Preventing unauthorised disclosure

Despite all 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.

USB Encryption Advice

The following advice is given to the use of USB devices.

If the information is:

- Public domain information – the data maybe secured on the unsecure area of the USB.
- Information that is commercially or clinically sensitive and requires a degree of protection, however individuals are not identifiable - the password secure area of the USB must be used.
- Personally identifiable information or information that is otherwise commercially or medically sensitive - Need to know principle is applicable - the password secure area of the USB must be used and the document itself should be password protected.
- Information that is more sensitive than patient identifiable information. Need to know principle is applicable - the password secure area of the USB must be used and the document itself should be password protected.

Remember, passwords are only as 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.

Remember:

Do

- read and understand this guide if your require assistance ask your line manger
- 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
- follow the USB encryption advice
- immediately report any actual or suspected loss, theft or unauthorised access/disclosure to BrisDoc's Head of Business Information and Projects or SIRO/Managing Director.

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 bag
- share passwords or access tokens.

Good practice guide

BrisDoc

Patient care by people who care

Mobile Computing

(Ref Vn 1.2)

The secure use of laptops, USBs and other mobile devices

Based on the NHS *Connecting for Health*

Mobile Computing Guide July 2008 Ref: 4165

Mobile computing and the risks

Within 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, USBs and mobile email devices and even mobile telephones where these are capable of storing data.

Mobile computing can bring about many benefits, 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 communication 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 implement, robust information security arrangements where mobile devices are 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 BrisDoc 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 BrisDoc 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.

BrisDocs' Mobile Computing Policy

The policy sets out the key issues::

- what is considered to be acceptable use
- how mobile devices are to be used and secured
- what information can and can't be used or sent etc
- what to do in the event of a loss or theft.

All staff will receive appropriate training and awareness to ensure that the policy is applied.

Minimise the risk of loss

The fact that mobile devices are so mobile and, in the case of PDAs 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 and BrisDoc will, as a minimum:

- make sure that laptops are physically secured to desks wherever possible.
- make sure that these devices are kept with you or locked away when not in use
- not leave your device visible in an unattended vehicle, even for a short time, and make sure it is out of site while in transit
- consider using carry cases/bags which are not obvious laptop bags
- not 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
- apply the same level of security that you would normally have in your place of work (if you are storing equipment at home)
- 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.