

## PREVENTING UNAUTHORISED DISCLOSURE

Despite all of your efforts to prevent your device being lost or stolen it remains a fact that unforeseen incidents can and will occur from time to time. It is important, therefore, that measures are taken to ensure that information cannot be viewed or extracted from, the device. To this end there are a number of measures which should be considered and implemented where required including:-

- Basic device or operating system passwords provide only basic security to the device—the data thereon may be accessible simply by removing the device drive and attaching it to another compatible device. To secure against this other security measures including data encryption may be necessary; advice should be available from the local information security manager. NHS requirements for data encryption apply equally to removable media; devices such as USB memory sticks etc.
- PDA's and mobile email devices will benefit through a remote wiping facility so that the device can be cleared and rendered useless if lost or stolen. Device users should know what to do in these circumstances.
- Patient data sent to or from your device must be encrypted on its "journey";
- Remember, passwords are only good as they are strong and secret. Don't share your password or access token with anyone else and make sure that your passwords are not easy to guess.

### Further Information

NHS Connecting for Health  
For additional information on mobile computing in the NHS:

## Remember

### DO

- Read and understand your organisation's information security policy and procedures;
- Make sure that your devices are physically secure when unattended;
- Keep the information you have on your device to a minimum and make sure that it is backed up in accordance with your organization's policy
- Encrypt devices and removable media that contain patient or sensitive information
- Ensure patient data that is sent to /from your device is encrypted.
- Immediately report any actual or suspected loss, theft or unauthorised access/disclosure.

### DON'T

- Leave your mobile devices unattended
- Leave them in your car, even for a short period
- Hold more information than is necessary
- Carry your device and any access tokens in the same bags
- Share passwords or access tokens

Published: February 2008

## Good Practice In .....



(Picture for illustration purposes)

## Mobile Computing

*The secure use of laptops, PDA's and other mobile devices*

# MOBILE COMPUTING

## MOBILE COMPUTING AND THE RISKS?

Within the context of the NHS, mobile computing is a term used to describe the use of mobile devices that process NHS data. Typically this will include items such as laptops, PDA's and mobile email devices and even mobile telephones where these are capable for storing data.

Mobile computing can bring about many benefits to the NHS. It allows for information to be available whilst working on the move, in remote or home working situations. It can improve the patient care experience and can contribute to the improvement of working lives.

These benefits, however, also present a new set of risks. Information is no longer retained within the hospital, Practice or office; it is moving around the city, the country and potentially even abroad on a variety of devices and through other communications channels. One only has to read the newspapers or watch the news to hear stories of information on devices such as laptops that get lost or stolen. Given the confidential nature of the information that the NHS holds, and the adverse impacts that may be caused if it is lost or stolen it is imperative that we not only implement, but are seen to implement, robust information security arrangements where mobile devices are to be used.

## MANAGING THE RISKS

It would be counterproductive to ban or reduce the use of mobile devices simply because there is a risk; to do so would prevent the benefits of using these devices being realised. Instead, it is essential that the use and control of these devices is assessed and managed on

the basis of risk. It is essential, therefore, that the organisation has a clear understanding of the mobile devices that it owns or permits in use, who they are used by, for what purposes and in what manner and, most importantly, what information is processed on them.

It should be acknowledged that the greatest risk is almost certainly the unauthorised disclosure of information rather than the physical loss of the equipment itself.

Risk assessments will give the organisation an indication of whether use is appropriate and beneficial and, therefore, what controls need to be deployed to facilitate and secure that use.

Regardless of the results of these risk assessments there are some basic controls that should be in place as a matter of course to secure mobile devices and, therefore, the data on them or that is sent to and from them.

## HAVE A MOBILE DEVICE SECURITY POLICY

The first stage in controlling any element of security is the organisation's information security policy. Each NHS organisation should have in place such a policy which sets out its security position and how, through supporting policies or procedures, this will be achieved.

The policy should set out key issues such as:-

- What is considered to be acceptable use
- How mobile devices are to be used and secured
- How mobile devices can connect to the internet or other networks for the transfer of information
- What information can and can't be used or sent etc
- What to do in the event of a loss of theft

Simply having policies and procedures, however, is not sufficient. All staff must receive appropriate training and awareness to ensure that the policies are applied.

## MINIMISE THE RISK OF LOSS

The fact that mobile devices are so mobile, and in the cases of PDA's etc so small, means that they are not only easier to misplace but are tempting to those intent on theft. In order to reduce the risk of loss or theft you and your organisation should, as a minimum:-

- Make sure that laptops are physically secured to desks wherever possible etc using appropriate locking mechanisms, especially when left unattended;
- Make sure that these devices are kept with you or locked away when not in use;
- Don't leave your device visible in an unattended vehicle, even for a short time, and make sure it is out of sight while in transit;;
- Consider using carry cases/bags which are not obvious laptop bags e.g. without manufacturer logos.;
- Don't store or carry any tokens used for accessing your device or systems in the same bag as your device; if you lose one, you will lose both;
- If you are storing equipment at home remember you should, as a minimum, apply the same level of security that you would normally have in your place of work;
- Minimise the amount of data that you hold on your device. Ensure this is limited to what you require to do your job. Not only is information on mobile devices at risk of unauthorised disclosure, there is a risk of complete loss and business disruption if the device is not backed up.

It is important to remember that these measures are not just for the protection of the equipment and the information thereon, they are also to protect you. Don't make yourself a target.