustees, managers, staff and volunteers can all bring a different perspective and contribute to a deeper analysis.

Once you have a strategic picture of the organisation's objectives, performance and future direction, you can review this from the perspective of the knowledge, skills and behaviours that can help your organisation to build on its strengths and address weaknesses.

Strengths
How can you capture the good practice and expertise that already exists? How can you build on the strengths, skills and knowledge already in the organisation?

Weaknesses
What skills, knowledge or behaviours could help address the identified weaknesses?

Opportunities
What skills, knowledge or behaviours that could help your organisation make the most of the available opportunities?

Threats
What skills, knowledge or behaviours could help your organisation manage and overcome the identified threats?

Team Level

Analysis of learning needs should also be undertaken at department/team level. If you are in a line management role, this means reviewing the skills needs within your team, against the team's own objectives.

It will involve taking into account both the needs of individuals, but also anything that can help your department or team to work together as effectively as possible.

A key tool for identifying learning needs at this level are appraisals or performance reviews. Normally undertaken annually, appraisal provides an opportunity to review work objectives for the previous year and agree objectives for the year ahead. Think about how you can support your staff (or volunteers if appropriate) in identifying learning needs related to these objectives.

SMART Objective
SMART is a way of checking that your objectives are clear. It applies to both work and learning objectives.

Specific: You know exactly what it is you have to do

Measurable:
There is a clear way of knowing when you have done it.

Achievable: It is achievable within your reasonable control

Realistic:
It is a realistic goal bearing in mind the time and the resources available (doesn't mean it shouldn't stretch or challenge you!)

Time-bound:
There is a date or deadline for achieving the objective.

Appraisal form design should include a section dedicated to learning and development. This can be kept separate from other areas of the appraisal form, so that information on training requirements can be included in the training and development plan, without making confidential information from the appraisal available to whoever is working on the plan.

Relying on an annual appraisal to identify learning needs will not allow for the flexibility of addressing challenges as they arise, so think about how you might build in more frequent reviews, for example, as part of regular supervision sessions.

You might also consider using a **Competence-Based TNA Diagnostic tool** (see Appendix 3) to help with identifying job-related learning needs. This example is designed for volunteer managers and draws on the relevant national occupational standards, and you can adapt this format using any relevant competency framework.

Skills for managers

In order for training/learning needs analysis to be effective, line managers will need to have the necessary knowledge and skills to work with staff and/or volunteers to help them identify their needs and how to meet them.

You might consider using a competency framework as a basis for job design, appraisal and training needs analysis. Competencies are statements of effective behaviour in meeting a particular outcome. You can develop competencies internally or draw on existing competencies as a starting point.

Managers can also be instrumental in identifying the broader skills and knowledge resource base that exists within the organisation. People may well have knowledge and skills that are not fully demonstrated within their current jobs, but which could be used in other ways – for example in mentoring new members of staff.

It may be that many learning needs can be dealt with on a team level, for example through cascading information at team meetings. However, this is more likely to be effective if it takes place within a system and culture which makes it easy for people to identify and ask for support from team members.

Creating a learning culture
A learning culture is one in which learning is valued and is embedded across an organisation. It takes time and commitment to establish a learning culture.
Here are some of the ways in which you can encourage and raise awareness of the value of learning:

- People learn a lot from teaching others – encourage people to share what they know with others – in writing, at team meetings, at staff conferences and events, informally
- …….

Individual Level

Appraisal and supervision meetings allow individuals to reflect on their own learning needs in relation to their work objectives. What additional skills and learning do they need to improve what they do?

It is important to take into account people's career ambitions and personal development objectives. With flatter organisational structures, there may not be endless opportunities to move up the career ladder, but people are unlikely to remain motivated if there is no progression or challenge built into their work.
However, there is also a need to be realistic about what you can offer by way of development opportunities and not to raise expectations too high.

Assessment tools such as 360 degree feedback systems can be helpful in getting a more rounded picture of individual performance, and the impact that people are making at different levels within the organisation. This tool is perhaps particularly appropriate for those in management or leadership roles.

Identifying learning needs at individual level is not just about what needs to be learnt, it is also about how best to do it. Find out how people have enjoyed and benefited from learning in the past. More information on learning styles visit the.

Some questions to ask for your personal development plan

1. What do you want to get from your work?
2. What are your strengths?
3. What areas would you like to improve?
4. Where would you like more responsibility?
5. What is preventing you from developing as you would like?
6. Which interests or talents would you like to develop?
7. How do you like to learn?
8. What skills or experience would allow you to feel more confident at work?

The outcome of training/learning needs analysis at an individual level should be a **Personal Development Plan** (see Appendix 4) which outlines personal learning objectives, linking them to the agreed work objectives.

Methods of meeting Learning Needs

There are many ways to meet people's learning needs. The methods you choose to meet the needs will depend upon how people prefer to learn, the number of people needing training, and your budget. Think also about any special needs people may have and how to support them, so that your training is equally accessible to all who need it.

Some of the methods you could consider are:

In-house courses

Developing a course to be run on your premises and tailored to the needs of your staff and volunteers. Useful if the training need is widespread across the organisation or is quite specific to your needs, for example training on a new system or process.

You might commission an external trainer to develop and deliver the course, or ask someone with relevant expertise within the organisation to deliver the training. If the latter, you might need to ask whether there is a need for some "train the trainer" training to ensure that they can communicate their knowledge effectively.

External training courses

Attending external training courses have the advantage of allowing you to network and learn from people in other organisations. This networking element is one of the reasons classroom based training remains so popular. External training can be expensive, but there are many courses available that are priced at affordable levels for voluntary organisations, sometimes on a sliding scale. Good starting points for information on local training are local infrastructure organisations.

Conferences and events

Conferences are ideal for getting up to date with developments and for networking and learning from others. For information on some of the events being run within the voluntary sector, try the Improving Support website which provides information on conferences and learning events being run by the National Support Services in areas such as HR and Employment Practice, Volunteering, Campaigning and Equality and Diversity.

- **E-learning/Blended Learning**

E-learning is increasingly being used to supplement traditional courses. With the developments in technology, structured E-learning is becoming more sophisticated and can be tailored to individual and small groups of learners. It can be used to provide large groups of people with the same material whilst still allow individuals to learn in their own time.

- **Mentoring**

Typically, mentors will be experienced managers (but not individuals' line managers) who regularly meet more junior colleagues to help them perform better and develop them for career advancement.

- **Shadowing**

Shadowing involves spending a short period time with someone in a different job – either within your own organisation or externally. This might include sitting in on meetings, observing how day to day tasks are done. Shadowing can be useful as part of an induction when you shadow more experienced staff.

It can also be used as a development opportunity where both parties can learn from each other, as being shadowed can help you review the ways in which you habitually work.

Prioritising learning needs

Once you have identified learning needs across the organisation, they need to be analysed and prioritised.

Areas to consider when prioritising:

- What impact will developing these skills have on our performance?
- What would be the cost/benefit of investing in developing these skills
- Which skills needs are the most important to our long-term success?
- Which skills needs are the most urgent?

Cost/benefit analysis means assessing the potential costs of learning and development activity against the potential gains in a quantifiable way. Making the case for the value of learning interventions to decision-makers and funders for investment in training is strengthened by a cost/benefits analysis. Potential gains might include:

- reduced turnover and savings on recruitment costs
- higher skill levels leading to more efficiency and fewer errors
- reduced risk of accidents or breaches of legislative requirements
- higher morale and levels of motivation
- impact on fundraising capacity through a higher skills base
- improvements to the quality of your service and reputation
- sustainability and succession planning

Of course, training or learning interventions will not always be the appropriate solution for organisational issues, and the process of undertaking a TNA and a cost/benefit analysis is likely to highlight areas where other solutions are required.

Evaluation of learning

It is important to consider evaluation of learning and development activities at the planning stage and build this into your TNA. Strong evaluation will help in planning future training and learning activity that has shown itself to be effective. The widely used Kirkpatrick model identifies four levels of evaluation.

Level 1 Reaction

This asks learners how they felt about the learning experience. It is usually assessed by means of a course evaluation questionnaire or "happy sheet". There are alternatives to questionnaire – for example you could end a training session by asking people to jot down answers on post-it notes, for example: what I liked? What could be improved? What I learnt? What else do I need to learn about the subject? These can then be collated on a flipchart.

Level 2 Learning

This will assess what has actually been learnt. So if the learning objective was some essential health and safety information, this could be tested with a quiz. If it was the ability to perform a particular task such as producing a spreadsheet or chairing a meeting, this could be tested and observed in the workplace.

Level 3 Behaviour

This looks at the effect the learning intervention has on an individual's behaviour in their job. This could be assessed by reviewing changes in knowledge, skills and competence as part of the supervision and appraisal process.

Level 4 Results

This looks at the impact of the learning on organisational performance as a whole. If the learning objectives are clearly linked to organisational objectives, then data linking learning to organisational changes will be easier to obtain and analyse.
Directly linking learning and development activity to overall performance is not always easy to do. However, if you carry out something like a SWOT analysis on an annual basis, trends can be assessed over time.

The Learning and Development Plan

Once you have reviewed the data gathered at organisational, team and individual level, bring this together into a **learning and development plan** (see Appendix 5).

The plan should not only identify the learning requirements within the organisation but should prioritise them and set out the ways in which the requirements can be met, the resources needed, the timescale, and the way in which the learning will be evaluated.

Appendix 1: Diagnostic Template
Identifying and meeting learning needs

This diagnostic looks at the organisational processes which can support training/learning needs analysis, and signposts to external resources that can help with filling gaps. Information and additional resources on these various areas can also be found within in the TNA section of the Skills

Question	Yes/No	Resources
Planning		
Do we have a strategic and organisational plan?		
Do we have a training strategy and/or a stated commitment to the value of learning and development for our staff/volunteers and trustees?		
Do we have a training budget?		
staff		
Do we have up to date job descriptions and person specifications for all posts?		
Is there a robust induction process in place for new staff?		

Do we have an appraisal system in place?		
Do we want to work towards externally recognised good practice standards in managing and developing our people?		
Are line managers competent in supporting the learning and development of their staff?		
Do we know where to access relevant training for our paid staff?		
Do we evaluate our training?		

Appendix 1:

S.W.O.T Analysis template

Strengths	*Weaknesses*
Opportunities	*Threats*

Appendix 3: Learning and Development Plan

Organisational Objective	Knowledge and skills required	Who will participate?	Learning and Development activities/methods	How will this be evaluated?	Cost	Date

Information Governance

Training Strategy

October 2022

Contents

1. Introduction

Information Governance is about how to manage, process and share personal data safely and securely, and particularly protection of our patient and staff data. Policies and guidance are clear and consistent and freely available to everyone working with NHS Lothian through a number of different training resources.

The training strategy identifies the varying learning needs within the organisation in Information Governance and Data Protection including NHS Lothian's core mandatory learning requirements and covers the following staff areas.

Staff who deal with Subject Access Requests (Annex A)

- Medical Legal Staff
- Dental Administrators
- Prison Staff
- GP Practice Managers
- Staff working in the Patient Experience Team
- All other staff within NHS Lothian

Staff who require essential information Governance training (Annex B)

- Information Governance & IT Security Staff
- Managers and Project Officers
- Data Sharing & Information Asset owners
- Senior Managers
- eHealth Senior management Team
- eHealth training staff
- HR Managers
- Executive team including Information Asset Owners
- All other staff within NHS Lothian

Staff who require essential data sharing training (Annex C)

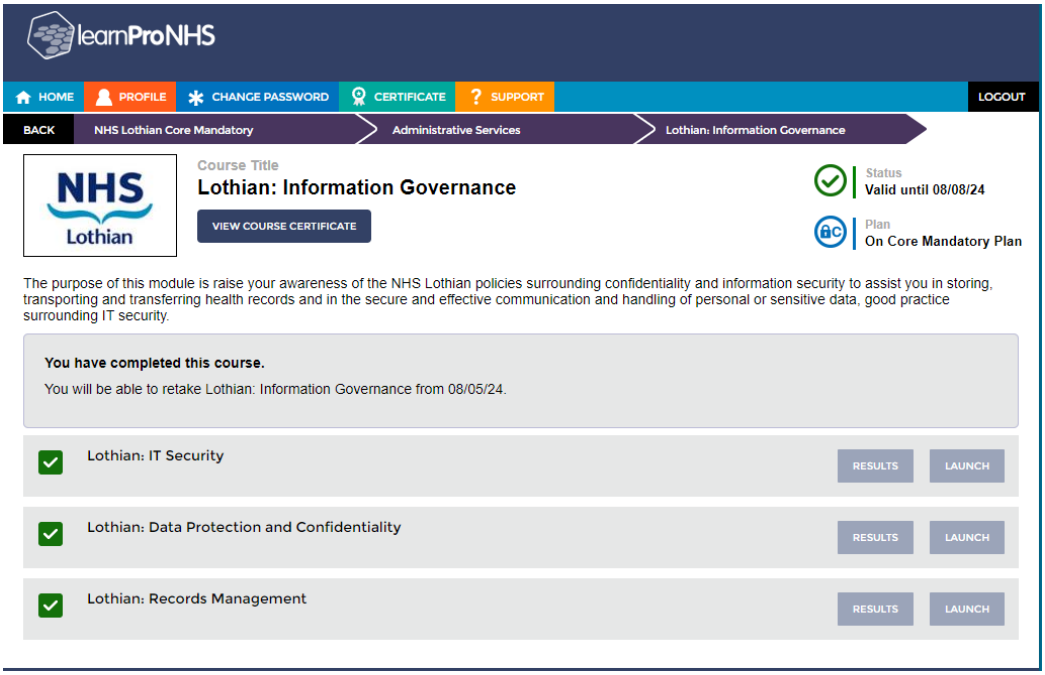
- Senior Managers
- Information Asset Owners
- Information Asset Administrators
- IG Project Officers
- SAR Team
- IG IT Security Staff
- Projects Team
- Innovation Team
- R&D staff
- Patient Experience Team (PET)
- All other staff within NHS Lothian

2. Core Mandatory Learning Needs

The organisation has a number of core mandatory learning requirements which must be undertaken by all new employees during their induction. The following Information Governance modules are completed through the organisations Learnpro software and repeated every 2 years by all staff. Some GP Practices have access to the LearnPro modules while some GP practices have their own Information Governance learning requirements that must be completed by their staff.

Lothian: Information Governance

- IT Security
- Data Protection Policy
- Records Management



Staff who do not complete online modules (e.g. ancillary staff without access to IT requirement" have specific presentations and videos delivered on mandatory Information Governance as "tailored talks". Thes are also on employment and every 2 years thereafter.

3. Methods of Meeting "Other" Learning Needs

Analysis and identification of other learning needs is undertaken within the Information Government team through a number of resources.

1. NHS Lothian Safety & Learning System (Datix) - This is web-based software where all staff record any potential data breach/safety concerns regarding patient or staff data. Information Government respond to the concerns being logged by staff in order to provide appropriate advice on how to mitigate and resolve the data breaches. Over a period of time the concerns are analysed to identify any patterns of concern and provides Information Governance with

the information needed to create and facilitate “other” training needs.

2. Fairwarning. This is the NHS Lothian monitoring system that tells us who, where and when staff are inappropriately accessing or downloading information on to electronic devices and what kind of information. When numbers are high against inappropriate staff access and downloading, Information Governance act appropriately. There are a number of training and guidance resources available for staff which Information Governance will advertise and make available via their own Information Governance Intranet Page.

Department and staff requests. Information Governance are contacted throughout the year to provide specific topics of data protection training to their departments and staff. Where there is a pattern to the types of requests being received Information Governance will create and facilitate “other” training needs.

3. Organisation wide Newsletter – Information Governance publish a quarterly newsletter on current data protection and IT Security practices offering practical help and advice. Training requests are often received following publication of the Quarterly newsletter.

4. Staff data protection survey – This is a newly introduced survey. Once a year Information Governance include a survey within the newsletter asking staff for feedback on what they would like to see in the newsletter. The survey also asks for specific training or guidance needs staff would like to undertake or be made available to them via the Intranet. The survey also asks pertinent question in relation to staff knowledge to gauge understanding and pinpoint areas for further learning.

5. Information Governance staff – ongoing training and development of staff through the annual Performance Development Plan via TURAS ensures that all staff continue to develop their knowledge within the role. Staff can reflect on their own learning and plan what further learning requirements are needed. This provides line manages with information on what training requirements are needed for all staff.

6. General Practice staff - ongoing training and development of staff in general practice setting. This will include; subject access and disclosure training, redaction training, general awareness session and Managers Bite Size session for GP’s and Practice Management. If required adhoc training can be provided when requested.

7. Knowledge and Skills Framework (KSF) Post Outline describes the knowledge and skills that need to be applied to each staff post within the organisation. Patient confidentiality and data protection fall within a number of the dimensions. Staff have an individual responsibility to ensure they meet the requirements of their KSFs and will contact Information Government with training requests. These requests facilitate the need for Information

Governance to review their training content and whether they need to provide additional training resource for the organisation.

8. Senior executive staff learning sessions. These are tailored and delivered by in house or external providers for the senior organisation team.

9. One off “all user” messages if the need requires.

The identification of “other” training needs involves considering both the needs of staff as individuals, but also anything that can assist NHS Lothian’s knowledge and awareness in Information Governance and Data Protection as an organisation. These are covered in the Information Governance Training Needs Analysis (TNA) for all staff at Annex B

4. Subject Access Requests

By the nature of the data held in NHS Lothian it is essential that this specialist area of the Data Protection Act is understood by all staff. In particular, the staff groups responsible for the compilation and dissemination of Subject Access Request require to have fundamental knowledge and learning in this area.

With this in mind NHS Lothian have a separate Training Needs Analysis (TNA) table which outlines the varied training options provided to and available to the staff groups - Annex A

It is important that line managers responsible for staff undertaking the Subject Access Requests along with the Information Governance team have the necessary knowledge and skills to work with the staff and support them with Subject Access Requests.

5. Learning Types

There are many ways to meet the learning needs of the organisation. Information Governance use a variety of types of learning methods in order to match people’s preference. Generally, there is more than one type of learning for a particular subject. NHS Lothian have a separate Training Needs Analysis table which outlines the varied training options provided to and available to the staff groups – **Annex B**

6. Information Governance Learning Types.

In-house training/presentation

Information Governance have developed a number of training presentations on a variety of data protection topics that have been tailored to the needs of all staff and the organisation. The training is available online for individuals to view via the Information Governance Intranet page or can be delivered in person or across video conferencing by the Information Governance team or Data Protection

Manager.

External training courses
Attending external training courses has the advantage of allowing staff to network and learn from people in other organisations. Departments hold their own budgets and have the final decision on whether their staff can attend relevant external courses recommended by Information Governance.

E-learning/Blended Learning
NHS Lothian has its own bespoke LearnPro system which has a number of core mandatory learning requirements that staff groups have to undertake. Induction takes place in the first few days of employment for all new members of staff must undertake the core mandatory learning requirements.

External Resources
There are a number of external resources used by Information Governance to develop staff understanding and knowledge as well as providing specific subject guidance.

Information Governance intranet
The Information Governance Intranet provides information and guidance to all members of staff. The site covers provides access to Data Protection and Security policies, processes, guidance, forms for completion, FAQ, training videos and copy presentations.

7. Evaluation of Learning

It is important to consider evaluation of learning and development activities and build this into your TNA. Strong evaluation will help in planning future training and learning activity that has shown itself to be effective. In order to do this we have developed appropriate questionnaires to be completed at the end of any training given.

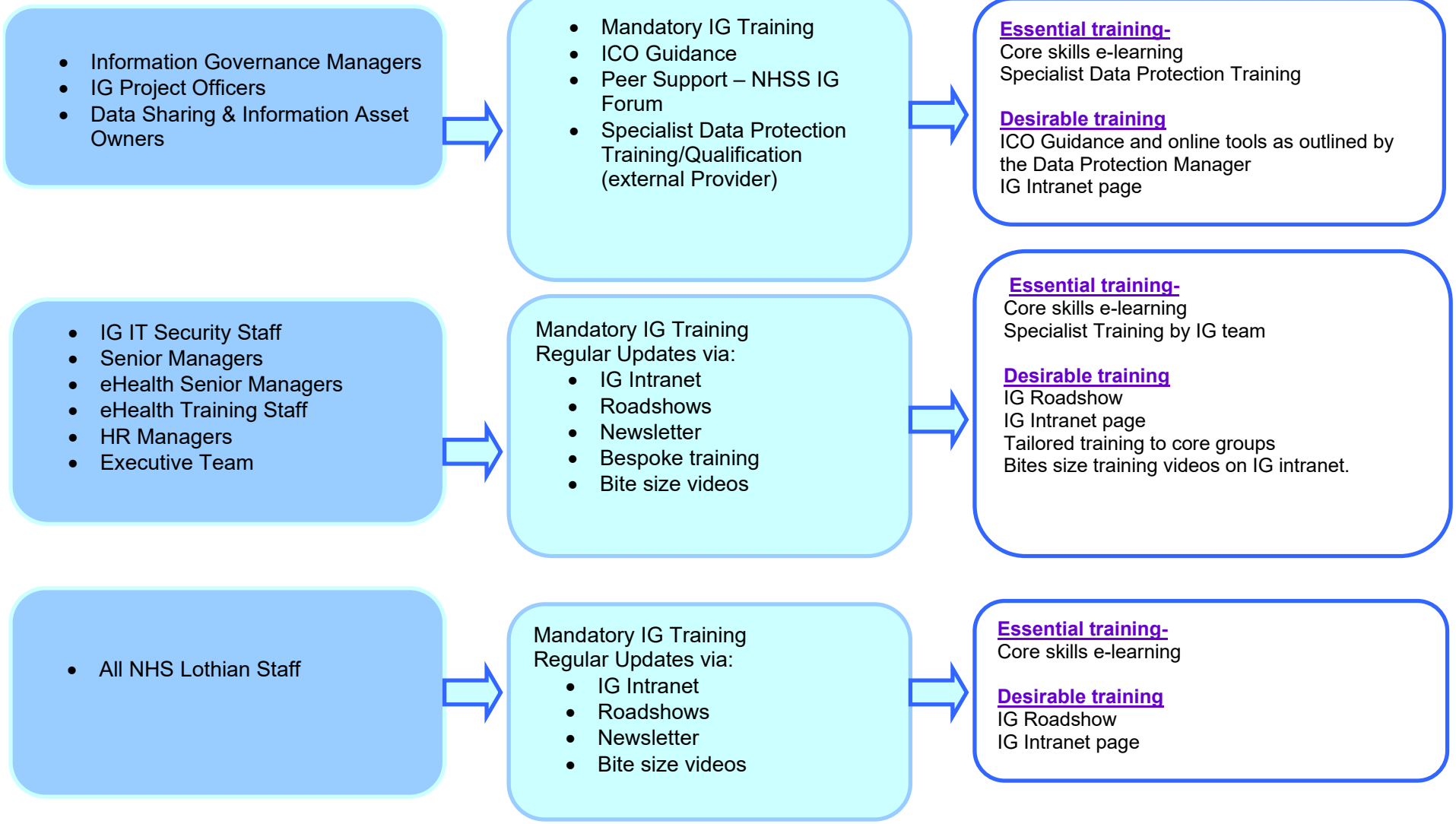
8. Annex A: TNA – Staff Dealing with Subject Access Requests

Recognising a Subject Access Requests: A Quick Guide to Essential Training

Staff Group	Training Required	Training to be Provided
Staff who deal with Subject Access Requests Medical Legal Staff Dental Administrators Prison Staff GP Practice Managers	Legal Background Subject Access Request: • Recognising • Processing • Handling • Redacting • Providing • Follow-up • Escalating	**Essential training-** Core skills e-learning Specialist SAR Workshop **Desirable training** IG Roadshow Redaction presentation/trainingDocuments & guidance on IG Intranet page
Staff working in the Patient Experience Team	Legal Background Subject Access Request: • Recognising • Processing • Providing • Follow-up • Escalating	**Essential training-** Core skills e-learning Specialist SAR PET Presentation **Desirable training** IG Roadshow Documents & guidance on IG Intranet page
All Staff including GP Practice staff	Subject Access Request: • Recognising • Escalating	**Essential training-** Core skills e-learning **Desirable training** IG Roadshow Documents & guidance on IG Intranet page

9. Annex B: TNA – Information Governance Training

A Quick Guide to Essential Information Governance Training



10. Annex C: TNA – Information Governance Training

A Quick Guide to Essential Data Sharing Training