Kort sagt om...

NST | Nasjonalt senter for telemedisin
UNIVERSITETSSYKEHUSET NORD-NORGE
WHO Collaborating Centre for Telemedicine

Mobile enheter og datasikkerhet

Mobile enheter er et samlebegrep for mobiltelefoner, PDA, ultramobil PC, bærbar PC og tilsvarende utstyr. Felles for alle er at de enkelt kan transporteres og benyttes der helsepersonell og andre jobber.

Ved riktig bruk vil mobile enheter (bildet) kunne være til stor nytte i helsevesenet. De kan gi tilgang til oppdatert informasjon fra ulike kilder om pasienten der pasienten er, og til steder der slik informasjon tradisjonelt har vært vanskelig tilgjengelig. Samtidig kan slik bruk medføre økt risiko for at opplysninger kommer på avveier.

Fordeler

I helsevesenet kan mobile enheter gi mange fordeler. For eksempel:

- Direkte oppslag i journalen ved sykeseng/visitt
- Tilgang til pasientopplysninger på reise
- I hjemmesykepleien – tilgang til arbeidsliste og journalopplysninger hjemmefra, underveis og hos bruker

Trusler mot datasikkerheten

Alle nye løsninger gir nye utfordringer mht. å ivareta datasikkerheten. Tradisjonelle trusler som virus, hacking, trojanere og lignende er like farlige for mobile enheter som for vanlige stasjonære maskiner. Mobile enheter gir ikke bare flere typer teknologi å forholde seg til. De medfører også endringer i bruken av ulike fagsystemer. Det siste forårsaker størst endring i risikobildet.

Mobile enheter gjør det mulig å ta for eksempel elektronisk journal med seg helt ut til pasientene; ved sykehussenger, i hjemmene eller til et ulykkessted. Sensitiv pasientinformasjon kan vises på skjermen "ute i felten" i stedet for inne på et kontor. Det kan i enkelte situasjoner være lett å glemme at andre enkelt kan se bilder og tekst på skjermen.

Når en mobil enhet forsvinner, kan det være vanskelig å vite om den er stjålet eller "bare" mistet. Konsekvensen er den samme – kontrollen over informasjonen på enheten er tapt. Vanligvis blir mobile enheter stjålet fordi de er lette å selge videre. Dessverre hender det også at tyverier blir foretatt med tanke på å skaffe spesifikk informasjon til veie.

Informasjon kan også stjeles på andre måter enn å ta selve enheten. Mobile enheter er laget for å være mest mulig tilgjengelige via ulike trådløse nettverk, som for eksempel mobiltelefonnett og blåtann. Alle disse gir en "angriper" eller en utenforstående mulighet til å trenge inn i enheten uten å stjele den. Ett viktig skille går mellom aktive og passive angrep. Passive angrep består i å avlytte trafikken mellom den mobile enheten og de ressurser den kommuniserer med. Aktive angrep er når angriperen på ulike måter prøver enten å påvirke enheten direkte eller påvirke kommunikasjonen mellom den og andre.

Tiltak

Det er mulig for helsepersonell å beskytte seg mot alle de nevnte truslene. Smugtitting kan unngås ved å være bevisst på omgivelsene når sensitive opplysninger behandles. God beskyttelse mot de andre truslene krever egne tekniske løsninger.

Ofte er det et større behov for beskyttelse av mobile enheter enn stasjonære maskiner, siden førstnevnte ikke står i et kontrollert miljø. Mobile enheter bør som et minimum beskyttes med:

- Antivirusprogrammer
- Personlig brannmur
- Automatisk eller jevnlig oppdatering av programvare

Mye av dette bør og må ivaretas av driftspersonell.

Helseopplysninger bør av sikkerhetsmessige årsaker ikke lagres på mobile enheter. Hvis slik informasjon likevel skal lagres må den beskyttes ved hjelp av kryptering. Det er viktig å benytte krypterings-programmer av høy kvalitet for å sikre at en ikke bare oppnår en falsk trygghet.

Følgende må være på plass i denne forbindelse:

- Støtte for sterk autentisering av bruker
- Backup av dekrypteringsnøkkel
- Mulighet for låsing av enhet over nett

Mye av dette må også ivaretas av driftspersonell.

>>

Man kan beskytte seg mot angrep over trådløse nett på ulike måter. Den enkleste er å slå av de trådløse funksjonene som ikke er i bruk. Informasjon som sendes over trådløse nett, må beskyttes mot innsyn og uautoriserte endringer. Dersom dette ikke er innebygd, kan beskyttelse oppnås ved å opprette krypterte VPN-forbindelser.

De viktigste tiltakene er:

- Slå av trådløse funksjoner som ikke brukes
- Ta i bruk sikkerhetsfunksjoner som er innebygd
- Bruk kryptert VPN for å beskytte informasjon som formidles via det trådløse nettet

Smugtitting har fått et eget navn på engelsk: "Shoulder surfing". Foto: Jan Fredrik Frantzen, NST.

Hva kan brukerne selv gjøre for å sikre data?

Alle trusler kan ikke avverges ved hjelp av tekniske løsninger. Den enkeltes holdning til hvordan mobile enheter skal brukes og tas vare på er vel så viktig.

Det kan se ut til å være et skille mellom håndteringen av enheter som helsepersonell eier selv og enheter som eies av helsevirksomhetene. Det er lett å forstå at utstyr eid av virksomheten skal behandles slik virksomheten bestemmer. Derimot er det ikke alltid like lett å huske på at private mobile enheter som brukes til å behandle sensitive opplysninger, må behandles på samme måte for å ivareta pasienters personvern.

Mange sikkerhetstiltak kan virke plagsomme. Det er imidlertid viktig for totalsikkerheten at alle lojalt følger de sikkerhetsbestemmelser og -prosedyrer det er lagt opp til, selv om det kan virke tungvint i det daglige arbeid. Manglende oppfølging vil kunne medføre ulike trusler mot personvernet, noe som ikke vil være i pasientens interesse.

Som bruker av mobile enheter kan du bidra til god datasikkerhet ved å:

- Følge de retningslinjene virksomheten gir for bruk av utstyret og bare benytte utstyret slik det er tenkt fra arbeidsgivers side
- Ikke benytte privat utstyr i jobbsammenheng, eller omvendt, med mindre det er avtalt med arbeidsgiver
- Slå av utstyret når det ikke er i bruk
- Sørge for at ingen kan sniklese via din skjerm
- Oppbevare utstyret trygt
- Bruke passord og PIN-koder når det er påkrevd og sørge for at uvedkommende ikke får kjennskap til dem
- Passe på at utstyret du bruker blir jevnlig sjekket og oppgradert

Forkortelser

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

Dette faktaarket er utarbeidet i samarbeid med Norsk Senter for Informasjonssikring (NorSIS, www.norsis.no).

Se også:
Følgende faktaark utformet i tilknytning til norm for informasjonssikkerhet i helsesektoren:

- Faktaark 18 - Bruk av bærbart utstyr
- Faktaark 26 - Trådløs teknologi
- Faktaark 30 - Mobilt utstyr

Link: http://www.shdir.no/samspill/informasjonssikkerhet/norm_for_informasjonssikkerhet_i_helsesektoren_53069

Kontaktpersoner ved NST:

Datasikkerhet:
Eva Henriksen
eva.henriksen@telemed.no
Tlf: +47 957 31 836

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

Juridiske spørsmål:
Ellen K. Christiansen
ellen.christiansen@telemed.no
Tlf: +47 416 84 705

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

Se www.telemed.no/faktaark for andre faktaark i serien.
Dette faktaarket foreligger også i engelsk versjon:
www.telemed.no/factsheets
Faktaarket ble sist revidert i juli 2008.