Ti gode grundregler for IT sikkerhed på klinikken

1. Brug professionelt programmel imod ondsindede programmer og vær sikker på, at det løbende opdateres.

2. Hold dine programmer, styresystemer og apps opdaterede.

3. Undgå skadelige downloads, når du besøger hjemmesider. Undlad brug af din PC til andet end arbejdsrelaterede opgaver. Tjek sikkerhedsniveauet i din browser.

4. Såfremt der findes trådløse netværk (WiFi) på klinikken, bør dette adskilles fra klinikkens arbejdsnetværk, så der ikke er forbindelse mellem de to netværk. Risikoen for en evt. "bagdør"/trojansk hest fra mobiltelefoner og andet it-udstyr er særdeles stor. Et WiFi netværk skal altid sikres med minimum WPA2 kryptering, og koden bør udskiftes med jævne mellemrum.

5. Åbn ikke links eller filer i e-mail, du får sendt uopfordret.

6. Brug adgangskoder med minimum 8 karakterer indeholdende tal, tegn og bogstaver.

7. Tag daglig sikkerhedskopier af dine data og kontroller, at sikkerhedskopien kan læses ind.

8. Undlad at indtaste personlige data på hjemmesider, du ikke kender.

9. Tilkobl aldrig USB-nøgler, cd’ere og transportable harddiske, du ikke kender.

10. Pas på dit nøglekort og din kode til NemID. De må kun anvendes af dig personligt, og kode samt nøglekort må aldrig opbevares sammen.

Samme grundregler bør anvendes fra en hvilken som helst PC/mobil/tablet, der måtte have adgang til klinikkens IT systemer - fx hvis klinikken giver tilladelse til at IT systemerne kan tilgås fra lokationer som er udenfor klinikkens kontrol, såsom hjemmepc’ere.