eHealth Security Policy

Unique ID: NHSL.
Category/Level/Type:
Status: Final
Date of Authorisation: 01/02/17
Date added to Intranet: 01/02/17
Key Words: eHealth Security Policy
Comments:

Author (s): T McKinley
Version: 2.5.09 January 2017
Authorised by: Director of eHealth
Review Date: January 2019

Contents

EXECUTIVE SUMMARY – eHealth Security Policy

ELEMENT	DESCRIPTION
Key Messages	The eHealth Security policy exists to comply with NHS Scotland Guidance in addition to ensuring that NHS Lothian continues to treat IT assets and personal identifiable data with due care and diligence. All staff using IT should understand that they are contractually responsible for following good IT security practice, 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 levels of security are in place to maintain the confidentiality, integrity and availability of information and information systems; and • all employees are aware of the limits of their authority and the levels of their accountability for their actions. Guidance note 1 NHS Lothian Staff Guide to eHealth Security Policies provides a high level summary of this policy This policy is available on **Corporate>A-Z>eHealth>Operations & Infrastructure> Information Governance**
Minimum Implementation Standards	All line managers of should have local dissemination and implementation plans in place to ensure all staff who need to interact with IT or other electronic equipment are familiar and adhere to all aspects of this policy. Information Governance and Security 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 Information Governance module which ALL staff must complete. All line managers should have local dissemination and implementation plans in place to ensure all staff are familiar with 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 IT security 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.

1. Information takes many forms including but not limited to, data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on CD, DVD, tapes and diskettes, or spoken in conversation, including over the telephone.

2. NHS Lothian is, as an employer, 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.

3. There are a number of Policies and Guidelines that form the legislative and administrative basis for this policy including appendices and the following:
   - NHS (Scotland) HDL (2006) 41, NHS Scotland Information Security Policy
   - Data Protection Act 1998
   - Computer Misuse Act
   - Civic Government (Scotland) Act 1982
   - Copyright Design and Patents Act 1988
   - Defamation Act 1996
   - Obscene Publications Act
   - Civil Contingencies Act 2004
   - Freedom of Information Act (Scotland) 2002
   - Confidentiality and Security Group Scotland (CSAGS)Report 2001
   - Caldicott Report 2000
   - CEL 25 2012 NHS Scotland Mobile Data Protection Standard
   - Human Rights Act 1997
   - CEL 25 2011 – Safeguarding Personal Data in Contracts – November 2011
   - Records Management NHS Code of Practice V 2.1 January 2012
   - Public Records (Scotland) Act 2011
   - Information Governance Policy
   - Data Protection Policy
   - Confidentiality of Personal Health Information Policy

4. Under Principle 7 of the Data Protection Act 1998, 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. Information Security is, within the NHS in Scotland, managed as part of its commitment to Information Governance, which is an integral part of Clinical Governance. Adherence to this policy will ensure that the minimum requirements are always met and where possible meet the highest levels recommended.

6. The purpose of this policy is to protect NHS Lothian's information assets from threats, internal or external, deliberate or accidental. This applies to all health, personnel, finance or any other information held on electronic media or written on paper.

7. NHS Lothian eHealth Security Policies will ensure that:

    - Confidentiality of information required through regulatory and legislative requirements will be assured
    - Integrity of information will be maintained
    - Information will be available to authorised personnel as and when required
    - Regulatory and legislative requirements will be met
    - Business Continuity Plans will be produced, maintained and tested
    - Information security training will be available to all staff
    - All breaches of information security, actual or suspected, will be reported to and investigated by an IT Security Officer

8. NHS Lothian follows the guidance of HDL (2006) 46 in that it focuses on:

    - developing a security culture through training and awareness events and by providing awareness education and training materials
    - adhering to Scottish, national UK and European policy, standards and best practice guidelines for security and data protection in the NHS
    - managing Incident Reporting, so that all security incidents are reported and recorded using an Incident Reporting Form

9. This policy addresses four fundamental security principles
    - Authority
    - Accountability
    - Assurance
    - Awareness

10. Its objectives are to ensure that:
    - all Information Technology (IT) systems used in NHS Lothian are properly assessed to ensure that corporate procedures, responsibilities and IT security objectives, in particular the legal requirements, are fully met

- appropriate levels of security are in place to maintain the confidentiality, integrity and availability of information and information systems
- all employees are aware of the limits of their authority and the levels of their accountability for their actions
- Further guidance on the four security principles is given in NHS Scotland Information Security Policy which is available within the NHS Lothian Intranet

11. The Director of eHealth, NHS Lothian will be responsible for the introduction and maintenance of the Information Security Policy and providing advice and guidance on its implementation and content.

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

13. This Security Policy consists of this statement and a number of Appendices laying out specific controls and standards by which the aims of the policy are met. It also has a number of guidelines enabling users to adhere to the policies by following the guidance.

Appendices:

Appendix 1 Identity controls including Access to Applications and Network
Appendix 2 Email, Acceptable use policy
Appendix 3 Internet, Acceptable use policy
Appendix 4 Computer devices Controls, including Generic work stations
Appendix 5 Remote Access Policy, including University of Edinburgh and other Organisations
Appendix 6 Mobile Computing Devices, including laptops, PDAs and Wireless Devices
Appendix 7 Removal of PCs, for investigation or quarantine of server as evidence
Appendix 8 Business Continuity and Disaster Recovery Plans

Guidance:

Guidance 1 NHS Lothian Staff Guide to eHealth Security Policies
Guidance 2 Research Data Storage
Guidance 3 Safe Email Transmission

Identity controls including Access to Applications and Network

1. NHS Employees

a. It is policy of the Scottish Government that all NHS staff have access to email, internet, intranet and applications, both clinical and administrative, to facilitate them in carrying out their role and responsibilities in the support and management of patient services and to facilitate their training.

b. To enable this it is necessary to provide each user with access to the network and to the various applications. "Single sign on" for specified systems is available, in addition to Virtual Desktop access cards.

c. Each employee, during their induction process, will be provided a form by HR, which when completed and appropriately authorised an approved signatory, will allow that person access to the network, email, internet and major applications as required. As part of that process the new user will sign that they have read and understood those parts of this policy, which are attached to the form, mainly those relating to appropriate and inappropriate behaviour, confidentiality and use of email and the internet.

d. Those IDs will then be activated after the employee has been trained in the appropriate systems and applications. It is not within the remit of a manager to attempt to deny access to email or the internet to a member of staff, only to ensure that correct applications are selected and that the level of access to the applications i.e. the security group for the application is confirmed. Each site will continue, for the foreseeable future, to have minor differences as to where this training and allocation of ID is presented to the user.

e. As part of the creation of the user ID each user will be allocated by eHealth a "Home" Directory or drive. That drive will be held on a server and backed up as required by Appendix 8. The user will not have access to the local "C" drive. Where departmental or shared drives are required the user will be instructed by the departmental "owner" how information on those drives is to be recorded.

2. Non NHS, Non University employees including Bank and Agency

a. Where a non NHS employee, contractor, or volunteer requires access to the network a separate application will be made by their NHS sponsor for them to be allowed access to specific services or devices. These applications should be discussed with IM&T security prior to any agreement being reached or contract signed as what might seem to the contractor as reasonable may breach other internal or external connectivity agreements.
b. A standard NHS Lothian Network access form must be completed to request access. The NHS Lothian sponsor is responsible for ensuring the applicant has read and understood obligations to NHS Lothian eHealth security policy and under legislation
c. A register of non-NHS Lothian users should be held and regularly reviewed by eHealth.

3. University and Research staff

a. Before an application will be processed for a member of the University of Edinburgh staff or for a researcher who does not already hold an NHS contract of employment, a honorary NHS contract or a letter of Research Access must be granted by the joint (University/ NHS) Research Office.

b. There are specific methods for the interconnection between the University of Edinburgh and the NHS, how it is to be achieved and its management; these are outlined at Appendix 5.

4. Password Controls

a. The network and all applications are to be password protected. Each user is responsible for maintaining the security of their passwords for their network and application ID. Staff are not to write down their password and leave them where they may be overlooked or found by unauthorised persons. Passwords are not to be shared with others. During any investigation into unauthorised or inappropriate access to systems or material, where a person claims that they shared the password with others and are therefore not responsible for any misdemeanour will not be accepted in defence but the person declaring such will be automatically in breach of NHS Lothian policies and therefore subject to disciplinary action.

b. To facilitate the maintenance by users of passwords all systems will be set where feasible to force users to change their password every 42 days. Staff are provided information in how to select and manage passwords at:

c. “Guidance Note 1 Setting Passwords” to this policy. Where the ability exists in applications to force complex passwords e.g. over 6 letters and containing alpha-numerics, it shall be set to force that action.

5. Leavers

a. Each month Human Resources will supply the System Administration Team with a list of leavers from NHS Lothian. The users IDs will be made inactive immediately but the “Home” drives will be maintained for 3 months unless request for additional time is agreed with eHealth. During this period if a department wishes to access any business information stored on the drive an application should be made to by the service manager to the eHealth security officer to arrange the access or movement of files.

b. If a person has been or is about to be dismissed or suspended by NHS Lothian, Human Resources or the line manager are to inform eHealth immediately so that the ID may be blocked to limit any wilful damage that might be done subsequent to that event.

6. Access to Records

a. Throughout NHS Lothian there are a number of areas where health, staff and corporate records may be held on a variety of media including paper and electronic. Access to this information, particularly that information deemed as sensitive under the Data Protection Act 1998, mainly but not exclusively, Health and Human Resources must be controlled. All records must be retained in accordance with the NHS Lothian Records Management Policies, where sensitive records are held in an area to which access is to be controlled.

b. Access to records must be in compliance with Data Protection Act. A written request must be made to the Legal Services Manager or Data Protection Officer. Access to your own or records of those whom you do not have a NHS Lothian role in care or administration is not permitted. Access is monitored for this purpose.

7. Server Rooms

a. Server rooms are by their nature one of the most vulnerable areas of the IM&T infrastructure. To prevent loss or damage of the equipment held in these areas strict access controls are to be applied. Server rooms are to be locked at all times and a record is to be maintained of those accessing them. This record

may be electronic where an electronic swipe or other access system is in place. The access records are to be checked at least monthly and access lists reviewed at that time. Where an electronic process is not available a record is to be kept of all entering and the purpose of that entry.

- Records of those who have been given the door access pin code will be maintained by the Server Team Manager, who will arrange to change pin codes every 3-month and inform IT security Manager of the active dates of new pin codes. Pin codes also will be changed if a staff member leaves or changes job role and no longer requires access.
- Electronic door access lists should be reviewed by Server Team Manager every 3 months and inform IT security Manager of completion. If a staff member leaves or changes job role, the access right of this staff member should be removed.
- Records will be maintained of keys issued to staff members with detailing who has keys and when they were issued. Keys must be returned when a staff member leaves or changes job role and no longer needs access.
- If keys are shared, they will be stored securely and there will be a record in place to log when and by whom the key has been 'used'.
- External contractors are not to be allowed unrestricted access to server rooms and are to be accompanied whilst working in those rooms.

b. Server rooms are to have wherever possible air conditioning of sufficient capability to maintain the room within the ideal temperature range for the equipment operating there.

c. All server rooms should have uninterruptable power supplies sufficient to maintain the servers where there is a loss of mains power. Allowing the servers to operate normally or to allow a controlled shutdown of the servers in the event of a sustained period without power.

d. Server rooms should have fire suppressant equipment installed which is capable of operating in a manual or automatic mode.

e. Where it is necessary to base servers outside dedicated server rooms, e.g. small Medical Practices, those servers should be placed in a room which can be secured (risk assessment available), has sufficient ventilation, is not close to heat sources and is relatively dust free. The server should also be fitted with a UPS which will allow automatic shutdown of the server if mains power is lost.

Appendix 2 NHS Lothian eHealth and IM&T Security Policy

Email, Acceptable use policy

1 The NHS Lothian Email service is provided for business use. When email is sent from an NHS Lothian email account, or from a NHS Net account from a NHS Lothian member of staff, the recipient will tend to view that message as an official statement from NHS Lothian.

2 The NHS Lothian email system shall not to be used for any of the following:

a) Any activity that violates the laws and regulations of the United Kingdom. Without exception such incidents will be referred to the police.
b) The creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
c) Subscribing to non-business related mailings and/or newsletters.
d) Sending or forwarding chain letters, jokes and other non-business related files such as personal photographs, windows media files and Mp3 music files.
e) When staff are using the email system for personal use they must comply with email policies and be aware that the NHS mail gateways which are nationally managed, block all of these file types
f) Mass emailings (over 50 addresses) without prior authorisation.
g) Sending virus or other malware warnings unless requested by NHS Lothian eHealth Security staff
h) The sending of confidential or patient identifiable information out-with the approved mail address lists or groups. This list will be revised regularly and published separately to this policy and is available to staff via the intranet titled Safe Email Transmission.
i) Emailing externally attachments over 15 Mb. (NHS external mail connections are set nationally at a maximum of 18 Mb which includes text, metadata, and attachment)

3 Personal use:

a) Using an insignificant amount of NHS Lothian resources for personal emails is acceptable. Non-work related email should be saved in a separate folder from work related email.
b) Staff should remember that they should not use their NHS Lothian or NHS Net account for subscriptions to non work related email newsletters. (The selling of email address lists is, although illegal in the UK, one of the primary sources of addresses for spam)

c) Following the recommendations of the Information Commissioner during an Audit of NHS Lothian's compliance with Data Protection and handling laws the use of non NHS web mail services is not recommended.

4 Monitoring

a) NHS Lothian uses software to scan all email both incoming and outgoing emails for SPAM, viruses, inappropriate content, restricted and prohibited file types.
b) NHS Lothian may be required under the Freedom of Information (Scotland) Act 2002 or other relevant legislation to produce emails sent or received by any member of staff in answer to a request for information
c) Messages quarantined or blocked by the system may be inspected and read by ehealth Security before being deleted or released. All messages released will carry a comment that they may have had to be read to clear them for release.
d) Messages blocked will be held for a maximum of fourteen days after which they will be deleted.
e) Emails from an "unknown" source will be quarantined and automatically deleted. An "unknown" source is where an email sender has contrived to hide or disguise the source of the email usually the email carries some form of malware.
f) Users should not attempt to change the type of file extension on attachments to avoid files being trapped. This increases the probability of the email being quarantined.
g) Where there is a reasonable ground for suspicion that email 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 eHealth, may authorise the monitoring of an individuals email traffic and if appropriate a search through server archived eMail

5 Forwarding of Mail

a) When staff wish to grant access to their email to someone whilst away for a period of time they should use "rules" to forward mail or grant a colleague delegate access to their mail box. Auto forward to external organisations is not supported.
b) Staff should not use "rule of reply to" to auto direct recipient to reply the email to the 3rd party which doesn't appear on the original email message.

6 Clinical and “Generic” Mailboxes

a) Clinical and generic mail accounts may be set up to meet clinical or business needs. Each of these accounts should have a specific owner who is responsible for checking the contents of the mailbox and approving and granting delegate access to any other member of staff. When mail is sent from such a mailbox it will show as being sent by the owner or delegate on behalf of the generic title.

Appendix 3. NHS Lothian EHealth and IM&T Security Policy

Internet, Acceptable Use Policy.

1 Whilst it is in NHS Lothian's and its staff's interest to have open access to the Internet, that access can easily be abused. Access to the Internet has been made available to staff for the following but not necessarily exclusive business purposes:
   a) Clinical Advice
   b) Education and Training.
   c) Guidance and Policy Information.
   d) On line libraries and journals.
   e) Travel booking for NHS Lothian business.

2 Staff are allowed to make enquiries using the internet for a limited amount of personal time and it is their manager's role to ensure that that access is not abused. That personal access should be, prior to starting work, during breaks or after work. Staff should however not access personal ISP mail accounts as by accessing these directly, significantly increases the risk of introducing malware into the NHS infrastructure.

3 NHS Lothian access to the Internet in via the NHS national network N3 and within that network priority is given to National Clinical applications including the transfer of digital images to and from the PACS applications. These applications have priority on that network. Other applications including the use of Webex , Blackboard and other training applications have a much lower priority and at times will run slowly. Staff using these applications are to understand that these priorities are not set through out UK and that there is a risk when using these applications that full functionality may not be available on all occasions depending upon clinical priorities.

4 Blocking of Internet sites

a) It is necessary for eHealth to block certain sites and groups of sites in order to prevent those activities which are banned within the NHS Lothian by other policies and procedures. These include pornographic, gambling including the National Lottery Games, offensive, violent, dating, hacking, racist and weapons related sites. We also have to consider that when certain types of sites are used the amount of information being transferred can have a significant impact on the bandwidth that we have available for business purposes and therefore block radio stations. Between 9a.m and

5 p.m. on weekdays, access to sports and property sites is also blocked as there is no business reason for allowing such access.

b) Where sites are intentionally blocked by IT Security this is clearly indicated giving reason for blocking. These messages are in colour and provide a specific telephone number for the user to call. Other messages relating to Server or Network Administration that may occur due to a fault and should not be referred to the IT Security Team but to the eHealth Service Desk for allocation to the correct team

c) Should a member of staff consider that there is a business reason for a site in the categories above being placed on an “approved” list then the Clinical Director or Service manager of that member of staff should contact the NHS Lothian eHealth Security staff to have that site approved.

d) At any time that the available bandwidth is reduced to an unacceptable level for any reason then internet access may be further reduced on a temporary basis and without notice.

5 Monitoring

a) NHS Lothian accesses the internet through a number of proxy servers. These servers maintain a log of the transactions of all users going on to the internet, including sites visited. The logs will be made available to support any disciplinary action against a member of staff or other user of the NHS Lothian Infrastructure.

b) Staff are not to use external proxy sites in an attempt to bypass NHS Lothian filters. If staff are found to be doing so this may lead to to disciplinary action being taken against them, up to and including dismissal.

6 Bulletin Board Service, Blogs and Social Networking sites

a) Staff should, when using other external bulletin boards or Blog Sites, not place any material which may be deemed to be offensive especially where they are identifiable as a member of NHS Lothian staff.

b) NHS Lothian staff are to be aware that disciplinary and / or legal action could be taken against them where material placed on such site amounted to defamation of another individual, bringing NHS Lothian into disrepute or a breach of patient or staff confidentiality including from home PCs or private phones.

c) Human resources policy may apply e.g. Social Media Policy.

Appendix 4. NHS Lothian eHealth and IM&T Security Policy

Computer devices Controls

1 General

a) The desktop computer is the primary method of accessing electronic information across NHS Lothian. To meet the needs security and confidentiality a number of restrictions are placed upon staff and in the manner with which they access information using PCs. Although there are at present differences between sites in the controls on desktop computers the intention is to produce a standard desktop across NHS Lothian. This policy refers to those standards.
b) Unless exceptional circumstances exist NHS Lothian does not permit the use of shareware or freeware software packages on the infrastructure as it is often difficult to assess the risk that these packages may have on the infrastructure. If a department wish to test a package prior to purchase then approval to do so must be sought from the IT Security team.

2 Clinical Work Stations

a) There are locations where the standard PC would hinder clinicians in their access to clinical applications and where the standard settings are not applicable. Those PCs are referred to as “Clinical Workstations” they are used in areas where at any time several clinical users might require almost simultaneous access to clinical applications. There are restrictions placed upon those PCs.
b) Clinical Workstations have the following characteristics:
c) The logon is hidden and is not to be revealed to non eHealth IT support staff
d) Although access is permitted to the Intranet, access to the Internet is not allowed with exceptions available by agreement (e.g. Toxbase, PECOS..)
e) Individual email accounts are not available
f) All clinical applications available through the clinical workstation will have individual user IDs and passwords.
g) The screen saver will not be password protected.
h) Where departments wish the workstations to be able to access departmental shared drives, those departments shall be responsible for all documentation available on those drives and for any inappropriate comments in or changes made to those documents. Confidential or personal information should not be store in this method.

3 Standard computer device configuration

a) Each member of staff in NHS Lothian shall have their individual network account Identity and password. That user ID and password may be used on any normal NHS Lothian computer device. Each user is responsible for their ID and password which they should not share with any other member of staff and should not divulge that to anyone. If their password is compromised for any reason then the staff member should change their password immediately. Guidance on password setting and reminders are given in the Guidance section of this policy.
b) The network ID will allow access to Email, MS Office products, Internet and Intranet. Clinical applications will be available through the desk top but may require an additional ID and password to access those applications. .

4 Storage Drives

a) In order to ensure that data is not lost through failures of local drives and to provide staff with access to their information wherever they log on, access to the local computer device hard drive, “C “drive is not available. Each user will be given access to a personal server drive “H” where they shall store any information. That drive will be backed up each night as part of the local support tasks.
b) The use of this drive can preclude the user’s ability to download certain file types from the internet and if this problem is encountered the assistance of the Support Desk should be requested.
c) Users should not use this drive to hold personal, videos, games, music (MP3) or other non work related files.

5 Remote Management

a) Each computer device is capable of being managed remotely and this facility may be used when a user places a Service Desk call because of a problem. The use of a remote management tool will be discussed with the user by the support desk and a warning that it is in use will be shown on screen. The remote management toll is configured in such a manner that it is not possible to use without informing a user. This is to mitigate potential breach of the Regulation of Investigatory Powers Scotland 2000 (RIPS) which could lead to prosecution of any member of staff who took that action.

6 Antivirus

a) All computer devices in NHS Lothian are protected by an antivirus product. This product runs in the background and is automatically updated several times each day. Users are not to attempt to stop any updates especially during initial start up of the PC. Computer devices without this product may not be connected to the network.

7 Use of Storage Devices

In order to protect confidentiality the ability to “Write” to external devices has been restricted on PC’s by default. This includes the permissions to write data to USB Pensticks, Digital Camera’s, memory cards and other mstorage devices. Where a user requires the ability to write data to a USB Device, encrypted memory sticks are available to staff. An application should be made using forms available on the intranet. If it is believed that Identifiable person data needs to be stored on a Penstick or other USB device or non network drive, this must be encrypted and/or application is to be made to the Caldicott Guardian for permission to do so. This includes video and audio recordings.

8 Software

a) The computer devices throughout NHS Lothian are optimised for the use of clinical applications. Where it is necessary to load additional software onto a PC consideration must be given not only to the single user but also to the needs of the applications used through out the organisation which may be effected by conflicting requirements. It is therefore necessary to prevent users having the ability to load software onto any PC or network server. Where it is believed that software is required to be loaded onto the network then the local Support desk should be contacted for advice and especially prior to purchase of any packages which may impact on clinical services.
b) No software which is not owned and licensed to NHS Lothian is to be loaded onto a desktop or server including games, music or video applications without the permission of the IT Security.

9 Port Control

a) All computer devices have software installed that restricts the use of devices that are plugged into any interface on the PC. This can include but is not limited to:
    - USB Pensticks & Hard Drives
    - Digital cameras
    - USB Printers
    - Dictation Equipment
    - Modems & Wireless Interface Cards
    - Tablet

    No non NHS Lothian owned device should be connected to the network via a PC without authorisation by IT Security

    Where appropriate all users by default have the ability to read & write to these devices but some services are restricted. If access to a device is required then a request should be made to the IT Security Department.

Read Only restrictions are in place with all removable media unless the device is an NHS Lothian provided encrypted device.

Appendix 5. NHS Lothian eHealth and IM&T Security Policy

Remote Access.

1 Remote access to the NHS Lothian IT Infrastructure may be required for a number of groups:

- Home working by staff including occasional access for email
- Remote diagnosis and support of the by IM&T staff
- Remote access by University of Edinburgh staff.
- Remote access by IM&T suppliers
- Remote access for approved organisation following agreement of formal access agreement (e.g. contracted voluntary agency etc)

2 Home Working

a) The NHS Lothian Policy on home working can be found on the NHS Lothian Intranet under the HR policies. Within that document the risks involved in Home Working including IM &T Security are highlighted. When staff are connecting to the NHS Lothian infrastructure and especially to those systems in which Health or staff records may be held they are to do so in strict accordance with this Appendix.

b) Remote access to the NHS Lothian infrastructure shall be achieved only through a secure SSL VPN connection, or approved remote connection tool such as Secure Global Desktop. No member of staff should attempt to connect through a modem, or other equipment, or method which has not been approved by the NHS Lothian IT Security Manager. To connect, other by an approved method will be regarded as gross misconduct and may lead to dismissal.

c) When remote access is required an application should be made to the NHS eHealth Department on the relevant proforma by the Service or Clinical Manager on behalf of the member of staff requiring access.

d) If the home user intends to use a home wireless connection to the internet then that must be declared. Any home wireless installation should be encrypted to WEP 128 bit encryption as a minimum. When the home user is regularly working from home then the encryption level must be to WPA standard. All wireless devices are to have ad hoc or peer to peer networking selected off.

e) When connected to the NHS infrastructure the PC or laptop should not be left unattended or used by any other person including family members.

3 Support Team

a) Members of the eHealth support teams shall access the infrastructure through the same route as other staff but should use Terminal Services or equivalent Citrix client to access servers etc.

4 University of Edinburgh Staff

a) Clinical and other staff holding joint posts with the University of Edinburgh and NHS Lothian may apply for access to the NHS systems including email from their University desktops. Currently access to clinical systems may only be achieved through the University LAN and not from any other system and certain restriction regarding operating systems and browsers apply. Applications for such access should be supported by the staff member's NHS Clinical Director and be made to the NHS Lothian eHealth Department. When the request is approved the staff concerned will be give instruction on how to achieve the connectivity required. Patient information is not to be removed through this connection and stored outside NHS Lothian's infrastructure unless permission has been sought by the Caldicott Guardian including those with research project permission that has been given as part of the ethics approval of that project. All R&D projects must be registered with the joint University of Edinburgh and NHS Lothian R&D department .

b) At present access cannot be given to staff holding joint posts with other academic institutions other than via the processes in place for Home workers.

5 3rd Party Support

a) When an application is being procured that will require support by a contractor then the following are to be adhered to:
    - No contract should be signed until the IT Security Manager has approved the method of connectivity that is intended for remote connectivity.
    - Only in exceptional circumstances will the contractor be allowed to direct access to desktop devices. Where this is necessary, the department or contractor will be responsible for the costs associated in the creation of a VLAN within the network and will accept responsibility for any damage caused to any other system on the network.
    - The preferred method of connection is via N3 (NHS Network) Contractors wishing to use this are reminded that approval to use this can take up to 1 year, approval however allows access to any NHS organisation throughout UK
    - Secondary method of connection is using Secure Global Desktop. Local connection will be achieved through Terminal services and be directed to the specific server.

- Use of ‘PC Anywhere’ within that server is strongly discouraged and needs prior approval by IT security. Use of VNC software products will not be allowed without risk assessment and prior approval. Any detection of unapproved software will result in the connection being terminated and the 3rd party will not be allowed remote access. All subsequent work will require attendance on site.
- When a server is being initially set up remotely and is not attached to the network a dial in connection is permitted. That connection will be terminated prior to the server or device being attached to the network.

Appendix 6 NHS Lothian eHealth and IM&T Security Policy

Mobile Computer Devices, including laptops, tablets, Wireless Devices and removable media

1. Mobile Computer Devices and Media

A mobile computer device is defined as any easily transportable computing device that is capable of storing data.

This definition covers a very wide range of equipment, from the basic pen stick memory card, low cost pocket memo devices to extremely complex and powerful laptop systems. It also includes those devices which may hold data but are generally considered as another form of device. This could include laptop, USB memory sticks,I-Pods, MP3 players, digital cameras, camcorders, audio recorders, CD/DVD, PDA, Tablets, Blackberries, Smartphones, iPads, iPhones and other external hard drives and many other devices where the storage media is not primarily considered as being capable of storing patient or other data. Patient, staff or other corporate records shall not be stored on these or any other mobile devices except when specifically authorised after a risk assessment:

Although some of these devices are a reduced security risk, they can still hold data pertaining to the NHS Lothian staff or patients if authorisation has been given only. Any data held on them is therefore still subject to the Data Protection Act 1998 and their users must ensure that these regulations are fully observed. These devices can and often do pose a risk to the NHS Lothian Infrastructure as they can also hold and transmit into the network a range of spyware, virus and other malware. There is also a wide range of communication methods for these devices including, infra-red, wireless local area networks, as well as conventional Ethernet connections.

The nature of these devices and their portability mean that they pose a higher than normal risk of theft, accidental loss or damage and therefore greater level of security is imposed on their general use.

a. Only devices purchased or owned by NHS Lothian can be used to store NHS Lothian data.
b. All NHS Lothian mobile equipment should be security marked.
c. The configuration of NHS Lothian computing equipment must only be changed by authorised IT personnel, and must be configured in line with NHS Lothian's eHealth Security policy.
d. Users with remote access to Division systems will adhere to the Remote Access Policy.

e. All mobile devices must be encrypted and secured with an access password. This password must be kept confidential, user specific and also non-transferable.
f. Laptops with shared access must only be used following agreement with eHealth on management acceptance of procedures restricting access and use to named staff only.
g. The password must conform to Scottish Government and guidance on passwords as given in Guidance document 2 to this policy.
h. All information stored in NHS Lothian equipment, is the property of NHS Lothian. Requests for access to this information must be authorised by the Caldicott Guardian where any patient identifiable data is concerned.
i. The storing of patient identifiable data on mobile devices is not permitted without the express permission of the Caldicott Guardian, following a risk assessment.

2. If such data is required to be stored on a mobile device the user must be aware of the increased risk, and the following additional steps must be taken:
   a. The appropriate exception documentation has been authorised by the Clinical Service Manager.
   b. Approval has been given from the Caldicott Guardian
   c. An additional level password and encryption is employed on files containing patient identifiable data.
   d. The data is transferred to a server drive as soon as it is reconnected to the NHS Lothian infrastructure.

3. Antivirus and Patching

   a. When the device is re-connected to the NHS Lothian network it will be updated with Antivirus software and any operating system patches prior to any additional work being carried out. Laptops are configured to retrieve updates from the antivirus vendor's website when a direct connection to the NHS Lothian network is not available. The user shall not make any attempt to prevent this occurring.

4. User responsibilities.

The users of mobile devices also have additional responsibilities

- Any breaches or suspicion of breaches should be reported to the eHealth Helpdesk or IT Security Officer immediately.
- The users of mobile devices are to comply with the IT security policies and guidelines as outlined in NHS Lothian IM & T Security Policy and in particular with those standards covered in this appendix.
- Only NHS Lothian staff are permitted to use the NHS Lothian's Mobile devices.

- Personal mobile computing devices are not permitted to connect to the NHS Lothian networks unless prior authorisation has been granted by the NHS Lothian eHealth Security Manager.
- Personal devices (Bring Your Own Device – BYOD) must be authorised for connecting via NHS Lothian Wifi via an authenticated service.
- Where a wireless connectivity is available on a mobile device it will be:
    - Defaulted off whenever the device is connected to an Ethernet (wired LAN) or 3G connection
    - Have “peer to peer” or “ad hoc” connections disabled preventing wireless connectivity with another computer.

5. Wireless Networks

Wireless devices, whilst convenient are inherently insecure and may interfere with clinical devices including wireless patient bedside monitoring.

- Only those wireless networks which are approved by the NHS Lothian Director of eHealth are to be used anywhere within NHS Lothian or where NHS Lothian Information is being shared on a network.
- The placing of a wireless device within the NHS Lothian Infrastructure without that approval by any individual or group may be considered as a gross misconduct if done by a staff member or breach of contract if activated by a supplier.
- Only approved BYOD users may connect via agreed authenticated services.

Where a wireless network is being considered then the advice of IT Security is to be sought on its suitability and the resources required for its management. Any requirements specified for its use are to be agreed prior to any procurement being initiated. The wireless network is to be set in accordance with the “Guidance for Wireless Networks, Connecting for Health Feb 2006” or equivalent document”.

6. Digital Cameras and Camcorders

Digital Images are to be stored and used in accordance with the guidance given by the NHS Lothian Medical Photography Policy. Where a digital camera is to be connected to the network to transfer images or to work in conjunction with a microscope it will require to be whitelisted in Lumension Sanctuary control. Application for this is to be made to the eHealth security team

7. Blackberry and other Telephone or Smartphone Devices

a. At present only Blackberry devices provided through the NHS Lothian Telecoms department are permitted to connect with NHS Lothian internal mail.
b. Staff using these devices are to report loss or theft of these devices immediately to the Telecoms team via the NHS Lothian Switchboard service
c. Where a smart phone or iPhone is synchronized to receive NHS.net mail and personal schedules. The following is to apply
   - The national helpdesk number is to be recorded separately so that in the loss or theft of the device the national Help desk may be contacted and data remotely wiped.
   - Connection to NHS.Net mail and schedules are to be in accordance with the guidance given within the NHS.Net code of connection agree by each user.
   - The mail client on a device which would download data to the device, you should use the nhsmail web client (www.nhs.net)within the browser and tick the box to say that it is a public computer. This will restrict to a degree what you can do with attachments but most ordinary mail can be handled safely and no differently from you using it on your home PC and given that nothing resides on the device the risk of it being a mobile device is mitigated. This is quite an important factor as no NHS Lothian data should be stored, even on a temporary basis on your personal/ mobile device.

8. Encryption

i) In line with the NHS Scotland Mobile Data Protection standard all Laptops and mobile data devices including removable media in use within NHS Lothian are encrypted using a using AES256 standard or equivalent approved full disk encryption product. This software prompts users to enter their log in credentials prior to the system booting.

9. Firewalls

ii) Where available all Mobile Devices are to be protected with a software firewall configured to only allow inbound access to recognized NHS Lothian services. The user shall not make any attempt to modify this.

Removal of computing devices, for Investigation or Quarantine of Server as Evidence

1. Users and managers should note there are occasions when either a PC may be required to be removed from their normal location, or information held on servers, including the Storage Area Network Systems (SANS) may be required for investigations. As the removal or quarantining of evidence is normally part of a serious investigation, this process is not to be undertaken lightly. It is often the prelude to a disciplinary process which may lead to dismissal or even criminal proceedings. It may also be required where the evidence held may be required by a tribunal or other process. In this latter case it is probable that it will have been preceded by a court or other statutory instrument being served on NHS Lothian. Which ever applies these processes are not to be initiated without the approval of an eHealth Executive Manager or without the permission of the NHS Lothian IM&T Security Manager in their absence.

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

4. The need for removal of evidence may be initiated through three main sources:
    a. Within the IS 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

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

6. When the request is from a departmental or service manager, it must be stressed that this is a serious matter and that the manager must be prepared to justify that the alleged offence is in clear breach of NHS Lothian policies. That request should be made formally, in writing or by email to the Director of eHealth, one of the eHealth Executive Managers or to the IM&T Security Manager in their absence. As this sequence of events may lead to disciplinary or criminal action it is

essential that the evidence be preserved and that a log of proceedings must be maintained throughout. An IM&T Security Officer will be allocated to the investigation and will have responsibility for initiating and maintaining the log.

7. The location of the staff or group under suspicion will determine the actual process to be followed as due to the differences in the infrastructure throughout NHS Lothian. The process to be adopted must be discussed and agreed prior to any PC or drive being searched or withdrawn from service.

8. That discussion must include the following personnel:
    a. eHealth Security Officer,
    b. Manager of department or of any individual under suspicion of wrong doing,
    c. Staff side representative, member of server or desktop support team responsible for that site and a member of HR department.

9. Where a computer device is involved or suspected of being used illegally the internal cache of that computer device may hold information which can be tied directly to an individuals log in ID and personal profile. Even where no access is routinely granted to the local hard drive by a user this information is cached on the local drive and may remain on that drive for the life of the computer device. It should be considered that where only a suspicion of an illegal process is held or where information is routinely stored on a server drive, removing the device for detailed analysis might be the only course of action. If necessary the member of staff should be informed of the nature of the suspicion by their manager in the presence of the staff side and HR representative. They should be asked about the matter under investigation and whether they have any comments. They should also be asked to disclose any passwords for any files and folders under their control. The device should be removed and if appropriate another connected. The "Home" drive of the member of staff should be frozen and another allocated if the staff member is to be allowed to continue in post whilst investigations are undertaken. Where the decision is taken to suspend a member staff during an investigation, their access to services and systems are to be removed.

10. 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 IM&T 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.

11. 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 or NHS Fraud investigation unit.

12. Four principles[1] 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 8 NHS Lothian eHealth and IM&T Security Policy

Business Continuity and Disaster Recovery Plans

1. The IM&T systems throughout NHS Lothian are critical to providing services directly for patients. Without these systems patient care cannot be delivered at an appropriate level. It is essential that processes and procedures are in place and tested which will allow NHS Lothian to provide patient care with minimum disruption at any time or for any reason. As part of the National Critical Infrastructure the NHS has a responsibility to protect that infrastructure and a legal requirement under Civil Contingency Act 2004 to have a continuity policy in place to cope with major incident, civil disaster including a pandemic.

2. Previously NHS Lothian's IT infrastructure was coterminous with its provision of service, its outer perimeter however no longer ends at the boundaries of NHS Lothian. With a number of international companies supplying services to NHS Lothian through internet connections and an increasing number of staff remotely accessing clinical systems and other services from home and elsewhere it is now world wide. It is therefore necessary to impose restrictions on its use to prevent abuse.

3. The critical areas may be broken into several categories:
    i. Network
    ii. WAN & LAN
    iii. Servers
    iv. Clinical Systems
    v. Trak/PAS/PIMS
    vi. Investigations and Monitoring
    vii. Ilab/PACS/RIS
    viii. Clinical Reporting Systems
    ix. Vision/SCI results/Gateway/UCS
    x. Non Clinical systems
    xi. Email
    xii. Finance and procurement
    xiii. PCSMR

4. **Network**

a. The network may be exposed to various types of incident:
    i. Physical Disruption through accidental or deliberate damage
    ii. Denial of Service through “malware” or email attack.

5. Disruption through Damage

Whilst it is possible that elements of the Wide Area Network (WAN) could be subject to an terrorist attack occurring at, or close to a building where one of its numerous switches are based, disruption of the service is most likely to be achieved by a person accidentally cutting through a cable during road maintenance. There is by the nature of the WAN, sufficient redundancy on routing between the main sites to avoid total loss of services to all sites. Should such an event occur the most likely occurrence would be an apparent slowdown of access to the various systems.

Should this occur, a warning will be sent to all users to reduce email traffic to a minimum and restrictions would be placed on access to the internet.

6. The WAN is maintained by Capita as part of the SWAN (Scottish Wide Area Network) national network procurement. It is possible that some health centre or community hospital which have only a single connection from the WAN might be isolated and loose connectivity whilst repairs are carried out.

7. All network communication and node rooms containing network switches and other devices are to be locked and access to those rooms restricted. An access list is to be maintained. Contractors or other unauthorised staff are to be accompanied whilst in these areas.

8. Denial of Service

9. A denial of service attack can be initiated through a number of events; the introduction of a Virus, Trojan or Worm into the network from sources including, external email, CDs, Pensticks and other USB storage devices. It can be triggered by a member of staff creating a chain email and it being forwarded to and from other staff. This effect simulating heavy traffic can also be produced by some “spyware” being introduced to a computer device whilst the user is on the internet.

10. To reduce and mitigate the effect of such attacks NHS Lothian has a number of defences in place including; Intrusion Detection Systems, antivirus applications, restricting the number of staff able to send “everyone” emails, restricting access to the network to NHS devices and NHS approved organisations, only allowing staff access to USB devices after a clear business or clinical need has been established.

11. NHS Lothian also filters incoming and outgoing mail for known virus definitions and blocks certain types of files which are known to present an increased threat to its services. This functionality is described at Appendix 2 .

12. All NHS Servers and PCs attached to the network are to have active NHS Lothian provided AV applications running to prevent virus or other attack

13. Clinical Systems

14. All the major clinical systems are server based and the servers are to be situated within Server rooms.

15. The server rooms are to be locked and access controlled. An access list is to be maintained and a record is to be kept of all staff entering the server room. Where entry is via a swipe card the entry log must show who entered the room and when they did so. Contractors and others not on the access list are not to be allowed un-supervised access to the server rooms.

16. All servers should be connected to either an individual or room served, Uninterruptible Power Supply (UPS). The UPS is to be capable of allowing a controlled or managed shutdown of the server(s) in the event of a loss of power.

17. The UPS when it is activated should be capable of sending a warning message to an IT Support team.

18. Server rooms are to have air-conditioning fitted wherever necessary to allow the servers to operate within their optimum temperature range regardless of the outside temperature

19. Servers

20. All servers are to be backed up in an approved cycle. This cycle should provide the ability to restore both the operating system and the data in the event of a failure. The back up media is not to be left with the server but removed and placed in a different location.

21. Where systems are deemed to be critical, a secondary or back up server is to be provided which will automatically take over the role of the primary in the event of its failure. This secondary server should ideally be in a different location to the primary

22. Where a secondary server is not available a risk assessment is to be carried out on the effect of the loss of the server and those results held within the NHS Lothian or Operating Division Risk Register.

23. The NHS Lothian Server team is to carry out a full restore of all critical servers annually.

24. Where a contract exists for the provision of server hardware in an emergency, this is to be rehearsed, if necessary in the contractor's premises and the operating system back up and the data restored within the agreed time limits. Each restore is to be logged and a report produced highlighting any issues raised and the remedial actions required.

25. A GP system server back up from each NHS Lothian GP system site is to be restored twice each year into the eHealth test environment and any faults reported and resolved.

26. Each contract for a managed service of hardware for major clinical systems is to include an annual failover of that system.

Guidance 1 NHS Lothian EHealth and IM&T Security Policy

NHS Lothian Staff Guide to eHealth Security Policies

1. Information takes many forms including but not limited to, data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversation, including over the telephone. Within NHS Lothian, staff have access to many forms of information much of it deemed to be sensitive.

2. 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.

3. The foremost policies and regulations which influence NHS Lothian's management of information are:
   NHS (Scotland) HDL (2006) 41, NHS Scotland Information Security Policy,
   Data Protection Act 1998,
   Computer Misuse Act,
   Civic Government (Scotland) Act 1982,
   Copyright Design and Patents Act 1988,
   Defamation Act 1996,
   Obscene Publications Act,
   Civil Contingencies Act 2004.
   Freedom of Information Act (Scotland) 2002.
   Confidentiality and Security Group Scotland (CSAGS)Report 2001,
   Caldicott Report 2000.
   CEL 25 2012 NHS Scotland Mobile Data Protection Standard
   Human Rights Act 1997
   CEL 25 2011 – Safeguarding Personal Data in Contracts – November 2011; Records Management NHS Code of Practice V 2.1 January 2012
   Public Records (Scotland) Act 2011
   Information Governance Policy
   Data Protection Policy
   Confidentiality of Personal Health Information Policy

4. The NHS Lothian eHealth and IM&T Security Policy which this guidance forms part is available for staff to read on the Intranet.

5. There is agreement within the regulations that both an organisation and its staff share responsibility for compliance. The organisation provides equipment, infrastructure and training for staff; who will act responsibly and in compliance with organisation policies and procedures.

NHS Lothian will provide:

- Computer devices and other equipment which will allow staff to work in an efficient and safe manner
- Computer devices will be available for staff to use during breaks, either within departments or in shared areas e.g. Libraries, training suites
- Access to “on line” and other training sites as agreed through CPD schemes.
- Screening of incoming email and access to internet for Anti Virus and inappropriate content including, “scams”,
- Staff with sufficient training to use the applications necessary to carry out their role in NHS Lothian. e.g. SCI Results, TRAK, Datix, EmPower, SCI Gateway. These applications will require the use of an additional user ID and Password.
- Staff with a network ID which will allow them access to the intranet, the internet, MS Office or similar and email.
- Access for all staff to the Internet and email for a limited amount of personal use. The authorised signatory agreeing the amount and when that is appropriate.
-
- A “H” or Home server drive in those areas where the “C” or local drive is inaccessible, for each user to store data and documents. This drive will only be accessible to the individual user. Data on this drive will be backed up as part of the routine IS processes. If information is permitted to be held by a user on a “C” drive the user is to ensure that data is to be backed up regularly. eHealth support staff will advise on best process and media to do this
- Access to shared departmental drives where necessary and authorised.
- Provide staff with guidance on password management

Staff will:

- Not connect to the network any device or software not provided by NHS Lothian including games, music (MP3), videos or personal photographs
- Never share passwords.
- Appropriately use NHS Lothian applications, noting all are routinely audited to identify potential misuse. Where an ID or password has been shared, the owner of that ID will have any errors caused attributed to them. Passwords should not be left where they can be used by others.
- Never download or store on any device, material which might cause offence to another

- Never attempt to view any information on patients whose care or management they are not directly involved.
- Never attempt to view the records or details of any other member of staff for whom they are not responsible.
- Never attempt to view the records or details of their own or family records. Access can be made via the legal services manager or Data Protection Officer for this purpose.
- Will not attempt to prevent any upgrade of software including anti virus occurring upon log on to network or at any other time.
- If involved directly in the provision of eHealth IT services they will familiarise themselves with both:
- NHS Lothian eHealth and IM&T Security Policy and
- NHS (Scotland) HDL (2006) 41, NHS Scotland Information Security Policy
- Not attempt to self help when the Anti Virus software produces a warning, report it to the Support desk. Normally when the AV reports a problem it is actually informing the user that it has found and already isolated the problem.
- Allow support desk staff to take control of their PCs remotely when requested. This process is only used to clear faults reported by users and with their permission.

eMail

- Do treat an email as an official document. Under Freedom of Information or other legislation, email might need to be released to meet certain requests.
- Don't use the email service for sending chain letters or advertising; use the Bulletin Board Service which can be accessed through the intranet.
- Do not send large attachments they will not go out through the NHS Gateway if they are above 15Mb. Although larger attachments can go between sites within Lothian it slows down the email system.
- Remember that emails regularly feature in tribunal cases where there are accusations of bullying or harassment. Do not send anything which might cause offence to another.
- Some email file types are blocked prior to network entry. When this occurs the intended recipient or sender will receive a warning message with instructions how to have it released if appropriate please follow those instructions.
- If you have any concerns about an email's origin do not open it
- Where there are reasonable grounds for suspicion that an individual may, through the use of email, have breached NHS Lothian policies including Confidentiality or Dignity at Work, then the Director of Human Resources may authorise monitoring of that individuals email or search through servers for archive files. This is in addition to the regular monitoring for potential inappropriate use.

Internet Access

6. A number of sites which are inappropriate or non health related are blocked permanently including eBay and You Tube. Sports and Property related sites are blocked between 09:00 and 17:00 Mondays to Friday. This blocking occasionally impinges on sites that are need for work or training related matters. If this occurs contact the eHealth Security Officers to have access to those sites cleared on an individual basis.

7. Some sites are blocked because they are known to attempt to place either tracking cookies or other spyware on the PC. Often these occur when using Google or another search engine to find a site and rather than producing the direct link it goes through another site and it is this secondary site's advertising that causes the problem. Check that this is not happening before reporting. It happens regularly with airline sites!

8. One of the greatest risks to the infrastructure is caused when staff, open at their desktop, their own ISP mail accounts e.g. MSMail, Blue Yonder as these initially bypass Lothian's AV screening. Members of staff shall not open attachments from their own ISP when are connected to NHS Lothian network.
9.

Password Management

10. NHS Lothian passwords must consist of a minimum of 6 characters, at least one of which should be non-alphabetic character. Ideally passwords should contain a mixture of the following
    a. English uppercase characters (A…Z)
    b. English lowercase characters (a…z)
    c. Base 10 digits (0…9)
    d. Non-alphanumeric (exclamation point [!], dollar sign [$], pound sign [#], percent sign [%], asterisk [*], etc.)

Password Suggestions

- Mnemonics - One way of creating a password meaningful to the user but not easily guessed by anyone else, is to choose a phrase and compose the password from the initial letters and numbers of the words.
- For example,
- ILIA2BH – I Live In A 2 Bedroomed House
- IGOH28J – I Go On Holiday 28th June
- MTNBW62 – My Telephone Number Begins With 62
- WSJR999P&C – Who Shot JR *number* Peaches and Cream (change the number – random increments)

- A viable alternative for selection is to open a book at random and select a phrase or word to form the basis of the password.
- Linking two words together with a non-alpha character. For example, CAT*FOOD or BELL%BOOK

Guidance to Research Staff on Data Management Best Practice

Introduction

All staff employed within NHS Lothian processing personal data whilst carrying out clinical research are required to comply with the Common Law on Confidentiality, The Data Protection Act (1998), the Caldicott Principles and any other legislation, current guidance or good practice protocols supported by NHS Lothian. It should be noted that this guidance applies to all data that can identify a 'living individual', including 'anonymised' data where individuals can be identified by cross-referring to a separately held database.

Personal (patient) data

1. All personal data must be processed in accordance with the NHS Lothian Data Protection and IT Security policies.

2. All data processed during the course of a researcher's duties remains under the 'ownership' of the Data Controller. In the vast majority of cases, this will be NHS Lothian, however there are limited circumstances where the Data controller will be University of Edinburgh or there may be Joint Data Controllers. Please refer to the appended 'Data Controller' flowchart for further guidance.

3. Databases containing personal data must be registered with the Data Protection Officer.

4. Regardless of who is identified as Data Controller, all personal data must be processed in accordance with this guidance and the eight principles of the Data Protection Act (1998).

5. To ensure 'fair and lawful' processing, research subjects must be provided with a 'fair processing notice' (FPN) and given the opportunity to raise any queries as part of the consent process. The FPN must include the name of the Data Controller(s), the purpose(s) for which the personal data is going to be processed and any other information required to ensure fair processing from the research subject's perspective. This may include how long the data will be held, whether the data is being shared with other researchers (and if so, to whom) and

whether the data is being transferred overseas for collaborative purposes.

6. In the instance of overseas transfer of data, the researcher must contact the NHS Lothian Data Protection Officer for further guidance, as the receiving country must meet certain levels of 'adequacy'. This is particularly important when transferring to non-EU countries.

7. Researchers should carefully consider the data that they hold. Identifiable data should be adequate, relevant and not excessive (DPA Principle 3). Particular care must be taken when analysing data to ensure that the underlying data cannot identify individuals. Best practice is to separate the identifiable data items from the other data, and link tables (look up table) only when absolutely necessary.

8. Where a look up table is used to identify research subjects from the remainder of the data set, it should be held securely and separately, and destroyed at the end of the project. The end of the project is defined as the length of time the data will be held in the Fair Processing Notice.

9. NHS Scotland is committed to using the CHI (Community Health Index) number on all clinical systems as a means to link across all local and national systems. This number can only be used as a patient identifier within the NHS and may only be shared with other agencies under strict protocols that must be agreed in advance of any information sharing.

10. The R&D department and/or NHS Lothian Data Protection Officer will provide best practice advice to researchers wishing to securely store paper or computerised data on completion of a research project.

11. In the event a researcher leaves their post, they must not take any personal data collected during their employment with NHS Lothian or University of Edinburgh to their new post.

IT Security

1. Research data must be held in a secure environment. Where practical, it should be stored on the research server provided by NHS Lothian R&D department. Alternatively, it should be stored on a secure network drive requiring password access and is regularly backed up.

2. Research data must never be exclusively stored on a laptop or PC hard drive. When it is not possible for data to be saved to a secure network environment, the following procedures must be taken:

a. The local hard disk must be suitably encrypted. Standard password protection of software packages, i.e., Microsoft Office, does not meet the required standard.

b. Research data must be backed-up on suitable media upon completion of the data processing.

3. Only NHS equipment, including PCs, laptops, tablets and memory sticks may be connected to the NHS network. Researchers should be aware that the NHS networks can readily identify non-NHS hardware and will take any breaches very seriously.

4. Emailing of personal information via the Internet is not permitted. This includes email sent from an NHS email account to a University email account. If a researcher wishes to send information electronically, they should seek further guidance from the NHS Lothian IT Security team for advice on suitable encryption methods and secure methods of transferring data.

Safe Email Transmission

Standard Operating Procedure (SOP) is published separately so that it can be regularly updated to reflect new security guidance.

Unique ID: NHSL.
Category/Level/Type:
Status: Final
Date of Authorisation: 01/02/17
Date added to Intranet: 01/02/17
Key Words: eHealth Security Policy
Comments:

Author (s): T McKinley
Version: 2.5.09 January 2017
Authorised by: Director of eHealth
Review Date: January 2019