Norm for informasjonssikkerhet - www.normen.no

Utgitt med støtte av: Direktoratet for e-helse

De viktigste sikkerhetskravene databehandlingsansvarlig må ivareta

Oppsummering 3
Versjon: 1.1
Dato: 08.09.2017

Journalsystemet er hos databehandler og tilgjengelig via helsenett eller Internett
Grønt skal databehandlingsansvarlig gjøre selv. Blått skal databehandler gjøre

1	Ikke send helseopplysinger eller 11-siffret fødselsnummer på SMS eller e-post (3.5)
2	PC, lagringsenhet og kommunikasjonsutstyr (ruter) skal sikres slik at de kun er tilgjengelig for deg og dine kolleger eller andre med rettigheter (3.1)
3	Tilgang til helse- og personopplysninger skal kun gis brukere som har en rolle i journalsystemet. Rollen gir rettigheter til å registrere, lese, skrive ut, endre og slette journal. Slutter en bruker, skal rettighetene brukeren hadde i rollen arkiveres i minimum 2 år fra det tidspunkt rettigheten ble tatt ut av bruk (2.1.1)
4	Sørg for at datamaskinene har installert en løsning for å hindre ondsinnet programvare (antivirusløsning) (3.2)
5	Opprett databehandleravtale med leverandør som drifter journalsystemet. Avtalen skal sikre taushetsplikt og at leverandøren sikrer dataene dine tilstrekkelig (2.2.3)
6	Gjør en sikkerhetsrevisjon minimum en gang i året så vet du at klinikken følger de etablerte rutinene (2.3.1)
7	Du må etablere to uavhengige tekniske sikkerhetstiltak mellom journalsystemet og helsenett eller Internett. Benytter du helsenett er tilkoblingen tilstrekkelig sikret med utstyret som leveres av Norsk Helsenett (3.2)
8	All tilgang til helse- og personopplysninger skal logges i journalsystemet. Det samme skal forsøk på uautorisert tilgang. Logger skal oppbevares i minimum 2 år (3.5)
9	Ta daglig sikkerhetskopi av alle helse- og personopplysninger slik at du kan gjenskape journalene om uhellet skulle være ute. Sjekk jevnlig at innholdet på kopiene kan gjenskapes. Sikkerhetskopiene skal oppbevares avlåst og brannsikret, og adskilt fra driftsutstyret. Ekstern oppbevaring av sikkerhetskopiene anbefales (3.2)
10	Ved kassering eller salg av utstyr (for eksempel kopimaskin, telefaks, multifunksjonsskriver, PC og server) må du påse at helse- og personopplysninger slettes på lagringsenheten/disken slik at opplysningene ikke kommer på avveie (3.2)

Detaljer om det enkelte kravet finner du i dokumentet Personvern og informasjonssikkerhet for psykologer, fysioterapeuter, manuellterapeuter og kiropraktorer. Kapittelnummer er angitt ovenfor.