

Mobile units and data security

The collective term “mobile units” includes mobile phones, PDAs, ultramobile PCs, laptops, and similar equipment. All of them are easy to transport and to use wherever health staff and other people work.



When correctly used, mobile units (picture) can be of great benefit in the public health service. They can provide access to up-to-date information from various sources about the patient wherever the patient is, and in locations in which such information has traditionally not been readily available. At the same time, such use can increase the risk of information going astray.

Benefits

In the public health service, mobile units can provide many benefits. For example:

- Direct lookups in the patient record at the bedside or during rounds
- Access to patient information during a journey
- In home nursing care – access to work lists and patient record information from home, on the way and at the user’s location

Threats to data security

All new solutions present new challenges with regard to data security. Traditional threats such as viruses, hacking and Trojan horses pose the same risks for mobile units as they do for desktops. Mobile units not only mean more types of technology to relate to. They also involve changes in the use of various specialized systems. The changes in the use of these systems cause the greatest changes in the risk profile.

For example, mobile units make it possible to take the electronic patient record out to patients: at a hospital bedside, at home, or at the scene of an accident. Sensitive patient information can be displayed on a screen “in the field” instead of in an office. In certain situations, it may be easy to forget that other people can see pictures and text on the screen.

When a mobile unit disappears, it can be difficult to know whether it has been stolen or “only” mislaid. The consequence is the same – control over the information on the unit is lost. Mobile units are usually stolen because they are easy to resell. Unfortunately, they may also be stolen with the aim of obtaining specific information.

There are other ways of stealing information than by taking the unit itself. Mobile units are designed to be as accessible as possible via various wireless networks, such as mobile telephone networks and Bluetooth. All of these enable an “attacker” or unauthorized person to hack into the unit without stealing it. One important distinction is between active and passive attacks. Passive attacks involve eavesdropping on traffic between the mobile unit and the resources with which it communicates. In active attacks, the attacker tries in various ways either to influence the unit directly or to influence the communication between it and others.

Measures

It is possible for health staff to protect themselves against all the threats mentioned above. Shoulder surfing can be avoided by being aware of what is happening around you when you work with sensitive information. Effective protection against the other threats requires specific technical solutions.

There is often a greater need for protection of mobile units than of desktops, since the former are not in a controlled environment. As a minimum, mobile units should be protected with:

- Antivirus software
- Personal firewall
- Automatic or regular updating of software

Much of this should and must be handled by operating staff.

For security reasons, health information should not be stored on mobile units. If such information is to be stored, however, it must be protected using encryption. It is important to use encryption programs of high quality to ensure that one is not just lulled into a false sense of security.

In this connection, the following must be in place:

- Support for strong authentication of the user
- Backup of the decryption key
- Possibility for locking the unit via the Internet

Much of this must also be handled by operating staff.

>>



It is possible to protect against attacks over wireless networks in various ways. The simplest way is to switch off the wireless functions that are not in use. Information transferred over wireless networks must be protected from access and unauthorized changes. If this is not built in, protection can be provided by creating encrypted VPN connections. The most important measures are:

- Switch off wireless functions which are not being used
- Use the security functions that are built in
- Use encrypted VPN to protect information in the wireless network



*“Shoulder surfing” is a security risk.
Photo: Jan Fredrik Frantzen, NST.*

What can users themselves do to secure data?

Not all threats can be prevented with the help of technical solutions. The individual's attitude to using and taking care of mobile units is just as important.

There may appear to be a distinction between units that health staff own themselves and units owned by the health care organizations. It is easy to understand that equipment owned by the organization must be treated in the way that the organization decides. In contrast, it is not always as easy to remember that private mobile units which are used to work with sensitive information must be treated in the same way in order to safeguard patients' privacy.

Many security measures may seem annoying. For the overall security, however, it is important that everyone loyally complies with the security regulations and procedures that have been established, even though they may seem tedious in day-to-day work. Lack of compliance may lead to various threats to the protection of personal data, which will not be in the patient's interests.

As a user of mobile units, you can contribute to good data security:

- Follow the guidelines laid down by your organization for the use of equipment, and only using the equipment as intended by your employer
- Do not use personal equipment for work, or vice versa, unless this has been agreed with your employer
- Switch off equipment when it is not in use
- Ensure that no one can “shoulder surf” to read information on your screen
- Keep the equipment in a safe place
- Use passwords and PIN codes when required and keep them secret from outsiders
- Make sure that the equipment you use is checked and upgraded regularly

Abbreviations

PDA – Personal Digital Assistant
PIN – Personal Identification Number
VPN – Virtual Private Network

This fact sheet has been prepared in collaboration with the Norwegian Centre for Information Security (NorSIS, www.norsis.no)

Contact:

Data security questions:
Eva Henriksen
eva.henriksen@telemed.no
Tel: +47 957 31 836

Legal questions:
Ellen K. Christiansen
ellen.christiansen@telemed.no
Tel: +47 416 84 705

Eva Skipenes
eva.skipenes@telemed.no
Tel: +47 911 77 515

Leif Erik Nohr
leif.erik.nohr@telemed.no
Tel: +47 901 43 166

See www.telemed.no/factsheets to see other fact sheets published in this series.
This fact sheet was revised July 2008.

