

					Utgitt med støtte av: Direktoratet for e-helse
Norm for informasjonssikkerhet - www.normen.no					Oppsummering 1 Versjon: 1.1 Dato: 08.09.2017
<p style="text-align: center;"><b>Journalssystemet er på eget utstyr uten tilknytning til helsenett eller Internett</b></p>					

<p style="text-align: center; font-size: 2em;"><b>1</b></p>	Ikke send helseopplysninger eller 11-sifret fødselsnummer på SMS eller e-post (3.5)
<p style="text-align: center; font-size: 2em;"><b>2</b></p>	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 sikkerhetskopien anbefales (3.2)
<p style="text-align: center; font-size: 2em;"><b>3</b></p>	Gjør deg kjent med rettighetene pasienten har ift innsyn, samtykke, endring og sletting av helse- og personopplysninger (2.2.5, 2.2.6 og 2.2.8)
<p style="text-align: center; font-size: 2em;"><b>4</b></p>	Alle avvik fra etablerte rutiner skal dokumenteres og følges opp (2.3.4)
<p style="text-align: center; font-size: 2em;"><b>5</b></p>	PC og lagringsenhet skal sikres slik at de kun er tilgjengelig for deg og dine kolleger eller andre med rettigheter (3.1)
<p style="text-align: center; font-size: 2em;"><b>6</b></p>	All tilgang til helse- og personopplysninger skal logges i journalssystemet. Det samme skal forsøk på uautorisert tilgang. Loggene skal oppbevares i minimum 2 år (3.5)
<p style="text-align: center; font-size: 2em;"><b>7</b></p>	Tilgang til helse- og personopplysninger skal kun gis brukere som har en rolle i journalssystemet. Rollen gir rettigheter til å registrere, lese, skrive ut, endre og slette journal. Slutten 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)
<p style="text-align: center; font-size: 2em;"><b>8</b></p>	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)
<p style="text-align: center; font-size: 2em;"><b>9</b></p>	Gjør en risikovurdering av behandlingen av helse- og personopplysninger. På den måten kontrollerer du at dataene er tilstrekkelig sikret. Gjør en ny risikovurdering om du endrer den tekniske løsningen eller anskaffer nytt journalssystem (2.3.3)
<p style="text-align: center; font-size: 2em;"><b>10</b></p>	Gjør en sikkerhetsrevisjon minimum en gang i året så vet du at klinikken følger de etablerte rutine (2.3.1)

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