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 Legislation 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.