Guidance 1 of 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 Legislation,
   - 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,
   - CEL 25 2012 NHS Scotland Mobile Data Protection Standard
   - Human Rights Act 1997
   - 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 individual’s 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. 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. What was no. 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 Bedderoomed 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