eHealth Data Access Policy

Giving Access to NHS Lothian Data in the Course of an Official Investigation
Contents

Executive Summary                           Page 3
eHealth Data Access Policy      Page 4
Appendix 1
Removal of Data Procedure                  Page 6
Appendix 2
Data Monitoring Procedure                   Page 8
## EXECUTIVE SUMMARY – eHealth Data Access Policy

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Key Messages**              | The eHealth Data Access policy exists to comply with NHS Lothian Policy. All staff using IT should understand that they are contractually responsible for following policy, are appropriately trained, and know where to locate appropriate support. 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. The policy ensures that:  
• appropriate authorization permits access to Data for investigation; and  
• all employees are aware of the limits of their authority and the levels of their accountability for their actions.                                                                                     |
| **Minimum Implementation Standards** | All line managers should have local dissemination and implementation plans in place to ensure all staff that come into contact with IT or other electronic equipment are familiar and adhere to all aspects of this policy.  
All line managers of should have local dissemination and implementation plans in place to ensure all staff are familiar with and adhere to all aspects of this policy.  
Unauthorised breaches of NHS Lothian policy will be taken very seriously and may result in an investigation into the alleged breach, and may result in disciplinary action in accordance with HR Policy Management of Employee Conduct – Disciplinary  

### Good Practice for Managers
- Has identified the staff in his or her area to whom this policy applies and has given the policy (or selected excerpts) to them.  
- Has assessed the impact of the policy on current working practices, and has an action plan to make all necessary changes to ensure that his or her area complies with the policy.  
- Has set up systems to provide assurance to him or her that the policy is being implemented as intended in his or her area of responsibility.  

### Good Practice for Employees
- Has read the policy (or selected excerpts) and considered what it means for him or her, in terms of how to conduct his or her duties.  
- Has completed any mandatory education or training that may be required as part of the implementation of the policy.  
- Has altered working practices as expected by the policy.  

NHS Lothian eHealth Data Access Policy

1. The purpose of this policy is to provide appropriate access to NHS Lothian’s Data for the purpose of investigations or statutory obligations.
   • Information will be available to authorised personnel as and when required
   • Regulatory and legislative requirements will be met.
   • All breaches of information security, actual or suspected, can be investigated by an IT Security Officer with assistance of technical personnel.
   • all employees are aware of the limits of their authority and the levels of their accountability for their actions.

2. Data and information takes many forms including but not limited to, data and metadata stored on email, systems and internet access logs, network areas, computers, tablets, transmitted across networks, printed out or written on paper, sent by fax, stored on CD, DVD, tapes removable media, or spoken in conversation, including over the telephone.

3. There are a number of Policies and Guidelines that form the legislative and administrative basis for this policy and includes but not limited to:
   • NHS Lothian eHealth Security Policy
   • NHS Lothian Management of Employee Conduct: Disciplinary Policy and Procedure
   • Data Protection Legislation,
   • Computer Misuse Act,
   • Information Governance Policy
   • Data Protection Policy
   • Confidentiality of Personal Health Information Policy

4. Under Data Protection Legislation, NHS Lothian is, as a Data Controller responsible for the maintenance and security of all personal identifiable data and records it holds on any media including health and staff records. “Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”

5. It is the responsibility of each employee, contractor or volunteer working for, or on behalf of NHS Lothian to cooperate with this Policy.
All managers are directly responsible for implementing the Policy within their business areas, and for adherence to the Policy by their staff.

6. As an employer NHS Lothian is committed to providing its employees a working environment safe from bullying, harassment or threat and is obliged to set an example in the manner in which it protects its assets and contributes to that role.

7. It is the responsibility of investigating staff to ensure the confidentiality and integrity of the investigation and those under investigation. As such details of investigation should only be shared with the investigation team.

8. There is agreement within the regulations that both an organisation and its staff share responsibility for compliance.

9. The Director of eHealth, NHS Lothian will be responsible for the introduction and maintenance of the Data Access Policy and providing advice and guidance on its implementation and content.
Appendix 1

Removal of Data Including PCs and Devices for Investigation or as Evidence

1. Where there is a reasonable ground for suspicion that Data including email use, internet use, systems use, data storage etc may have been used by an individual to contravene existing NHS Lothian policies including but not exclusively those relating to Confidentiality or Dignity at Work; Any of the following staff may authorise the one off search of an individual’s activity for investigation or as evidence
   - Director of Human Resources
   - Associate Director of Human Resources
   - Head of Human Resources
   - Director of eHealth
   - Head of eHealth Operations and Infrastructure
   - Information Governance and Security Manager

2. It is good practice that any line management enquiry requiring removal of data will not be actioned without Human Resources authorisation to the eHealth Security Manager, Information Governance and Security Manager, Head of Operations and Infrastructure or Director of eHealth. These investigation requests must be in writing or email.

3. However for any suspected policy breach, potential Police or legal issue eHealth Security Manager, Information Governance and Security Manager, Head of Operations and Infrastructure or Director of eHealth, may authorise urgent or immediate seizure of data or PC/device for investigation. Justification must be recorded.

4. Technical staff will only be requested as appropriate to assist the investigation by eHealth Security Manager, Information Governance and Security Manager, Head of Operations and Infrastructure, Director of eHealth or Director of Human Resources. These investigation requests must be in writing or email, and confidentially stored (not on the eHealth helpdesk system).

5. The need for removal of evidence may be initiated through three main sources:
   a. Within the eHealth department from information gathered through routine examinations of the network or servers
   b. When asked by a departmental other senior manager through a suspicion or other evidence of improper behaviour.
   c. Court Order or other legal requirement

6. When the information is discovered through routine monitoring, the member of eHealth staff making the discovery is inform the eHealth Security Manager or Security Officer immediately, they will discuss this
with the Information Governance and Security Manager or senior eHealth managers the most appropriate approach.

7. Where the decision is taken by Human Resources to suspend a member staff during an investigation, they should inform eHealth so that the staff members access to services and systems are to be frozen or removed as appropriate.

8. The guidance within this Policy is taken from the Association of Chief Police Officers, ACPO, “Good Practice Guide to Preserving Computer Evidence”

9. When a PC is removed or a server drive is involved, no attempt is to be made to check the data held until two copies of those drives have been made. The PC and drive copies should be labelled and secured by the eHealth department. One of the copies will be used for initial forensic examination, the other held should a problem exist on the first or if external forensic specialists are required. The log of proceedings must identify all events and copies where they were made, when and by whom.

10. During the initial forensic examination if, at any time, any evidence of an illegal activity is uncovered, e.g. paedophile pornography or fraud, the investigation is to be halted and NHS Lothian senior managers advised prior to the investigation being handed over to the appropriate authority, Police Scotland or NHS Counter Fraud investigation unit.

11. Four principles1 must be followed at all times:
   • Principle 1. No action should be taken to change data held on a computer or storage media which may subsequently be relied upon in court.
   • Principle 2. In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
   • Principle 3. An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
   • Principle 4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

---

1 “Good Practice Guide for Computer based Electronic Evidence v.3”, Assoc of Chief Police Officers p 6
Appendix 2

Data Monitoring for Investigation or as Evidence

1. Where there is a reasonable ground for suspicion that Data including email use, internet use, systems use, data storage etc may have been used by an individual to contravene existing NHS Lothian policies including those relating to Confidentiality or Dignity at Work, the Director of Human Resources or Director of eHealth, may authorise the ongoing monitoring of an individual’s activity. This will be in compliance with the Regulation of Investigatory Powers Act.

2. Investigation requests must be in writing or nhs email.

3. The logs including archives will be made available to support any disciplinary or legal action against a member of staff or other user of the NHS Lothian Infrastructure.