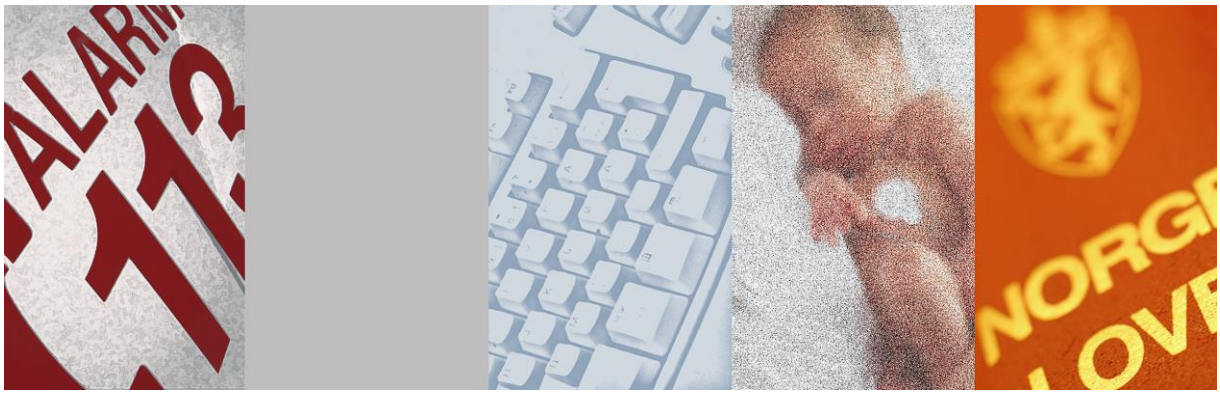
Personvern og informasjonssikkerhet for psykologer, fysioterapeuter, manuellterapeuter og kiropraktorer

- en veileder med maler

Veilederen er et støttedokument til Norm for informasjonssikkerhet



Utgitt med støtte av:

Helsedirektoratet

Versjon 2.0

www.normen.no

Merknad 24.03.2019: Dokumentet er ikke oppdatert fra siste versjon av Normen (5.3), ny personopplysningslov, endringer i helselovgivningen, eller EUs personvernforordning

INNHOLD

1 INNLEDNING 5

1.1 MÅLGRUPPE OG PRAKTISK BRUK AV VEILEDEREN 5
1.2 ANSVAR 7
1.3 BAKGRUNN 8
1.4 OM NORMEN 9

2 OPPGAVER DATABEHANDLINGSANSVARLIG SKAL IVARETA 9

2.1 KRAV TIL INFORMASJONSSIKKERHET 9
2.1.1 Sikkerhetsmål 9
2.1.2 Sikkerhetsstrategi 10
2.1.3 Nivå for akseptabel risiko 10
2.1.4 Oversikt over behandlinger av helse- og personopplysninger 11
2.2 OPPGAVER VED BEHANDLING AV HELSE- OG PERSONOPPLYSNINGER 12
2.2.1 Tilgangsstyring 12
2.2.2 Sikring av teknisk løsning 14
2.2.3 Inngåelse og oppfølging av leverandøravtaler 15
2.2.4 Opplæring og kompetanseheving 15
2.2.5 Pasientinformasjon og informert samtykke 16
2.2.6 Overholdelse av innsynsrett 16
2.2.7 Utlevering av journal eller opplysninger i journal 17
2.2.8 Retting og sletting av pasientopplysninger, herunder oppbevaring av pasientjournal 17
2.2.9 Overføring av helse- og personopplysninger til utlandet 17
2.3 OPPFØLGING AV INFORMASJONSSIKKERHETEN 18
2.3.1 Sikkerhetsrevisjon 18
2.3.2 Fornyelse av melding til Datatilsynet 18
2.3.3 Risikovurdering 18
2.3.4 Avvikshåndtering 19
2.3.5 Ledelsens gjennomgang 20

3 OPPGAVER SOM HELT ELLER DELVIS KAN IVARETAS AV DATABEHANDLER 22

3.1 FYSISK SIKRING AV OMRÅDER OG UTSTYR 22
3.2 SIKKERHET I NETTVERK, DATAUTSTYR OG TEKNISKE LØSNING 23
3.3 HENDELSESREGISTRERING 25
3.4 HJEMMEKONTOR OG MOBILT UTSTYR 25
3.5 ELEKTRONISK KOMMUNIKASJON SOM E-POST OG SMS 26

4 VEDLEGG 27

4.1 OVERSIKT OVER SENTRALE LOVER 27
4.1.1 Personopplysningsloven 27
4.1.2 Pasientjournalloven 27
4.1.3 Helsepersonelloven 28
4.1.4 Pasient- og brukerrettighetsloven 29
4.1.5 Barnevernloven 29
4.1.6 Psykisk helsevernloven(jf. psykologspesialist med vedtakskompetanse) 29
4.2 DEFINISJONER 30
4.3 SAMTYKKEERKLÆRING 36
4.4 INFORMASJONSPLAKAT 37
4.5 GJENNOMFØRING AV RISIKOVURDERING 38

4.5.1 Mal for risikovurdering 38
4.6 MAL FOR STYRINGSSYSTEM 43
4.6.1 Oppgaver databehandlingsansvarlig skal ivareta 43
4.6.2 Databehandlingsansvarliges oppfølging av oppgaver som helt eller delvis kan ivaretas av databehandler 44
4.6.3 Oppfølging av informasjonssikkerheten 46
4.6.4 Databehandlingsansvarliges sjekkliste for ivaretakelse av Normen 47
4.7 REFERANSER 52
5 DELTAGERE I UTARBEIDELSE AV VEILEDEREN 52

Endringshistorikk for og godkjenning av dokumentet

Versjon	Endringer	Godkjent av styringsgruppen for Normen (dato)
1.0	Første utgave av veilederen	5. juni 2014
1.9	Oppdatert ihht Normen 5.0 og ny helseregisterlov og pasientjournallov	Sekretariatet april 2015
2.0	Godkjent av styringsgruppen	4. juni 2015

1 INNLEDNING

1.1 Målgruppe og praktisk bruk av veilederen

Hensikten med denne veilederen er å forenkle arbeidet til psykologer, fysioterapeuter, manuellterapeuter og kiropraktorer, som driver som næringsdrivende, i å ivareta lovpålagte krav til personvern og informasjonssikkerhet.

Lovverket pålegger alle *virksomheter* som behandler *helse- og personopplysninger* (i bl.a. *elektronisk pasientjournal (EPJ))* en rekke sikkerhetstiltak. Kravene til personvern og informasjonssikkerhet er samlet i *Normen*, og denne veilederen er en praktisk veiviser for å oppfylle disse kravene. Veilederen er tilpasset små og mellomstore *virksomheter* og enkeltpersonforetak. Ord i veilederen som er markert i kursiv er definerte ord og er samlet i kapittel 4.2.

Veilederen er primært skrevet for *databehandlingsansvarlig* eller roller som støtter *databehandlingsansvarlig* i *virksomheter* innen de fire profesjonene. *Databehandleransvarlig* er den som er ansvarlig for personvern og informasjonssikkerhet i forbindelse med pasientbehandling. Alle *virksomheter* som benytter elektronisk registrering av *helse- og personopplysninger* og som bruker IT-systemer for dokumentasjon har en *databehandlingsansvarlig.* Normalt er denne rollen representert ved *virksomhetens* daglige leder, administrerende direktør eller eier av enkeltpersonforetak.

Databehandlingsansvarlig kan benytte en *databehandler* til å levere *EPJ* via *helsenett* eller Internett og for å utføre oppgaver som omhandler personvern og informasjonssikkerhet. *Databehandler* kan bl.a. bidra med viktig teknisk kompetanse for å sikre personvern og informasjonssikkerhet.

Veilederen er ikke utfyllende med hvilket ansvar og oppgaver *databehandler* påtar seg ved å *behandlehelse- og personopplysninger* på vegne av *databehandlingsansvarlig.* For en komplett beskrivelse av *databehandlers* oppgaver og ansvar henvises det til *Normen*.

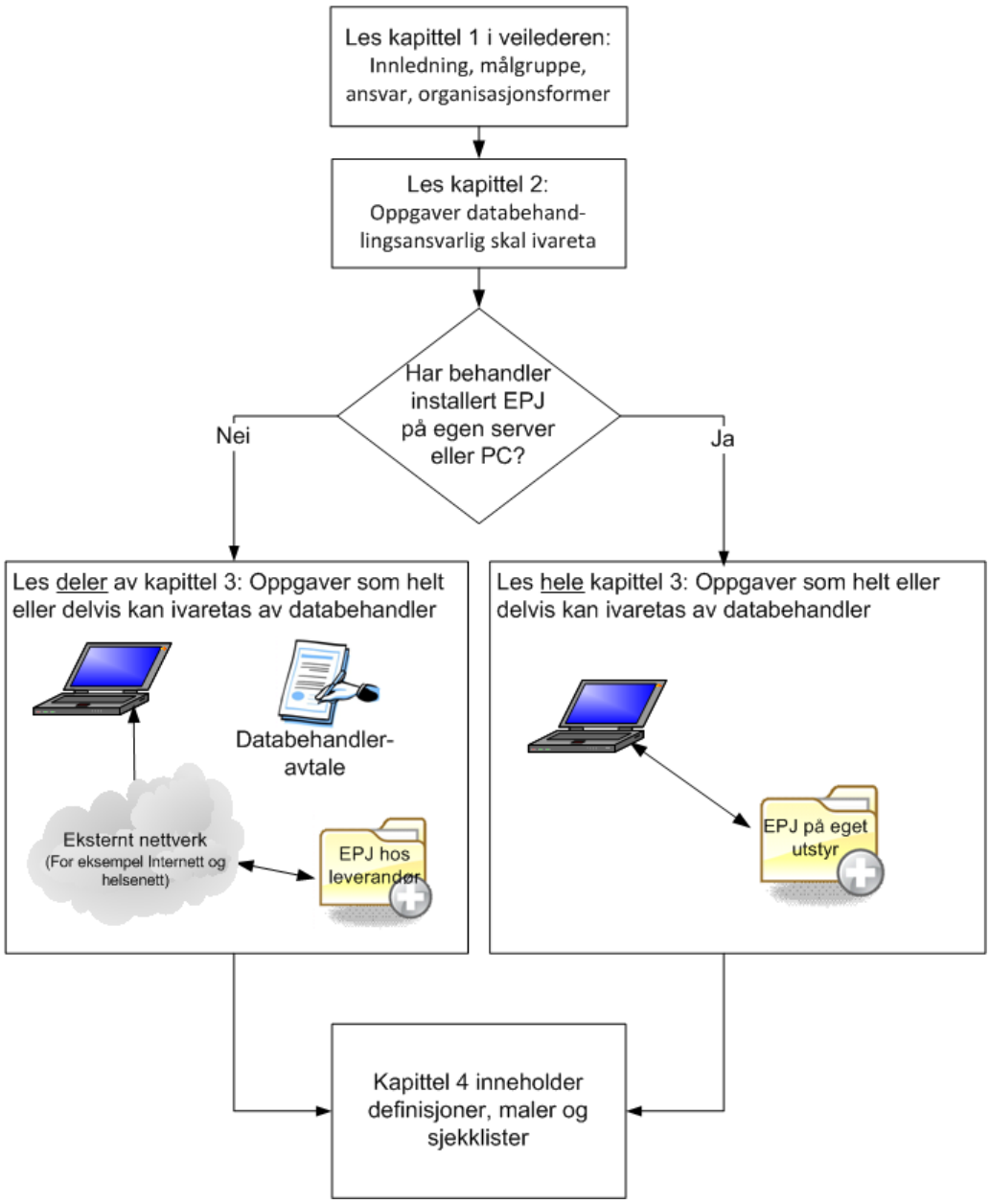
Veilederen omfatter ikke rollen psykologer har som sakkyndige.

Veilederen er bygget opp med følgende kapitler:

- Kapittel 1 inneholder beskrivelse av målgruppe, ansvar og bakgrunnsinformasjon
- Kapittel 2 beskriver oppgaver som skal ivaretas av *databehandlingsansvarlig*
- Kapittel 3 beskriver oppgaver som helt eller delvis kan ivaretas av *databehandler*
- Kapittel 4 inneholder lovgrunnlag, definisjoner, mal for styringssystem og sjekkliste for ivaretakelse av personvern og informasjonssikkerhet

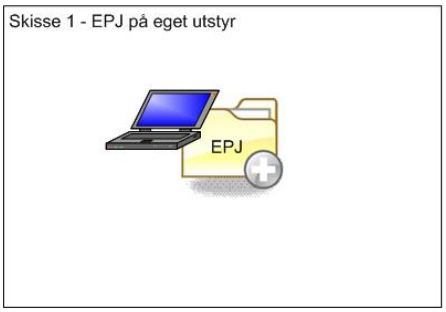
Figuren nedenfor viser hvordan veilederen bør leses, avhengig av om *virksomheten* bruker *databehandler* (*EPJ* er installert hos og driftes av en *leverandør*), eller om *virksomheten* har *EPJ* på eget datautstyr.

Leseveiledning

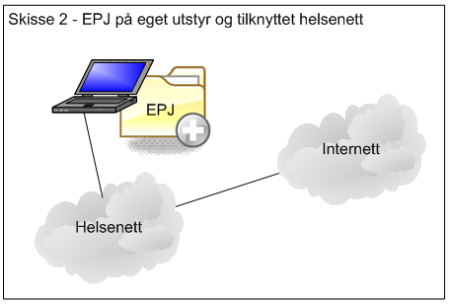


Virksomhetene har forskjellige løsninger ved å installere *EPJ* på eget utstyr, benytte *databehandler*som drifter EPJ hos seg og tilknytning til*helsenettet*. Skissene nedenfor illustrerer alternativer og gir veiledning i hvilket omfang kravene i kapittel 0 må ivaretas.

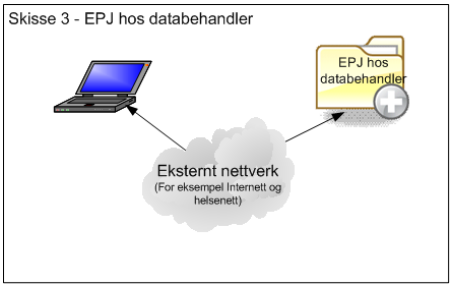
Virksomheten har installert *EPJ* på eget utstyr(server eller PC) som ikke er tilknyttet Internett og må ivareta alle relevante krav i kapittel 0.Se kapittel 3.1, 3.2, 3.3 og 3.5 (kun SMS).



Virksomheten har installert *EPJ* på eget utstyr(server eller PC) og har tilkobling til *helsenettet* for tilgang til Internett og ekstern e-post. *Virksomheten* må ivareta flere av kravene i kapittel 0. Se kapittel 3.1, 3.2, 3.3,3.4og 3.5.



Virksomheten benytter *databehandler*som drifter *EPJ* hos seg og behandler har tilgang til *EPJ* via *helsenett* eller Internett. *Virksomheten* må ivareta enkelte av kravene i kapittel 0.Se kapittel 3.1, 3.2, 3.4 og 3.5.



1.2 Ansvar

Det er *virksomhetens* ledelse, ved *databehandlingsansvarlig*, som er ansvarlig for at personvern og informasjonssikkerhet ivaretas. Det vil si at den *databehandlingsansvarlige* skal sørge for at:

- kravene til *konfidensialitet*, *integritet*, *tilgjengelighet* og *kvalitet* blir ivaretatt
- *taushetsplikten* som påhviler helsepersonellet ivaretas i *virksomheten*
- *pasientens* rettigheter blir ivaretatt

Virksomhetene kan være organisert på ulike måter:

- Som et *enkeltpersonforetak*. Eieren av foretaket er *databehandlingsansvarlig*
- *Formalisert arbeidsfelleskap*. I et *formalisert arbeidsfellesskap* er det minst to *virksomheter* (som kan være enkeltpersonforetak). I utgangspunktet er hver av *virksomhetene databehandlingsansvarlig*. Ved etablering av *formalisert arbeidsfellesskap* må ansvarsforholdene være klart definerte ved at *virksomhetene* må ta stilling til hvem som skal være *databehandlingsansvarlig* for felles journal[1] (dvs. én eller alle). Et *formalisert arbeidsfellesskap* kan ha ulike former:
    - *Gruppesamarbeid* med flere *virksomheter* hvor alle arbeider innen samme profesjon og hvor det er etablert felles journal. Rollen som *databehandlingsansvarlig* for felles journal er gitt til én *virksomhet*, eller alle *virksomhetene* er *databehandlingsansvarlige* for felles journal
    - *Profesjonssamarbeid* består av flere profesjoner som arbeider sammen og hvor det er etablert felles journal. Rollen som *databehandlingsansvarlig* or felles journal er gitt til én *virksomhet*, eller alle *virksomhetene* er *databehandlingsansvarlige* for felles journal
- Aksjeselskap. Styret ved styreleder skal forvalte databehandlingsansvaret på vegne av selskapet, men i det daglige vil oppgavene normalt være delegert til daglig leder, dersom *virksomheten* har daglig leder

[1]Med «felles journal» menes *virksomhetsovergripende pasientjournal*. Se veileder "Veileder med avtaleeksempler ved samarbeid om felles journal", på www.normen.no

- Ansvarlig selskap (ANS/DA). Virksomhetens øverste administrative leder skal forvalte databehandlingsansvaret på vegne av selskapet

Den som har det daglige ansvaret for informasjonssikkerheten (databehandlingsansvarlig), kan delegere oppgaver til egne ansatte eller eksterne, eksempelvis til en leverandør. Ansvaret for at personvern og informasjonssikkerhet ivaretas i virksomheten vil uansett tilfalle databehandlingsansvarlig.

Velger *virksomheten* å benytte *databehandler*, skal *databehandlingsansvarlig* og *databehandler* til sammen sørge for tilfredsstillende personvern og informasjonssikkerhet.

Når *databehandlingsansvarlig* overlater *helse- og personopplysninger* til en *databehandler* skal det inngås en databehandleravtale. Databehandleravtalen regulerer hva *databehandlingsansvarlig* har ansvaret for og hva *databehandler* har ansvaret for. Forslag til databehandleravtale kan hentes på www.normen.no (se Faktaark 10 – Bruk av databehandler (ekstern driftsenhet)).

1.3 Bakgrunn

Behandler virksomheten *helse- og personopplysninger* innebærer det at *virksomheten* må følge lover og forskrifter og ha tilfredsstillende rutiner for behandling, bruk og beskyttelse av opplysningene.

Økt elektronisk samhandling og bruk av IT-systemer i *behandlingen* av *helse- og personopplysninger* preger arbeidsdagen for *virksomhetene*, både i det offentlige og det private. *Virksomhetene* må derfor ha personvern og informasjonssikkerhet på agendaen, og tenke gjennom relevante problemstillinger for å unngå uønskede hendelser og være forberedt dersom uhellet likevel skulle inntreffe. *Databehandlingsansvarlig* bør reflektere over bl.a. følgende problemstillinger:

- Vil klinikken kunne fortsette virksomheten dagen derpå hvis det oppstår brann på klinikken og datamaskinen ødelegges?
- Vil det være mulig for andre å komme inn på PCen din og lese opplysninger om pasientene hvis du mister din bærbare PC på vei hjem fra jobb?
- Hva er konsekvensene for din virksomhet om *helse- og personopplysninger* kommer på avveie?

Problemstillingene over er kun noen av mange eksempler på hvorfor personvern og informasjonssikkerhet er viktig og relevant for din *virksomhet.* Ved å ha fokus på personvern og informasjonssikkerhet, og ved å følge denne veilederen kan risikoen minimeres for at uønskede hendelser oppstår, samtidig som *virksomheten* stiller forberedt dersom de likevel skulle inntreffe.

Veilederen er utarbeidet for styringsgruppen for *Normen* med støtte fra Helsedirektoratet av KPMG, i samarbeid med psykologer, fysioterapeuter, manuellterapeuter og kiropraktorer og leverandører.

1.4 Om Normen

Norm for informasjonssikkerhet (*Normen*) ble lansert i august 2006. *Normen* skal bidra til tilfredsstillende informasjonssikkerhet hos den enkelte *virksomhet*, og i helse- og omsorgssektoren generelt. I tillegg skal *Normen* bidra til at den som utleverer *helse- og personopplysninger* kan være trygg på at mottaker har tilfredsstillende informasjonssikkerhet.

Normen bygger på gjeldende bestemmelser om personvern og informasjonssikkerhet, bl.a. reglene i personopplysningsloven og helseregisterloven. Personvern- og helselovgivningen stiller krav til informasjonssikkerhet. Disse kravene gjelder uavhengig av *Normen*, og aktuelle tilsynsmyndigheter (særlig Datatilsynet og Helsetilsynet) kan kontrollere den enkelte *virksomhets* etterlevelse av det til enhver tid gjeldende regelverk. *Normen* stiller enkelte krav som supplerer gjeldende regelverk.

Enhver *virksomhet* som etterlever *Normen* vil tilfredsstille alle grunnkrav i lovverket til informasjonssikkerhet. Alle virksomheter som er tilknyttet *helsenettet* er avtalerettslig forpliktet til å følge *Normen*.

2 OPPGAVER DATABEHANDLINGSANSVARLIG SKAL IVARETA

Denne delen av veilederen handler om oppgavene som skal ivaretas av *databehandlingsansvarlig* for å sikre personvern og informasjonssikkerhet. Oppgavene kan ikke delegeres til personer utenfor *virksomheten*.

Lovverket beskrevet i kapittel 4.1stiller krav til personvern og informasjonssikkerhet. Kravene er gjeldende uavhengig av *Normen*, og aktuelle tilsynsmyndigheter (særlig Datatilsynet og Helsetilsynet) kan kontrollere *virksomhetens* etterlevelse av det til enhver tid gjeldende regelverk. Datatilsynet har sanksjonsmuligheter om kravene ikke følges.

Normen pålegger *virksomheten* å etablere et styringssystem for informasjonssikkerhet. Et styringssystem angir aktiviteter for å rettlede og styre *virksomheten* og er en del av den ordinære internkontrollen. Kapittel 2.1, 2.2 og 2.3 beskriver tiltak som inngår i styringssystemet.

Mal for etablering av styringssystem finnes i vedlegg 4.6. Malen fylles ut av *databehandlingsansvarlig* og eventuelt med støtte fra *databehandler*.

2.1 Krav til informasjonssikkerhet

2.1.1 Sikkerhetsmål

Databehandlingsansvarlig er ansvarlig for å utarbeide sikkerhetsmål for behandling av helse- og personopplysninger. *Behandlingen* av *helse- og personopplysninger* og *virksomhetens* sikkerhetstiltak skal gjennomføres i tråd med sikkerhetsmålene.

Sikkerhetsmålene bør være konkrete, målbare og lett å operasjonalisere i en sikkerhetsstrategi. Eksempler på sikkerhetsmål er:

- *Virksomheten* har nulltoleranse for brudd på lovverk tilknyttet personvern (se kapittel 4.1)

- *Databehandlingsansvarlig* skal sikre at informasjon behandles iht. krav i relevante lover og forskrifter (se kapittel 4.1)
- *Behandling* av *helse- og personopplysinger* skal skje i tråd medreglene om *taushetsplikt*, slik at uautoriserte ikke får kjennskap til opplysningene
- *Virksomhetens* informasjonsbehandling skal beskyttes mot identifiserte trusleriht fastsatt nivå for akseptabel risiko, både interne og eksterne, samt tilsiktede og utilsiktede (se kapittel 2.1.3 nedenfor)
- Ansatte som bruker *virksomhetens* informasjonssystemer skal ha kompetanse for bruk av systemene og ivareta sikkerhetskravene

Normen fastsetter at som minimum skal *helse- og personopplysninger*:

- Være tilgjengelig for rett personell til rett tid i henhold til fastsatte prinsipper for tilgangsstyring (se kapittel 2.2.1 nedenfor)
- Behandles i tråd med reglene om *taushetsplikt* og være beskyttet slik at uvedkommende ikke får kjennskap til opplysningene. Uvedkommende omfatter også personell som ikke har tjenstlig behov
- Være fullstendige, oppdaterte og korrekte når de brukes og iht krav til ajourhold
- Være et resultat av rettmessige registreringer og kontrollerte aktiviteter
- Begrenses slik at kun det som er nødvendig av *helse- og personopplysninger behandles*

2.1.2 Sikkerhetsstrategi

Med utgangspunkt i sikkerhetsmålene skal *databehandlingsansvarlig* utarbeide en sikkerhetsstrategi for *virksomheten*. En sikkerhetsstrategi er en overordnet beskrivelse av hvordan sikkerhetsmålene skal nås gjennom ulike sikkerhetstiltak.

Sikkerhetsstrategien vil være ulik for *virksomheter* som har delegert oppgaver til en *databehandler*(ekstern drift av *EPJ*) enn for *virksomheter* som har valgt å beholde dette ansvaret internt. Sikkerhetsstrategien skal gjenspeile dette valget.

Sikkerhetsstrategien skal være så entydig at *virksomheten* ut fra den kan etablere nødvendige tiltak og utarbeide prosedyrer i styringssystemet for informasjonssikkerhet.

Eksempel på innhold i en sikkerhetsstrategi:
- Fysiske sikkerhet skal hindre at uautoriserte får adgang til lokaler der *helse- og personopplysninger* lagres og *behandles*
- *Tilgang* til systemer og informasjon skal kun gis til medarbeidere etter tjenstlig behov
- *Tilgang* til systemer og informasjon for uvedkommende skal forhindres
- All *tilgang* og forsøk på uautorisert *tilgang* til helse- og personopplysninger skal hendelsesregistreres
- Brukere av informasjonssystemet skal læresopp i bruk av systemene og i sikkerhetstiltakene
- Alle som får *tilgang* til *helse- og personopplysninger* skal signere taushetserklæring

2.1.3 Nivå for akseptabel risiko

Forsvarlig risikostyring krever at det finnes kriterier å styre etter slik at det er mulig å si når en risiko øker ut over det som er fastsatt som nivå for *akseptabel risiko*.

Utarbeidelse av nivå for akseptabel risiko er fastsatt i personopplysningsforskriften og det er *databehandlingsansvarlig* som skal bestemme nivået. Se *Normen* kapittel 4.4 for minimumsnivå for *akseptabel risiko*.

Arbeidet med informasjonssikkerhet skal gjennomføres etter prinsippet om forholdsmessig sikring av*konfidensialitet*, *integritet*, *tilgjengelighet* og *kvalitet*. I noen situasjoner kan sikkerhetsbehovene komme i konflikt. Særlig vil *konfidensialitet* og *tilgjengelighet* kunne være vanskelig å forene. Det er viktig at kryssende hensyn identifiseres, og at prioritering mellom forskjellige sikkerhetsbehov fremgår i beskrivelsen av akseptabelt risikonivå.

Eksempel på nivå for *akseptabel risiko*:
- *Virksomheten* aksepterer ikke at serveren med *EPJ-systemet* blir stjålet (*konfidensialitet*)
- *Virksomheten* aksepterer ikke at utskrifter med helseopplysninger kommer på avveie (*konfidensialitet*)
- *Virksomheten* aksepterer ikke at helseopplysninger sendes i e-post (*konfidensialitet*)
- *Virksomheten* aksepterer ikke at *EPJ-systemet* er nede i mer enn 4 timer per uke(*tilgjengelighet*)
- Det tillates maksimalt ett driftsavbrudd med varighet over én arbeidsdag per år (*tilgjengelighet*)
- *Sensitive personopplysninger* i *EPJ- systemet* skal ikke kunne endres uten at dette er sporbart (*integritet*)

2.1.4 Oversikt over behandlinger av helse- og personopplysninger

Databehandlingsansvarlig skal til enhver tid ha oversikt over hvilke *behandlinger* av *helse- og personopplysninger* som skjer i *virksomheten*. For profesjonene i denne veilederen vil det være føring av pasientjournal i *EPJ-systemet* og eventuelt forskning. Se eksempel på oversikt i kapittel 4.6.1.

Det er viktig at *virksomheten* er bevisst på at den ikke kan bruke *helse- og personopplysninger* til andre formål og i andre sammenhenger uten at det foreligger samtykke fra *pasienten*.

Føring av pasientjournal i *EPJ-systemet* er lovhjemlet og *virksomheten* skal sende melding til Datatilsynet.

For forskning vises det til veilederen ”Personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren”.

Nærmere om *meldeplikten*

Alle *behandlinger* av *helse- og personopplysninger* skal meldes til Datatilsynet før *behandlingen* tar til (jf. kapittel 4.1.1). Det er *databehandlingsansvarlig* som har ansvaret for å melde *behandlingen*.

Meldingen skal blant annet inneholde hvem som har det daglige ansvaret for oppfyllelse av *databehandlingsansvarliges* plikter. Når det skjer endringer i behandlingsmåten, skal det sendes en endringsmelding. *Databehandlingsansvarlig* skal hvert tredje år melde *behandling* av personopplysninger til Datatilsynet (jf. kapittel 4.1.1).

Alle meldinger sendes inn til Datatilsynet via skjemaet "Melding om behandling av personopplysninger" på nettstedet www.datatilsynet.no

2.2 Oppgaver ved behandling av helse- og personopplysninger

Denne delen av veilederen omfatter de daglige, løpende oppgavene *databehandlingsansvarlig* står overfor ved*behandling* av *helse- og personopplysninger*.

2.2.1 Tilgangsstyring

Med tilgangstyring menes at *databehandlingsansvarlig* har kontroll med alle som har tilgang til *pasientopplysninger*, hvilken rolle de har og hvilke rettigheter de har i *EPJ-systemet*.

> *Taushetsplikten* og generelle personvernprinsipper gjør at *tilgang* til *helse- og personopplysninger* bare skal gis i den grad dette er nødvendig for å yte helsehjelp og iden grad *pasienten* ikke motsetter seg det.

Databehandlingsansvarlig er ansvarlig for å administrere slik at *tilgangen* til *helse- og personopplysninger* kun gis ved *tjenstlig behov*(arbeidsoppgaver). I de fleste *EPJ-systemer* styres tilgang av hvilke roller medarbeiderne har, men medarbeiderens rolle skal ikke alene gi *tilgang* til *helse- og personopplysninger* og bruk av *informasjonssystemene.* For eksempel forekommer det at sekretæren må føre journal, lese eller på annen måte fremskaffe informasjon i løpet av en behandlingsseanse.

Tilgangsstyringen må derfor ta utgangspunkt i hvordan den enkelte *virksomheten* konkret er organisert. Prosedyrene som beskriver tilgangsrettighetene skal speile praksisen i *virksomheten*. Momenter som vil kunne påvirke den konkrete tilgangsstyringen er bl.a.:

- størrelsen på *virksomheten*
- organisasjonsform (jf. kap. 1.2)
- bruk av *databehandler*, f.eks. ved at en tredjepart drifter og lagrer journalopplysninger
- *leverandør* av journalsystem, der *leverandøren* har *fjernaksess*
- *nødrettstilgang*

Virksomheten bør utarbeide en oversikt som viser *tilgangene* per rolle. Det er *databehandlingsansvarligs* oppgave å etablere rutiner som sikrer at dette blir gjennomført. For å motvirke at en *tilgang* til informasjonssystemet misbrukes, skal den enkelte bruker *autentiseres* ved hjelp av for eksempel passord. *Autentiseringen* for å bekrefte en påstått identitet skal være forholdsmessig ut fra *virksomhetens* størrelse og virkefelt. Med dette menes at *autentisering* blant annet må sees i sammenheng med hvor mange brukere som er tildelt *autorisasjon*. *Autentisering* bør derfor begrunnes i *virksomhetens* risikovurdering (se kapittel 2.3.3 nedenfor).

Krav til passord

- For pålogging til interne systemer (nettverk, *EPJ* internt o.l.) bør det benyttes minimum brukernavn/passord – systemet bør *konfigureres* til å stille krav om minimum 7 tegn, minst et tall og både store og små bokstaver
- For pålogging fra eksterne nett, f.eks. *hjemmekontor*, som gir tilgang til *helse- og personopplysninger*, skal *autentiseringen* ikke innebære økt risiko utover det som gjelder for stasjonært utstyr

Krav til bruk av passord

- Utlån av passordet til andre personer er ikke tillatt
- Passordet skal ikke skrives ned slik at uautoriserte kan finne og bruke det
- Det skal være prosedyrer for periodisk bytte av passord. Er det mistanke om at passordet er kommet på avveie eller gjort kjent for andre skal passordet også byttes
- Passord skal ikke oppgis på telefon uten at det er trygghet for at det er den rette personen som får oppgitt passordet

Når en person er *autorisert* for *tilgang*, skal vedkommende rent faktisk oppnå *tilgang* i samsvar med *autorisasjonen*. *Virksomheten* må derfor opprette brukere i informasjonssystemet (brukerkontoer) iht. dette. All tildeling av *autorisasjon* skal registreres i et *autorisasjonsregister*(se Faktaark 47 – Autorisasjonsregister, for krav til innhold og oppbevaring av *autorisasjonsregisteret*). *Databehandlingsansvarlig* er ansvarlig for å etablere rutiner som sikrer at det minimum årlig blir gjennomført kontroll av tildelte *autorisasjoner*.

Det er viktig å være klar over at helseregisterloven ikke tillater at personell utenfor *databehandlingsansvarliges* instruksjonsmyndighet har *tilgang* til *virksomhetens helse- og personopplysninger*. For eksempel har en leder myndighet til å bestemme hvordan en ansatt skal utføre en oppgave og instruere *databehandler* gjennom databehandleravtalen.

Når det gjelder felles journal i *formalisert arbeidsfelleskap* reguleres *tilgang* ift avtalen mellom partene i det *formaliserte arbeidsfellesskapet*. For mer informasjon, se Veileder med avtaleeksempler ved samarbeid om felles journal.

Snoking i pasientjournalen er forbudt (jf. helseregistreringsloven § 13 a.). Dette innebærer blant annet at det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte *helseopplysninger* uten at det er begrunnet i helsehjelp, administrasjon av helsehjelp, internkontroll, kvalitetssikringen av helsehjelpen eller har særskilt hjemmel i lov eller forskrift.

Se også Faktaark 14 - Tilgangsstyring, Faktaark 31 - Passord og passordhåndtering og Faktaark 47 - Autorisasjonsregister på www.normen.no.

2.2.1.1 **Taushetserklæring**

Alle som får tilgang til fortrolige opplysninger om *virksomheten* eller *virksomhetens pasienter*, skal signere en taushetserklæring. Taushetserklæringen er ment som et hjelpedokument i forbindelse med bruk av eksterne konsulenter/*leverandører* til *behandling* av *helse- og personopplysninger*.

Undertegnet taushetserklæring innebærer en absolutt *taushetsplikt* for alle *helse- og personopplysninger*. Det er *databehandlingsansvarliges* oppgave å innhente underskrevet taushetserklæring fra eksterne *leverandører* eller avtale med *leverandør*(for eksempel *databehandler*) at denne forvalter taushetserklæringer om egne ansatte.

Eksempel på taushetserklæring kan hentes på www.normen.no.

2.2.2 Sikring av teknisk løsning

Databehandlingsansvarlig skal sikre *virksomhetens* tekniske løsning på en slik måte at uautorisert personell ikke får adgang til IT-utstyr og tilgang til *helse- og personopplysninger*.

Dette innebærer at *databehandlingsansvarlig* er ansvarlig for å sikre rutiner og en bevisstgjøring som forhindrer at *helse- og personopplysninger* kommer på avvei, enten via IT-utstyr eller utskrifter som blir tilgjengelige for uautoriserte. Dersom *databehandlingsansvarlig* ikke selv har den tekniske kompetansen til å sikre de tekniske løsningene, skal *databehandlingsansvarlig* sørge for at dette gjøres av teknisk kyndig personell og at det er gjennomført risikovurdering før *behandlingen* av *helse- og personopplysninger* starter.

PC og mobiltelefon

Lagres *helse- og personopplysninger* på mobilt utstyr som PC og mobiltelefon, skal data krypteres med krypteringsstyrke som oppfyller "Kravspesifikasjon for PKI i offentlig sektor"[2].Mobilt utstyr utgjør en større risiko enn stasjonært utstyr når det kommer til tap, tyveri og annet uautorisert bruk (slik som av barn). Ingen andre enn den som er *autorisert* til å bruke *virksomhetens* PC skal benytte denne. Av dette følger at PC som inngår i *hjemmekontor* ikke bør brukes til private oppgaver. Det mobile utstyret skal sikres med *autentisering* (for eksempel passord) for å hindreuautorisert *tilgang* mv. på samme måte som stasjonært utstyr på klinikken. Det er *databehandlingsansvarlig* som må påse at *virksomheten* oppfyller kravene for sikring av PC og mobiltelefon.

Mobilt utstyr som PC og mobiltelefon kan rammes av ondsinnet programvare som inneholder virus e.l. *Databehandlingsansvarlig* skal etablere rutiner og en kultur som hindrer at personell benytter utstyret på nettsider som kan medføre ondsinnet programvare. *Databehandlingsansvarlig* skal påse at det etableres løsning for å hindre ondsinnet programvare (se kapittel 3.2).

Skriver

Skriverutgjør en risiko for lekkasje av *helse- og personopplysninger*. *Databehandlingsansvarlig* skal sørge for gode rutiner rundt håndtering av utskrift av *helse- og personopplysninger.* Dette innebærer at alle utskrifter hentes med én gang av den personen som skrev ut opplysningene og at feilsendt utskrift rettes opp ved umiddelbar fjerning av utskriften. Videre skal *databehandlingsansvarlig* påse at skrivere som benyttes til *helse- og personopplysninger* er plassert på steder som er avlåst eller bevoktet, det vil si at skrivere ikke skal plasseres i områder som er åpne og uten tilsyn.

Internett og trådløst nettverk

Databehandlingsansvarlig må gjøre *virksomhetens* ansatte kjent med risikoen ved uforsiktig adferd på Internett og bruk av trådløse nettverk og faren for ondsinnet programvare som uforsiktig bruk medfører. Skade fra ondsinnet programvare kan blant annet forhindres ved å unngå nettsider med skadelig innhold og ved å unngå oppkobling på eksterne nettverk via *virksomhetens* mobile enhet.

[2] https://www.regjeringen.no/nb/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/

Trådløse nettverk er også sårbare for at uvedkommende kopler seg på, dersom sikringen ikke er tilstrekkelig. *Databehandlingsansvarlig* må påse at trådløst nettverk er sikret iht gjennomført risikovurdering (se kapittel 2.3.3 nedenfor).

Tilkobling til *helsenettet* (Norsk Helsenett SF) ivaretar kravet til en sikker tilkobling til Internett.

2.2.3 Inngåelse og oppfølging av leverandøravtaler

Virksomheten må inngå og administrere avtaler med *leverandører* i sammenheng med informasjonssikkerheten.

Antall *leverandører* som benyttes bør begrenses, da datasystemer i stor grad henger sammen, og det kan bli komplisert for *databehandlingsansvarlig* å finne frem til hvem av *leverandørene* som er årsak til eventuelle hendelser og problemer.

Databehandler

Hvis *virksomheten* benytter en *databehandler*, er det lovpålagt at partene inngår en skriftlig databehandleravtale. Det må klargjøres hvem som er *databehandlingsansvarlig* og hvem som er *databehandler*.

Leverandør av elektroniske tester som psykologer benytter vil være *databehandler* ved at det lagres *personopplysninger* og testresultater på *leverandørens* utstyr og det må inngås en databehandleravtale.

Utgangspunkt for en slik avtale finnes på www.normen.no. Se kap. 1.2.

Øvrige leverandører

Hvilke *leverandører virksomheten* inngår avtale med, avhenger av spesialisering, hvilket marked *virksomheten* retter seg mot, *virksomhetens* interne kompetanse, mv. For at *virksomheten* skal oppfylle informasjonssikkerhetskravene, kan det være aktuelt å inngå avtaler med følgende *leverandører:*

- *leverandør* av *EPJ-system* og andre pasientadministrative systemer
- sikkerhetsleverandør som benytter *fjernaksess*(jf. Veileder for *fjernaksess* for vedlikehold og oppdateringer mellom *leverandør* og virksomhet på www.normen.no)

Innholdet i avtaler med leverandører er ivaretakelse av *taushetsplikten* for helse- og personopplysninger og ansvaret for konkrete oppgaver ifm informasjonssikkerhet.

2.2.4 Opplæring og kompetanseheving

Databehandlingsansvarlig har ansvaret for å tilrettelegge og sørge for at det gjennomføres opplæring i informasjonssikkerhet og i bruk av de ulike informasjonssystemene.

Formålet med opplæringen er å gi *virksomhetens* medarbeidere tilstrekkelig kompetanse slik at de kan ivareta personvern og informasjonssikkerhet etter gjeldene krav. Gode opplæringstiltak vil bl.a. bidra til at ledere og medarbeidere:

- forstår hensikten med og blir i stand til å ivareta personvernet

- blir bevisste på krav i *Normen* og i denne veilederen
- blir oppmerksom på ansvarsforhold med hensyn til informasjonssikkerhet

Databehandler er også ansvarlig for å gjøre seg kjent med informasjon i Faktaark 9 - Opplæring av ledere og medarbeidere på www.normen.no.

2.2.5 Pasientinformasjon og informert samtykke

Behandling av helse- og personopplysninger er som hovedregel kun tillat dersom *pasienten* samtykker til det. Likevel kreves det ikke samtykke for å opprette en pasientjournal og *pasienten* kan ikke motsette seg at *helse- og personopplysninger* blir journalført hvis helsehjelpen mottas. Helsepersonellets journalføringsplikt går foran den enkeltes rett til å samtykke eller til å nekte registreringen.

At samtykket er "informert" betyr at det foreligger en frivillig, uttrykkelig erklæring fra *pasienten* om at han eller hun godtar *behandling* av opplysninger om seg selv. Loven stiller ikke noe krav om at et informert samtykke skal være skriftlig, men skriftlighet sikrer varig og sikker dokumentasjon av at samtykke foreligger. Om ønskelig kan samtykkeerklæring i kapittel 4.3 benyttes.

> Når *virksomheten* registrerer *helse- og personopplysninger* ved ytelse av helsehjelp skal *pasienten* være informert om at registreringen skjer samt til hvilket formål. *Pasienten* skal ha informasjon om sine rettigheter knyttet til samtykke, reservasjon, innsyn, retting og sletting. *Virksomheten* kan gi informasjonen om dette ved oppslag på kontoret, i brev til *pasienten* eller i en brosjyre. Eksempel på informasjonsplakat finnes i kapittel 4.4.

Mangler *pasienten* samtykkekompetanse gjelder spesielle regler for samtykke (se kapittel 2.2 i dokumentet Video-, lyd- og bildeopptak i helse- og omsorgssektoren - en veileder).

Pasienten har rett til både å gi og å tilbakekalle samtykke etter eget valg. *Pasienten* har ikke noen plikt til å begrunne valget.

2.2.6 Overholdelse av innsynsrett

Pasient- og brukerrettighetsloven gir *pasienten* som hovedregel innsynsrett. Innsynsretten består av tre elementer som *virksomheten* må kunne håndtere for at innsynsretten skal bli reell og effektiv:

- *Pasienten* har rett til å se på og lese i sin egen journal med bilag
- *Pasienten* har, etter nærmere forespørsel, rett til kopi av (deler av) journalen
- *Pasienten* har, etter nærmere forespørsel, rett til en enkel og kortfattet forklaring av faguttrykk eller lignende
- *Pasienten* har rett til å se hvem som har sett/brukt journalen og hvor ofte dette har skjedd

> Det er viktig å være klar over at *pasienten* har rett til innsyn i journalen med bilag. Bilag er for eksempel røntgenbilder, video- og lydopptak, pleieplaner og andre skriftlige nedtegnelser. Alle former for journaler omfattes av innsynsretten, både papir- og *elektronisk pasientjournal (EPJ)*.

2.2.7 Utlevering av journal eller opplysninger i journal

Pasienten har rett til å motsette seg utlevering av journal eller opplysninger i journal. Opplysningene kan heller ikke utleveres dersom det er grunn til å tro at *pasienten* ville motsette seg dette ved forespørsel. *Databehandlingsansvarlig* kan likevel utlevere *helse- og personopplysninger* dersom tungtveiende grunner taler for det.

Helsepersonell som yter helsehjelp skal gis nødvendige og relevante *helse- og personopplysninger* i den grad det er nødvendig for å kunne gi helsehjelp til *pasienten* på forsvarlig måte. Det skal fremgå av journalen at annet helsepersonell er gitt *helse- og personopplysninger* (for eksempel ved tverrfaglig kommunikasjon).*Helse- og personopplysninger* kan gis av *databehandlingsansvarlig* eller helsepersonell som har dokumentert opplysningene.

Utlevering til barneverntjenesten

Når det er grunn til å tro at et barn blir mishandlet i hjemmet eller det foreligger andre former for alvorlig omsorgssvikt skal helsepersonell gi opplysninger til barneverntjenesten.(jf. lov om barneverntjenester §6-4 tredje ledd, jf. §§ 4-10, 4-11 og 4-12).

Utlevering til nødetater

Helsepersonell skal varsle politi og brannvesen dersom dette er nødvendig for å avverge alvorlig skade på person eller eiendom (jf. helsepersonelloven § 31).

2.2.8 Retting og sletting av pasientopplysninger, herunder oppbevaring av pasientjournal

Pasienten kan kreve at feil i *helse- og personopplysningene* om vedkommende blir rettet eller slettet. F.eks. kan *pasienten* kreve at mangelfulle, feilaktige eller utilbørlige *helse- og personopplysninger* eller utsagn blir rettet. Det er helsepersonellet som må vurdere om det er adgang til å rette eller slette opplysninger i journalen.

Ved retting i pasientjournal er det *databehandlingsansvarlig som* skal sørge for at opplysningen korrigeres evt. suppleres med ny journalføring slik at informasjonen samlet sett gir et mest mulig riktig bilde. Utfyllende regler om retting og sletting finnes i pasientjournalforskriften.

Helse- og personopplysninger i pasientjournaler skal oppbevares i minst 10 år etter siste innføring i journalen.

Databehandler er også ansvarlig for å gjøre seg kjent med informasjon i Faktaark 25 - Lagringstid og sletting av helse- og personopplysninger på www.normen.no.

2.2.9 Overføring av helse- og personopplysninger til utlandet

Ved overføring av *helse- og personopplysninger* til utlandet skal *databehandlingsansvarlig* påse at reglene for dette følges.

Helse- og personopplysninger kan overføres til land innen EU/EØS-området og til land som har vært vurdert og godkjent av EU-kommisjonen til å ha forsvarlig beskyttelsesnivå for personopplysninger. Overføring av *helse- og personopplysninger* til land utenfor EU/EØS-

området er som hovedregel ikke tillatt. Det vil imidlertid være tillatt på særskilt grunnlag, f.eks. hvis den utenlandske mottakeren skriftlig forsikrer overfor den norske *databehandlingsansvarlige* at opplysningene vil bli behandlet i samsvar med EUs regelverk og *pasienten* har gitt samtykke. For mer informasjon, se www.datatilsynet.no.

2.3 Oppfølging av informasjonssikkerheten

Denne delen av veilederen omfatter oppgavene *databehandlingsansvarlig* skal utføre for å påse at *behandlingen* av *helse- og personopplysninger* er iht sikkerhetsmålene, strategien og vedtatte prosedyrer.

2.3.1 Sikkerhetsrevisjon

Databehandlingsansvarlig skal følge opp at sikkerheten ivaretas ved jevnlig og minimum årlig sikkerhetsrevisjon. Det skal foreligge en plan for sikkerhetsrevisjoner som en del av internkontrollen. Sikkerhetsrevisjonen må som et minimum omfatte en vurdering av *virksomhetens* organisering, sikkerhetstiltak og bruken av kommunikasjonspartnere og *leverandører*.

Formålet med å gjennomføre sikkerhetsrevisjon er at *databehandlingsansvarlig* skal kunne:

- kontrollere at det er gjennomført nødvendige sikkerhetstiltak
- verifisere at sikkerhetstiltakene fungerer
- kontrollere at lover og regler vedrørende informasjonssikkerhet følges
- sikre at etablerte prosedyrer for sikkerhet er kjent, at de benyttes og at de fungerer etter hensikten

Om ønskelig kan Faktaark 6b - Sikkerhetsrevisjon – sjekkliste på www.normen.no, benyttes av *databehandlingsansvarlig* som utgangspunkt for sikkerhetsrevisjoner. Vær oppmerksom på at sjekklisten er omfattende og bør tilpasses egen virksomhet.

2.3.2 Fornyelse av melding til Datatilsynet

Det er krav at melding om behandling av personopplysninger til Datatilsynet, skal fornyes hvert tredje år.

Fornyelsesmeldingen sendes via www.datatilsynet.no (på samme måte som den opprinnelige meldingen, se kap. 4.1.1). *Databehandlingsansvarlig* må påse at slik fornyelse finner sted, gjerne ved at meldinger legges inn som et fast punkt i sikkerhetsrevisjonen.

2.3.3 Risikovurdering

Databehandlingsansvarlig skal påse at det gjennomføres risikovurderinger for å kartlegge risikoområder og sannsynlighet og konsekvens for uønskede hendelser. Resultatet av risikovurderingen skal sammenlignes med nivå for akseptabel risiko. Er kartlagt risiko høyere enn det fastsatte nivået må det gjennomføres tiltak.

Ved større endringer eller vesentlige *avvik* skal *databehandlingsansvarlig,* eventuelt sammen med *databehandler,* gjennomføre en risikovurdering før informasjonssystemet tas i bruk. Gjennom risikovurderingen må *virksomheten* vurdere hensynet til personvernet og informasjonssikkerhet opp mot hensynet til å kunne yte helsetjenester på en effektiv måte.

Ofte vil det være en konflikt mellom hensynet til *tilgjengelighet* for *helse- og personopplysninger* og hensynet til *konfidensialitet* for de samme opplysningene. Begge hensyn er legitime, og den konkrete avveiningen mellom dem må være hensiktsmessig; ytterligheter i begge retninger er uheldig.

Følgende momenter kan være aktuelle å risikovurdere*:*

- uautorisert *tilgang* til og bruk av informasjonssystemet (for eksempel ved manglende eller for svake passord)
- uautoriserte (for eksempel *pasienter*) får innsyn i andres *helse- og personopplysninger* fra skjermer eller utskrifter
- bruk av minnepinne (innebærer f.eks. risiko for ondsinnet programvare og at *helse- og personopplysninger* kommer på avveie)
- risiko knyttet til utlån av brukernavn og passord og dermed feil ved signering av journaler
- *hendelsesregistreringen* er mangelfull slik at uautorisert *tilgang* ikke oppdages
- sikring slik at uautoriserte personer utenfor *virksomheten*, uansett ressurser og kunnskap, ikke skal kunne få *tilgang* til og/eller kunne endre eller slette *helse- og personopplysninger*
- at data kan tilbakekopieres fra sikkerhetskopier om data blir slettet eller blir inkonsistente

Risikovurderingen gjennomføres ved en vurdering av uønskede hendelser opp mot eksisterende tiltak. Løser eksisterende tiltak risikoen i hendelsen vil konsekvensene og sannsynligheten for at hendelsen inntreffer være lave. Motsatt om eksisterende tiltak ikke løser risikoen i hendelsen. Da må det iverksettes tiltak for å bringe risikoen ned på et akseptabelt nivå. Risikovurderinger skal gi følgende resultater:

- oversikt over identifiserte trusler (uønskede hendelser)
- sannsynlighet for at en uønsket hendelse kan inntreffe, hensyntatt eksisterende tiltak
- konsekvenser av en uønsket hendelse, hensyntatt eksisterende tiltak
- forslag til nye tiltak for å bringe for høy risiko ned på nivå for akseptabel risiko

Se kapittel 4.5 for mal for gjennomføring av risikovurdering i *virksomheten.*

Se også Faktaark 7 – Risikovurdering på www.normen.no for hvordan risikovurdering kan gjennomføres.

2.3.4 Avvikshåndtering

Alle *virksomheter* som *behandler helse- og personopplysninger* skal ha prosedyrer for håndtering av *avvik*.

Databehandlingsansvarlig skal sikre at *virksomheten* har tilstrekkelige prosedyrer for avviksbehandling og retningslinjer for eskalering ved vesentlige hendelser.

Formålet med avviksbehandling er å sikre at:
- *virksomhetens* ledelse er tilstrekkelig involvert i hendelser som kan medføre lovbrudd eller hindrer effektiv utførelse av arbeidet
- sikkerhetsbrudd håndteres på en systematisk måte
- normaltilstanden gjenopprettes etter et sikkerhetsbrudd
- endringer i sikkerhetsarbeidet vurderes for å hindre framtidige sikkerhetsbrudd
- Datatilsynet varsles ved uautorisert utlevering av *helse- og personopplysninger*

Avviksskjema (se eksempel nedenfor) skal fylles ut av den som oppdager *avviket* og sende det til *databehandlingsansvarlig.*

Informasjon	**Fyll ut for avviket**	**Kommentar**
Avvik registrert av:		Hvem som registrerer avviket – inkl. kontaktinformasjon
Tidspunkt:		Når avviket inntraff
Hendelse:		Beskrivelse av avviket
Strakstiltak:		Eventuelle strakstiltak som er innført
Korrigerende tiltak:		Hvilke korrigerende tiltak som er besluttet innført
Evaluering av tiltak:		Hvem som er ansvarlig for å evaluere tiltakene, og når
Varsling:		Hvem som er varslet om avviket (hvis avviket innebærer uautorisert tilgang til helse- og personopplysninger skal Datatilsynet varsles)

Krav til avviksbehandling er omtalt nærmere i Faktaark 8 – Avviksbehandling på www.normen.no.

2.3.5 Ledelsens gjennomgang

Databehandlingsansvarlig (ledelsen) skal jevnlig, og minimum årlig, gjennomgå sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene i *virksomheten.* Dette skal kontrolleres opp mot *virksomhetens* behov og eventuelt oppdatere sikkerhetsmål, sikkerhetsstrategi og organisering.

Det anbefales at sikkerhetsrevisjoner gjennomføres forut for ledelsens gjennomgang. Dette begrunnes med at eventuelle kostnader til tiltak kan besluttes på ledelsens gjennomgang.

Tabellen under gir en sjekkliste for gjennomføring av ledelsens gjennomgang.

Hva	**Hvordan**
Når	• En gang pr år som en fast ordning • Om det oppstår vesentlige sikkerhetsbrudd
Vurderinger	Følgende skal som minimum gjennomgås: • Resultat fra sikkerhetsrevisjoner • Resultat fra risikovurderinger • Resultater fra avviksbehandling. *Virksomhetens* ledelse skal regelmessig følge opp at tiltak på grunnlag av avvik planlegges og gjennomføres • Ansvarsforhold og organisering mht. sikkerhet • Formål med *behandling* av *helse- og personopplysninger* og oversikt over *helse- og personopplysninger* som behandles i virksomheten • Konfigurasjonskart over informasjonssystemene. • Sikkerhetsmål, nivå for akseptabel risiko og strategier for informasjonssikkerhet

Hva	Hvordan
Tiltak	Dersom gjennomgangen avdekker at virkelig situasjon ikke oppfyller fastsatt nivå for akseptabel risiko skal: • Det vedtas tiltaksplaner for å oppnå fastsatt nivå for akseptabel risiko, med plassering av ansvar
Dokumentasjon	Resultat fra ledelsens gjennomgang skal dokumenters og oppbevares i virksomheten i minst 5 år

3 OPPGAVER SOM HELT ELLER DELVIS KAN IVARETAS AV DATABEHANDLER

Mens kapittel 2beskriver oppgavene som påligger *databehandlingsansvarlig*, tar dette kapitlet for seg oppgavene som helt eller delvis kan ivaretas av en *databehandler*. Dersom oppgavene skal ivaretas av *databehandlingsansvarlig* kommer disse i tillegg til oppgavene beskrevet i kapittel 2.Ivaretas oppgavene av en *databehandler*, er det fortsatt *databehandlingsansvarlig* som har ansvaret for at oppgavene beskrevet under blir ivaretatt. Ansvaret til *databehandler* reguleres i en databehandleravtale.

Databehandler har ansvaret for at det foreligger nødvendige prosedyrer og oversikt over systemet for å ivareta nivå for *akseptabel risiko* som *databehandlingsansvarlig* har fastsatt.

Eksempel på ivaretakelse av oppgavene ved bruk av *databehandler*:

Kapittel	Databehandlings-ansvarlig	Databehandler
3.1 Fysisk sikring av områder og utstyr	- Kontorsikring - PC, skriver - Medisinsk teknisk utstyr	- Servere - Nettverksutstyr

3.2 Sikkerhet i nettverk, datautstyr og tekniske løsning	- Kontroll med eget utstyr
	- Tilkobling av utstyr (PC, skriver, ruter) på klinikken til *helsenettet*
	- Antivirusløsning på eget utstyr
	- Utfasing av eget datautstyr
		- Drift av
		  o Servere
		  o Nettverksutstyr
		  o EPJ-system
		- Dokumentasjon
		- Konfigurasjonsendringer
		- Tilkobling av teknisk løsning til*helsenettet*
		- Sikkerhetskopiering
		- Antivirusløsning
		- Utfasing av datautstyr

3.3 Hendelsesregistrering		- All hendelses-registrering
3.4 Hjemmekontor og mobilt utstyr	- Sikring av eget utstyr	- Teknisk løsning
3.5 Elektronisk kommunikasjon som e-post og SMS	- Regler for bruk	

3.1 Fysisk sikring av områder og utstyr

Det er viktig at *virksomheten* sikrer både sitt fysiske område (kontorer, arkivrom, behandlingsrom, mv.) og utstyret som inneholder *helse- og personopplysninger* (hver enkelt PC, fotoutstyr, mv. med *helse- og personopplysninger* mv.). Sikringen har som formål å hindre at uautoriserte får adgang til utstyret.

Konkret bør *virksomheten* utarbeide prosedyrer for sikring av kontordører/-vinduer (låsing, alarmsystem), resepsjonsområde, PC, skriver, telefaks, kopimaskin, bærbare PC mv. *Virksomheten* skal sikre at utskrift ikke kommer på avveie. Dokumenter som inneholder

helse- og personopplysninger, og som ikke skal tas vare på, skal slettes fullstendig, helst ved makulering.

Eksempler på sikring av områder og utstyr er:

- skriver og arbeidsstasjoner som er plassert i tilknytning til fellesområder (resepsjoner, venterom, vaktrom, korridorer og lignende) sikres slik at uvedkommende ikke får adgang til *helse- og personopplysninger*
- servere og annet nettverksutstyr skal oppbevares i låst skap eller rom. Dersom det benyttes et skap, skal dette skrus fast til veggen eller gulvet. Skapet skal ikke plasseres i resepsjonen/publikumsområde. Resepsjon/publikumsområde skal heller ikke benyttes som rom for oppbevaring avutstyret
- medisinsk teknisk utstyr som *behandlerhelse- og personopplysninger* skal inkluderes i arbeidet med informasjonssikkerhet, herunder risikovurderinger, adgangsregulering, fysisk sikring og prosedyrer for bruk

Databehandler kan finne mer informasjon i Faktaark 17 - Fysisk sikring av områder og utstyr på www.normen.no.

3.2 Sikkerhet i nettverk, datautstyr og tekniske løsning

Innholdet i dette kapittelet er omfattende og komplisert og det kan være nødvendig for *databehandlingsansvarlig* å søke bistand.

Konfigurasjonskontroll

Med konfigurasjonskontroll menes at *databehandlingsansvarlig* har oversikt over alt utstyr og programvare som benyttes i *behandlingen* av *helse- og personopplysninger*. Konfigurasjonskontroll omfatter i denne sammenheng maskinvare (for eksempel PC og server), programvare (for eksempel operativsystem og *EPJ-system*) og nettverket (for eksempel trådløst nettverk ved klinikken).

Figurene i kapittel 1.1 viser ulike løsninger for drift av EPJ:

- **Skisse 1 – *EPJ* på eget utstyr** som ikke er knyttet til Internett eller ekstern e-post er konfigurasjonskontrollen enkel. Skal *virksomheten* knytte egen teknisk løsning til Internett og benytte e-post må det etableres tekniske sikkerhetstiltak. Det anbefales å benytte bistand til dette arbeidet. *Virksomheten* må ha konfigurasjonskontroll for hele løsningen
- **Skisse 2 – *EPJ* på eget utstyr og tilknyttet *helsenett*** har klinikken en teknisk løsning som oppfyller kravene til sikkerhet og konfigurasjonskontrollen skal kun dekke egen løsning
- **Skisse 3 – EPJ hos *databehandler*** vil *databehandler* ivareta konfigurasjonskontroll for drift av server og *EPJ-systemet*. *Virksomheten* må ha konfigurasjonskontroll for egen løsning (PC, skriver, ruter)

Databehandlingsansvarlig skal sørge for at den tekniske løsningen (*konfigurasjonen*) er dokumentert med et konfigurasjonskart (teknisk tegning)og tekstlig beskrivelse av sikkerhetstiltakene. Ved bruk av *databehandler* skal denne ivareta dette. Dokumentasjonen skal inneholde:

- sikkerhetsbarrierer (for eksempel brannmur)

- hvor eventuelle servere er plassert
- hvor *EPJ-systemet* er plassert
- plassering av arbeidsstasjoner og skrivere
- plassering av betalingsterminal(er)
- internettilknytning (inklusive at gjeldende sikkerhetskrav ivaretas)
- eventuell tilknytning til *helsenettet*
- kryptering av ekstern kommunikasjon (krypteringsstyrke skal minimum oppfylle Kravspesifikasjon for PKI i offentlig sektor, eller tilsvarende styrke, se https://www.regjeringen.no/nb/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/

Databehandlingsansvarlig er videre ansvarlig for at *konfigurasjonsendringer*, dvs. endringer i utstyr og/eller programvare, ikke settes i drift før følgende tiltak er gjennomført:

- risikovurdering som viser at nivå for *akseptabel risiko*er oppfylt
- test som sikrer at forventede funksjoner er ivaretatt
- implementering som sikrer mot uforutsette hendelser
- ny *konfigurasjon* er dokumentert
- *konfigurasjonsendringer* er godkjent av *virksomhetens* leder eller den ledelsen bemyndiger. Godkjennelse kan overlates til *databehandler* iht. avtale

Ansvaret for *konfigurasjonsendringer* kan ivaretas av *databehandler*.

Tekniske løsninger for ekstern datakommunikasjon og kobling til helsenett

Tilkobling til eksterne datanettverk skal sikres med to uavhengige *tekniske tiltak* i forhold til nettverk der det *behandles helse- og personopplysninger*.

For utdypning skal *databehandler* gjøre seg kjent med informasjon i Faktaark 28 - Alternative tekniske løsninger for primærhelsetjenester på www.normen.no.

Sikkerhetskopiering

Databehandlingsansvarlig skal påse at *helse- og personopplysninger* sikkerhetskopieres etter en fastsatt prosedyre. I tillegg skal oppsett av *EPJ-systemet*, servere mv. sikkerhetskopieres jevnlig slik at hele informasjonssystemet kan tilbakekopieres. *Databehandlingsansvarlig* skal sikre at sikkerhetskopiene oppbevares avlåst og brannsikret, og adskilt fra driftsutstyret som er sikkerhetskopiert. Det skal jevnlig foretas test av at sikkerhetskopiene er korrekte og kan tilbakeføres.

For utdypning skal *databehandler* gjøre seg kjent med informasjon i Faktaark 21 - Sikkerhetskopi (backup) på www.normen.no.

Beskyttelse mot ondsinnet programvare

Databehandlingsansvarlig skal sørge for at datamaskinene i *virksomheten* har installert en løsning for å hindre ondsinnet programvare (antivirusløsning).

Databehandlingsansvarlig skal sørge for at programvaren er installert slik at den automatisk henter ned og installerer oppdateringer. Dette forutsetter en sikker internettilknytning. Oppdateringer skal hentes inn til *sikker sone*. Om *virksomheten* ikke har internettilknytning til

hele eller deler av sin tekniske løsning, må oppdateringer installeres i henhold til spesifikasjoner fra *leverandøren*.

Databehandler er også ansvarlig for å gjøre seg kjent med informasjon i Faktaark 19 - Tiltak for å hindre ondsinnet programvare på www.normen.no.

Utfasing av utstyr

Ved utfasing av utstyr (for eksempel kopimaskin, telefaks, multifunksjonsskriver, PC, server mv.) skal *databehandlingsansvarlig* påse at *helse- og personopplysninger* slettes slik at opplysningene ikke kan gjenskapes.

Vanlig sletting av datafiler og formattering er ikke tilstrekkelig. Et godkjent sletteprogram skal benyttes, alternativt kan lagringsmediene ødelegges fysisk.

Det anbefales at *virksomheten* inngår en avtale med en *leverandør* som påtar seg oppdrag med sikker sletting. I slike tilfeller skal det undertegnes en databehandleravtale mellom *virksomheten* og *leverandøren*.

Se Faktaark 34 - Håndtering av lagringsmedia på www.normen.no.

3.3 Hendelsesregistrering

Databehandlingsansvarlig skal påse at *databehandler* har etablert *hendelsesregistreing* og prosedyrer for kontroll av *hendelsesregistre. Hendelsesregistre* er den viktigste kilden til at *avvik* oppdages. Følgende hendelser skal som et minimum registreres: – tildeling av *autorisasjoner* – *autorisert* bruk av *EPJ-systemet* – forsøk på uautorisert bruk av *EPJ-systemet* – bruk av *nødrettstilgang* (blålysfunksjon)

Uautorisert eller forsøk på uautorisert bruk skal også meldes umiddelbart som *avvik* til *databehandlingsansvarlig*.

Det skal være enighet mellom *databehandlingsansvarlig* og *databehandler* for hvordan *hendelsesregistrene* skal analyseres slik at hendelser oppdages før de får alvorlige konsekvenser. *Hendelsesregistre* skal analyseres fortrinnsvis innen 1 uke.

Hendelsesregistret skal oppbevares til det av hensyn til formålets karakter ikke lenger antas å bli bruk for dem.

Databehandler er også ansvarlig for å gjøre seg kjent med informasjon i Faktaark 15 - Hendelsesregistrering og oppfølging på www.normen.no.

3.4 Hjemmekontor og mobilt utstyr

Med *hjemmekontor* menes tekniske løsninger som er *virksomhetens* eiendom og som skal benyttes til arbeidsoppgaver knyttet til *virksomheten*. *Virksomheten* må etablere en sikker teknisk løsning og prosedyrer for bruk av denne.

Med mobilt utstyr kommer problemstillinger knyttet til at enhetene kan bli stjålet eller gjenglemt. Eksempler på mobilt utstyr er PC, PDA, mobiltelefoner mv. Om det lagres *helse- og personopplysninger* på det mobile utstyret skal data krypteres med krypteringsstyrke iht kravspesifikasjon for PKI i offentlig sektor, eller tilsvarende styrke, se https://www.regjeringen.no/nb/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/

Det mobile utstyret skal sikres med *autentisering* (for eksempel passord) for å hindreuautorisert tilgang mv. på samme måte som stasjonært utstyr på klinikken.

Databehandler er ansvarlig for å gjøre seg kjent med informasjon i Faktaark 18 - Sikring av bærbart utstyr,Faktaark 29 - Hjemmekontor og Faktaark 30 - Sikring av mobilt utstyr utenfor hjemmet på www.normen.no.

3.5 Elektronisk kommunikasjon som e-post og SMS

Virksomheten skal ikke bruke SMS eller e-post til overføring av *helseopplysinger* eller 11-siffret fødselsnummer.

For hva SMS og e-post kan bruks til, se ”Personvern og informasjonssikkerhet i kontakten med pasient/bruker, En veileder i bruk av portalløsninger, SMS og e-post” på www.normen.no.

4 VEDLEGG

4.1 Oversikt over sentrale lover

Dette kapitlet gir en oversikt over de mest sentrale lovene som gjelder personvern og informasjonssikkerhet, men er ikke en uttømmende liste. *Databehandlingsansvarlig* skal ha oversikt over lover som er relevante for *virksomhetens* aktiviteter.

4.1.1 Personopplysningsloven

Personvern handler om retten til å ha et privatliv, og at den enkelte skal kunne ha kontroll over og i størst mulig grad kunne bestemme over egne opplysninger. Personopplysningsloven er den generelle loven som skal beskytte den enkeltes personvern, og gir grunnleggende regler og definisjoner innen personvern og informasjonssikkerhet. *Normen* bygger bl.a. på reglene i personopplysningsloven. Definisjoner brukt i denne veilederen er i stor grad hentet fra personopplysningsloven . Personopplysningsloven gir blant annet detaljerte føringer for sikring av informasjonssikkerhet (jf. kapittel 2) og gjennomføring av *internkontroll* (jf. kapittel 3).

Databehandlingsansvarlig skal sørge for at *personopplysningene* som *behandles* bare *behandles* når dette er tillatt etter personopplysningslovens § 8 og § 9, bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den *databehandlingsansvarliges virksomhet*.

Databehandlingsansvarlig skal ikke bruke *personopplysningene* senere til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at *pasienten* samtykker.

Databehandlingsansvarlig skal sørge for at *personopplysninger* er tilstrekkelige og relevante for formålet med *behandlingen*. Videre skal *databehandlingsansvarlig* sørge for at *personopplysninger* er korrekte og oppdatert, og ikke lagres lenger enn det som er nødvendig ut fra formålet med *behandlingen*, jf. personopplysningsloven §§ 27 og 28.

V*irksomheten* har*meldeplikt* til Datatilsynet for sine *behandlinger* av *helse- og personopplysninger*. *Meldeplikten* gjennomføres ved å fylle ut og sende elektronisk skjema "Melding om behandling av personopplysninger" på www.datatilsynet.no. Meldingen skal fornyes hvert tredje år.

4.1.2 Pasientjournalloven

Pasientjournalloven gir sentrale definisjoner. De viktigste er gjengitt i kapittel 1.5.

Etter pasientjournalloven § 9 åpnes det opp for at to eller flere virksomheter kan samarbeide om behandlingsrettede helseregistre.
I praksis innebærer det at hver pasient har én journal innen samarbeidet, og at helsepersonellet tilknyttet fellesskapet fører opplysninger i denne journalen. Én felles journal vil gjøre det lettere å se de ulike tiltakene i sammenheng og vurdere helheten i pasientbehandlingen. Det vil kunne gi en bedre pasientsikkerhet at journalføringen skjer i samme journal.

Bestemmelsen gjelder fagsystemer og andre journaler hvor helsepersonell som yter helsehjelp nedtegner eller registrerer opplysningene om pasientene i samsvar med dokumentasjonsplikten.

Det er viktig å merke seg at en etablering av felles journal vil erstatte den virksomhetsinterne journalen,

Loven åpner også for at to eller flere virksomheter kan inngå avtale om tilgang til helseopplysninger på tvers av virksomhetsgrenser. Lovens § 19 er den databehandlingansvarlig pliktig til å sørge for at relevante og nødvendige opplysninger er tilgjengelig for helsepersonell og annet samarbeidende personell, innenfor rammen av taushetsplikt og det som er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp for den enkelte. Det er den databehandlingsansvarlige som bestemmer på hvilken måte opplysningene skal gjøres tilgjengelig ihht krav til tilfredsstillende informasjonssikkerhet, og dette gjelder både internt i virksomheten og tilgjengeliggjøring av opplysningene for personell fra andre virksomheter.

Pasientjournalloven og helsepersonelloven slår blant annet fast forbudet mot snoking i pasientjournaler uten at det er begrunnet i helsehjelp til pasienten, administrasjon av helsehjelp, internkontroll, kvalitetssikringen av helsehjelpen eller har særskilt hjemmel i lov.

Forholdet mellom personopplysningsloven og helseregisterloven

Personopplysningsloven med forskrifter gjelder som utfyllende bestemmelser på områder helseregisterloven ikke har egne bestemmelser.

4.1.3 Helsepersonelloven

Helsepersonelloven skal bidra til sikkerhet for *pasienter* og kvalitet i helsetjenesten samt tillit til helsepersonell og helsetjeneste. Etter helsepersonelloven § 48 er psykolog, fysioterapeut og kiropraktor helsepersonell. Den som yter helsehjelp har plikt til å føre journal (§ 39).

Helsepersonelloven gir regler om *taushetsplikt*. Helsepersonell har som hovedregel *taushetsplikt* om pasientforhold (jf. § 21). *Taushetsplikten* hindrer ikke at opplysninger gis til samarbeidende personell når det er nødvendig for å kunne gi forsvarlig helsehjelp. Dette er vanlig i den kliniske hverdagen for psykologer, fysioterapeuter, manuellterapeuter og kiropraktorer. Imidlertid har pasienten reservasjonsrett, dvs. rett til å motsette seg at opplysninger gis til samarbeidende personell (jf. § 25).

Loven åpner for at personell som bistår med elektronisk bearbeiding av opplysningene, eller som bistår med service og vedlikehold av utstyr, kan få *tilgang* til opplysninger som er taushetsbelagte. Dette gjelder når slik bistand er nødvendig for å oppfylle lovbestemte krav til dokumentasjon, dvs. nødvendig for å oppfylle journalføringsplikten. Slikt personell har *taushetsplikt* på lik linje med helsepersonell som yter helsehjelp.

Virksomheten kan derfor benytte seg av ulike grupper *leverandører* uten at *taushetsplikten* er til hinder for det. Journalopplysninger kan lagres hos en *databehandler* og servicepersonell kan bistå ved håndteringen av informasjonssikkerheten i pasientregistre mv. Når *virksomheten* gir servicepersonell mv. *tilgang* til informasjonssystemet, må den sørge for at personellet undertegner taushetserklæring.

Helsepersonelloven sier at en *virksomhet* som yter helsehjelp skal organiseres slik at helsepersonellet blir i stand til å overholde sine lovpålagte plikter (jf. § 16). God organisering av arbeidet med informasjonssikkerhet er derfor en plikt *virksomheten* har etter helsepersonelloven.

4.1.4 Pasient- og brukerrettighetsloven

Pasient- og brukerrettighetsloven skal bidra til å sikre at *pasienter* får tilgang på helsehjelp av god *kvalitet*. Loven skal også bidra til å fremme tillitsforholdet mellom *pasient* og helsetjeneste og ivareta respekten for den enkelte *pasients* liv, menneskeverd og *integritet*.

Pasient- og brukerrettighetsloven § 3-6 sier at opplysninger om sykdomsforhold, og andre personlige opplysninger, skal *behandles* i samsvar med *taushetsplikten*. Loven sier også at *helse- og personopplysninger* skal *behandles* med varsomhet og respekt for *integriteten* til den opplysningene gjelder. Gode informasjonssikkerhetsprosedyrer bidrar til etterlevelse av dette.

Den som har krav på taushet kan samtykke i at *helse- og personopplysninger* gis videre, og *taushetsplikten* faller da bort så langt samtykket dekker. Pasienten har også rett til å motsette seg utlevering og overføring av journalopplysninger (jf. § 5-3). Pasient- og brukerrettighetsloven slår fast at *pasienten* som hovedregel har rett til innsyn i sin egen journal (jf. § 5-1).

4.1.5 Barnevernloven

Barnevernloven sikrer at barn og unge som lever under forhold som kan skade deres helse og utvikling, får nødvendig hjelp og omsorg til rett tid, og videre bidrar til at barn og unge får trygge oppvekstvilkår.

Databehandlingsansvarlig skal se til at enhver som utfører tjeneste eller arbeid med mindreårige har *taushetsplikt* etter forvaltningsloven §§ 13 til 13 e (jf. barnevernloven § 6-7). *Taushetsplikten* gjelder alle *personopplysninger*, også opplysninger om fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted. Likevel kan yrkesutøvere i medhold av helsepersonelloven gis opplysninger når dette er nødvendig for å fremme bestemte institusjoners oppgaver, eller for å forebygge vesentlig fare for liv eller alvorlig skade for noens helse.

4.1.6 Psykisk helsevernloven(jf. psykologspesialist med vedtakskompetanse)

Psykisk helsevernloven sikrer at etablering og gjennomføring av psykisk helsevern skjer på en forsvarlig måte og i samsvar med grunnleggende rettssikkerhetsprinsipper. Formålet er videre å sikre at de tiltakene som er beskrevet i loven, tar utgangspunkt i pasientens behov og respekt for menneskeverdet.

Databehandlingsansvarlig skal sikre (jf. § 5-6a) at den faglig ansvarlige, uten hinder av lovbestemt *taushetsplikt*, gir påtalemyndigheten og retten de opplysninger som er nødvendig for å vurdere om tvungent psykisk helsevern skal opprettholdes, jf. straffeloven § 39 b. *Databehandlingsansvarlige* skal informere den domfelte, om mulig på forhånd, om hvilke opplysninger som gis.

Databehandlingsansvarlig skal sikre (jf. § 5-6a) at den faglig ansvarlige og påtalemyndigheten, uten hinder av *taushetsplikt*, gir koordineringsenheten opplysninger som skal registreres i henhold til psykisk helsevernloven § 5-2b. *Databehandlingsansvarlig* skal informere den tiltalte eller domfelte, om mulig på forhånd, om hvilke opplysninger som gis.

4.2 Definisjoner

Definisjoner er hentet fra *Normen*. Nye begrep er definert og samlet etter definisjoner fra *Normen*. Definerte ord er markert i *kursiv* i teksten.

Definisjoner fra *Normen* (Februar 2015)

-A-

Med "***akseptabel risiko***" menes i *Normen* hvor stor risiko *sektoren* kan akseptere for at det inntreffer en hendelse som kan forårsake brudd på *konfidensialitet*, *tilgjengelighet*, *integritet* eller *kvalitet* for *helse- og personopplysninger*. Risikoens størrelse avhenger av hvor stor sannsynlighet det er for at hendelsen skal inntreffe og av konsekvensen av en slik hendelse. *Normen* beskriver et nivå for *akseptabel risiko* i *sektoren*. Hver enkelt *virksomhet* må foreta en konkret vurdering av hvordan *akseptabel risiko* for vedkommende *virksomhet* skal oppnås.

Med "***autentisering***" menes i *Normen* prosessen som gjennomføres for å bekrefte en påstått identitet.

Med "***autorisere/autorisert/autorisasjon***" menes i *Normen* at en person i en bestemt rolle kan gis eller er gitt bestemte rettigheter til lesing, registrering, redigering, retting, sletting og/eller sperring av *helse- og personopplysninger*. *Autorisasjon* kan bare gis i den grad det er nødvendig for vedkommendes arbeid, er begrunnet ut fra *tjenstlig behov* og er i henhold til bestemmelser om *taushetsplikt*.

Med "***autorisasjonsregister***" menes i *Normen* et *register* over utstedte *autorisasjoner* som føres av den *databehandlingsansvarlige.*

Med "***avvik***" menes i *Normen* enhver håndtering av *helse- og personopplysninger* som ikke utføres i henhold til gjeldende regelverk, retningslinjer og/eller prosedyrer samt andre sikkerhetsbrudd.

-B-

Med "***behandling***" menes i *Normen* enhver formålsbestemt bruk av *helse- og personopplysninger*, som f.eks. innsamling, registrering, sammenstilling, lagring ogutlevering eller en kombinasjon av slike bruksmåter, jf. helseregisterloven § 2 c), pasientjournalloven § 2 b) og personopplysningsloven § 2 nr. 2).

Med "***behandlingsrettet helseregister***" menes i *Normen* journal- og informasjonssystem eller annet *helseregister* som har til formål å gi grunnlag for handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende mål i forhold til den enkelte *pasient* og som utføres av helsepersonell, samt administrasjon av slike handlinger, jf. helseregisterloven § 2 nr. 7. Se også *elektronisk pasientjournal (EPJ)* og *tjenestedokumentasjon*.

Med "***bruker***" menes i *Normen* en person som anmoder om eller mottar tjenester omfattet av helse- og omsorgstjenesteloven som ikke er helsehjelp, jf. pasient- og brukerrettighetsloven § 1-3 bokstav f.

-D-

Med "***databehandler***" menes den som *behandler helse- og personopplysninger* på vegne av den *databehandlingsansvarlige*, jf. personopplysningsloven § 2 nr. 5. Det presiseres at en *databehandler* er en ekstern person eller *virksomhet* utenfor den *databehandlingsansvarliges virksomhet*. Det vil si at den *databehandlingsansvarliges* egne medarbeidere ikke er dennes *databehandlere*.

Med "***databehandlingsansvarlig***" menes den som bestemmer formålet med *behandlingen* og hvilke hjelpemidler som skal brukes, hvis ikke *databehandlingsansvaret* er særskilt angitt i loven eller i forskrift i medhold av loven, jf. helseregisterloven § 2 e), pasientjournalloven § 2 e) og personopplysningsloven § 2 nr. 4 (her benyttes begrepet "behandlingsansvarlig"). Det presiseres at det er *virksomheten* som er *databehandlingsansvarlig* for *behandling* av *helse- og personopplysninger.* Ansvaret skal ivaretas av den daglige ledelsen av *virksomheten,* og *virksomheten* er pliktsubjekt.

-E-

Med "***elektronisk pasientjournal (EPJ)***" menes i *Normen* elektronisk ført samling eller sammenstilling av nedtegnede/registrerte opplysninger om en *pasient* i forbindelse med helsehjelp, se også helsepersonelloven § 40 første ledd og forskrift om pasientjournal § 3 a. Dette inkluderer både somatisk og psykiatrisk journal o.a., hver for seg eller samlet. Se også *behandlingsrettet helseregister.*

Med "***elektronisk pasientjournalsystem (EPJ-system)***" menes i *Normen* elektroniske systemer med nødvendig funksjonalitet for å registrere, søke frem, presentere, kommunisere, redigere, rette og slette opplysninger i *elektronisk pasientjournal (EPJ).* Dette inkluderer både radiologisystemer, systemer for somatisk og psykiatrisk journal, pasientadministrative systemer og andre systemer som inneholder *helseopplysninger.*

-F-

Med "***fagsystem***" menes i *Normen* en applikasjon eller et IT-system som *behandler helse- og personopplysninger*. Begrepet systemløsning brukes også om et *fagsystem*. Eksempler på *fagsystem* er: pleie- og omsorgsystem (PLO), legekontorsystem og barnevernsystem. Opplysninger i ulike *fagsystemer* kan både utgjøre *elektronisk pasientjournal (EPJ)* og annen *tjenestedokumentasjon*.

Med "***fjernaksess***" menes i dette dokumentet ekstern *tilgang* fra *leverandør* til helsevirksomhet via kommunikasjonslinje for å utføre vedlikehold og oppdateringer av IT-løsninger.

Med "***formalisert arbeidsfellesskap"*** menes i *Normen* samarbeid mellom to eller flere *virksomheter* som tydelig fremstår som en enhet. En *kommune* som inngår avtale med andre offentlige eller private tjenesteytere etter helse- og omsorgstjenesteloven § 3-1 femte ledd for å yte helhetlige helse- og omsorgstjenester anses som *formalisert arbeidsfellesskap.*

-H-

*"**helse- og personopplysninger**"* benyttes i *Normen* som en fellesbetegnelse for *helseopplysninger* og/eller *personopplysninger* innenfor *Normens* virkeområde.

Med "***helsenettet***" menes i *Normen* nettverket som tilbys av Norsk Helsenett SF.

Med "***helseopplysninger***" menes i *Normen* taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en enkeltperson, jf. helseregisterloven § 2 nr. 1.

Med "***helseregister***" menes i *Normen* registre, fortegnelser, m.v. der *helseopplysninger* er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen, jf. helseregisterloven § 2 nr 6.

Med "***hendelsesregister***" menes i *Normen* et logisk *register* der hendelser i informasjonssystemet er nedtegnet, se neste definisjon.

Med "***hendelsesregistrering***" menes i *Normen* registrering av hendelser i et informasjonssystem, bl.a. med sikte på å forebygge, avdekke og hindre gjentagelse av sikkerhetsbrudd.

Med "***hjemmekontor***" menes i *Normen behandling* av *helse- og personopplysninger* på PC som *virksomheten* har stilt til disposisjon, fra f.eks. hjem, hytte, hotellrom eller lignende. Bruk av PC som *virksomheten* ikke har stilt til disposisjon (for eksempel PC på Internettkafé, hotell-PC, flyplass-PC) er ikke definert som *hjemmekontor*.

-I-

Med "***integritet***" menes i *normen* at *helse- og personopplysninger* må være sikret mot utilsiktet eller uautorisert endring eller sletting og være korrekte, oppdaterte, relevante og tilstrekkelige som grunnlag for å yte helsehjelp.

Med *"**internkontroll**"* menes i *Normen* planlagte og systematiske tiltak som skal sikre at *virksomhetens* aktiviteter planlegges, organiseres, utføres og vedlikeholdes i samsvar med krav fastsatt i eller i medhold av lovgivningen.

-K-

Med "***kommune***" menes i *Normen* en juridisk enhet som *kommune* og fylkeskommune.

Med "***konfidensialitet***" menes i *normen* at *helse- og personopplysninger* må være sikret mot at uvedkommende får kjennskap til opplysningene.

Med "***konfigurasjon***" menes i *Normen* informasjonssystemets utforming inklusive både teknisk utstyr og programvare.

Med "***konfigurasjonsendring***" menes i *Normen* en endring av informasjonssystemets utforming som følge av installasjon, oppgradering eller fjerning av utstyr eller programvare.

-L-

Med "***leverandør***" menes i *Normen* juridisk enhet som yter tekniske og/eller administrative tjenester til *virksomheten*. Eksempler er EPJ-leverandør, røntgenleverandør, *leverandør* av løsning for SMS-meldinger, IKT-leverandør mv.

-M-

Med "***meldeplikt***" menes i *Normen* plikten den enkelte *databehandlingsansvarlige* har til å melde om *behandling* av *helse- og personopplysninger* til Datatilsynet. *Meldeplikten* følger av personopplysningsloven § 31.

-N-

Med "***Norm/Normen***" menes dette dokumentet. Andre dokumenter i tilknytning til *Normen*, som for eksempel faktaark og veiledninger, er ikke omfattet av begrepet.

Med "***Norsk Helsenett***" menes i *Normen* Norsk Helsenett SF.

Med "***nødrettstilgang***" menes i *Normen* en *tilgang* hvor prinsippene for tilgangsstyring ikke blir fulgt, fordi det for å avverge fare eller skade er behov for øyeblikkelig *tilgang* til *helse-ogpersonopplysninger*, og dette ut fra de foreliggende omstendigheter må vurderes som rettmessig.

-P-

Med "***pasient***" menes i *Normen* en person som henvender seg til helse- og omsorgstjenesten med anmodning om helsehjelp, eller som helse- og omsorgstjenesten gir eller tilbyr helsehjelp i det enkelte tilfelle, jf. pasient- og brukerrettighetsloven § 1-3 bokstav a.

"***pasientopplysninger***", se *helse- og personopplysninger.*

Med "***personlig kvalifisert sertifikat***" menes i *Normen* to-faktor autentisering hvor en faktor er dynamisk basert på kvalifiserte sertifikater og ellers tilfredsstiller kravene til sikkerhetsnivå 4 i "Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor".

Med "***personopplysninger***" menes i *Normen* opplysninger og vurderinger som kan knyttes til en enkeltperson, jf. personopplysningsloven § 2 nr. 1).

Med "***PKI/Public Key Infrastructure***" menes en teknologi for utstedelse, administrasjon og bruk av digitale sertifikater over datanett. Anvendelsesområder for *PKI* er *autentisering* (legitimering av en person, organisasjon eller gjenstands identitet), digital signatur (av dokumenter eller programvare) og verifisering av dataintegritet.

-R-

Med "***register***" menes i *Normen* en logisk sammenstilling av opplysninger. En database eller et regneark er en teknisk løsning for et *register*.

Med "***registrert/den registrerte***" menes i *Normen* den som opplysninger kan knyttes til, jf. personopplysningsloven § 2 nr. 6. Eksempler og begreper som brukes om *den registrerte* er søker, *pasient/bruker* og tjenestemottaker. En ansatt kan være omfattet av begrepet.

-S-

Med "***sektor/sektoren***" menes i *Normen* helse-, omsorgs-, og sosialsektoren eller en eller deler av de nevnte.

Med "***sensitive personopplysninger***" menes i *Normen* opplysninger om:
a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning
b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
c) helseforhold (*helseopplysninger)*
d) seksuelle forhold
e) medlemskap i fagforeninger,

jf. personopplysningsloven § 2 nr. 8).

Med "***sikker sone***" menes en avgrenset del av *virksomhetens* informasjonssystem, der det bl.a. *behandles helse- og personopplysninger* og hvor kun *autoriserte* brukere gis *tilgang.*

-T-

Med "***taushetsplikt***" menes i *Normen* lovpålagt eller avtalt plikt til å hindre at andre får adgang eller kjennskap til *helse- og personopplysninger*, jf. helsepersonelloven § 21, helseregisterloven § 17, pasientjournalloven § 15, helse- og omsorgstjenesteloven § 12-1, spesialisthelsetjenesteloven § 6-1ogforvaltningsloven §§ 13 til 13e, samt annen informasjon med betydning for informasjonssikkerheten, jf. personopplysningsforskriften § 2-9. *Taushetsplikt* innbefatter både en passivplikt til å tie og en plikt til aktivt å hindre uvedkommende i å få kunnskap om taushetsbelagte opplysninger.

Med "***tekniske tiltak***" menes i *Normen* tiltak av teknisk karakter som ikke kan påvirkes eller omgås av medarbeidere, og ikke er begrenset av handlinger som den enkelte forutsettes å utføre. Eksempler på slike tiltak kan være *autentisering* ved *personlig kvalifisert sertifikat* eller *konfigurering* av en brannmur slik at den kun tillater bestemt trafikk eller en meldingstjeneste som er laget slik at alle meldinger automatisk blir kryptert.

Med "***tilgang***" menes i *Normen* at *helse- og personopplysninger* om en eller flere bestemte *pasienter/brukere* er eller gjøres tilgjengelige for *autorisert* personell. Beslutning om *tilgang* til *behandlingsrettede helseregistre* skal treffes etter en konkret vurdering basert på at det ytes helsehjelp til *pasienten. Tilgang* til *fagsystemer* i forbindelse med ytelser til *pasient/bruker* skal iverksettes basert på *tjenstlig behov*. *Tilgang* i forbindelse med kvalitetssikring og administrative oppgaver skal også besluttes ut fra *tjenstlig behov*.

Med "***tilgjengelighet***" menes i *normen* at *helse- og personopplysninger* som skal *behandles*, er tilgjengelig til den tid og på det sted det er behov for opplysningene.

Med "***tjenstlig behov***" menes i *Normen* at personer med nærmere bestemte arbeidsoppgaver, trenger nødvendige *helse- og personopplysninger* for å yte helsehjelp, omsorgs- eller sosialtjeneste og/eller utføre administrasjon i forbindelse med dette. Dersom *pasienten* har

sperret hele eller deler av *helse- og personopplysningene* kreves særskilt hjemmel for *tilgang* til disse.

Med "***tjenestedokumentasjon***" menes i *Normen* dokumentasjon for planlegging, kartlegging, oppfølging og informasjonsutveksling som vedrører tjenestemottakerens søknad, praktiske og medisinske problemer, behov, ressurser, tiltak i form av helsehjelp, hjelpemidler, mm. Sammen med *elektronisk pasientjournal (EPJ)* vil *tjenestedokumentasjonen* utgjøre dokumentasjonsplikten etter helsepersonelloven mv. Det er ingen lovfestet dokumentasjonsplikt etter sosialtjenesteloven.

-V-

Med "***virksomhet***" menes i *Normen* juridisk enhet som helseforetak, *kommune*, sykehus, legepraksis, tannklinikk, apotek, apotekkjede, røntgeninstitutt, frittstående laboratorium, universitet, høyskole, stiftelse m.v.

Med "***virksomhetsovergripende pasientjournal***" menes i *Normen behandlingsrettet helseregister* i *formalisert arbeidsfellesskap* hvor helsepersonell, og personell som yter helse- og omsorgstjenester etter helse- og omsorgstjenesteloven, nedtegner eller registrerer opplysninger om pasient og bruker, jf. helsepersonelloven § 39 og § 40.

Definisjoner i denne veilederen (hentet fra veileder med avtaleeksempler ved samarbeid om felles journal, se www.normen.no)

-G-

Med "***gruppepraksis***" menes i denne veilederen et *formalisert arbeidsfellesskap* mellom *virksomheter* med behandlere i samme gruppe helsepersonell (jf. helsepersonelloven § 48). For eksempel samarbeid innenfor grupper av fysioterapeuter, leger eller tannleger.

-P-

Med "***profesjonssamarbeid***" menes i denne veilederen et *formalisert arbeidsfellesskap* mellom *virksomheter* med behandlere fra ulike grupper helsepersonell (jf. helsepersonelloven § 48). For eksempel samarbeid mellom lege og psykolog.

4.3 **Samtykkeerklæring**

Databehandlingsansvarlig avgjør om det skal benyttes et skjema for samtykke eller om samtykke innhentes muntlig. I enkelte *EPJ-systemer* kan det også være en avkrysning for samtykke kombinert med for eksempel registrering av *pasientens* mobiltelefonnummer.

Samtykkeerklæring

Mitt samtykke gjelder frem til samtykket trekkes tilbake. Jeg kan når som helst og formfritt, dvs.på hvilken som helst måtetrekke tilbake mitt samtykke.

Jeg godkjenner bruk av:

Formål	Samtykke
Bestilling av timeavtale	☐
Varsel om timeavtale	☐
Aksept av timeavtale	☐
Engangspassord for pålogging til portalløsning	☐
Varsel om melding i annet system	☐

i kommunikasjon mellom meg og <virksomhet>.

Opplysningene skal ikke brukes til annet enn formålene som er angitt ovenfor.

Tildelt tilgang til <portalløsning> er personlig og skal ikke lånes ut til andre.

Samtykkeerklæringen arkiveres (elektronisk eller manuelt) i pasienten/brukerens journal.

Sted:
Dato:

Navn:
Fødselsdato:

_____

Signatur

4.4 Informasjonsplakat

Informasjon til pasienten

Rett til informasjon om behandlingen av helse og personopplysninger
Du har rett til å få vite hvordan opplysningene om deg blir behandlet.

Du har rett til innsyn
Du kan henvende deg til oss og be om å få vite hvilke opplysninger vi har om deg, hva de brukes til, og hvor de er innhentet fra. Dette gjelder både elektronisk og manuell journal. Du har krav på å få svar innen 30 dager.

Du kan kreve at feilaktige eller mangelfulle opplysninger om deg blir rettet
I utgangspunktet skal klinikken/instituttet av eget tiltak rette mangelfulle eller feilaktige opplysninger i journalen. Men det er ikke alltid lett for den som behandler store mengder opplysninger å bli klar over at noe mangler eller er feil. Vi anbefaler derfor at du bruker innsynsretten, og gir beskjed til virksomheten om det er feil.

Du kan kreve at opplysninger i journalen slettes dersom de er feilaktige og misvisende og føles belastende for deg eller åpenbart ikke er nødvendige for å gi helsehjelp.

Du skal kunne utøve dine rettigheter gratis
Når du ber om innsyn, retting og sletting er dette gratis.

Du kan be om utskrift av journalen eller deler av journalen.

Informasjonssikkerhet

- Vi har etter lovgivningen ansvar for å sørge for at helse- og personopplysningene er tilstrekkelig sikret.
- Vi har, blant annet etter prioriteringer fra risikovurderinger, innført prosedyrer som skal gi den nødvendige sikkerhet.
- Vi sikrer at kun de som har et tjenstlig behov, får tilgang til opplysningene. Videre sikrer vi at opplysninger ikke kan endres eller slettes av andre enn de som er autorisert til å gjøre dette.
- Vi sikrer at helse- og personopplysningene er tilgjengelige når det er nødvendig for å utføre våre arbeidsoppgaver, for å gi deg en best mulig tjeneste.
- Vi revurderer våre prosedyrer periodisk slik at sikkerheten til enhver tid skal være så god som mulig. Dersom vi oppdager at en prosedyre ikke er fulgt følges dette grundig opp.

4.5 Gjennomføring av risikovurdering

Figurene i kapittel 1.1 viser ulike løsninger for drift av *EPJ*. Omfanget av risikovurderingen må gjenspeile om det benyttes *databehandler* eller ikke. Den samlede risikovurderingen skal dekke alle områder av *behandlingen* av *helse- og personopplysninger* for å oppnå tilstrekkelig *konfidensialitet*, *integritet*, *tilgjengelighet* og *kvalitet* som er fastsatt i nivå for *akseptabel risiko*.

4.5.1 Mal for risikovurdering

EKSEMPEL PÅ RISIKOVURDERING	
Virksomhet:	
Vurdert av:	**Dato:**
Formålet med risikovurderingen: Kartlegge risikoområder og sannsynlighet og konsekvens for uønskede hendelser. Foreslå tiltak og følge opp at tiltaket er gjennomført.	

Forhold som er vurdert (uønsket hendelse / senario)	**Sannsynlighet**				**Konsekvens**				**Risiko** (sannsynlighet x konsekvens)	**Tiltak? Alltid Ja på høy**	**Beskrivelse av tiltak**	**Betydning/ kommentar**	**Dato for gjennomført tiltak**
Sannsynlighet: 1. Usannsynlig: en gang hver 5. År eller sjeldnere 2. Mindre sannsynlig: 1 gang hvert år 3. Mulig: En gang hver måned 4. Sannsynlig: Daglig eller oftere	1 = Usannsynlig	2 = Mindre Sannsynlig	3 = Mulig	4 = Sannsynlig	1 = Ubetydelig	2 = Moderat	3 = Alvorlig	4 = Kritisk					

1. Ubetydelig / Ingen	**2. Moderat**	**3. Alvorlig**	**4. Kritisk**
• Stans i <system> 0 minutter (kontinuerlig drift) • Intet uautorisert innsyn i personopplysninger • Data er komplett	• Stans i <system> inntil 30 minutter • Uautorisert innsyn i enkelte personopplysninger og lovbrudd • Noen mangler eller feil i data	• Stans i <system> inntil 1 time • Uautorisert innsyn i enkelte personopplysninger, mulighet for endring og brudd på lov • Viktige mangler eller feil i data	• Stans i <system> 4 time eller mer • Fullt uautorisert innsyn i eller mulighet for endring av alle personopplysninger og brudd på lov • Kritiske mangler eller feil i data

Forhold som er vurdert (uønsket hendelse / senario)		Sannsynlighet	Konsekvens	Risiko (sannsynlighet x konsekvens)	Tiltak? Alltid Ja på høy	Beskrivelse av tiltak	Betydning/ kommentar	Dato for gjennomført tiltak
1.	Uautoriserte (for eksempel pasienter) får innsyn i helse- og personopplysinger fra skjermer eller utskrifter	☐☐☒☐ 1 2 3 4 <eksempel>	☐☐☒☐ 1 2 3 4 <eksempel>	☐ 1-4: Lavt ☐ 6-8: Middels ☒ 9-16: Høy	☐ Nei, ikke nødvendig. ☒ Ja	Plassere skjermer og skrivere slik at pasienter ikke får innsyn fra venterommet og når de skal betale i skranke	Ommøblering	
2.	Ansvar og oppgaver for informasjonssikkerhet er ikke dokumentert og gjort kjent i virksomheten med fare for at Normen ikke etterleves og sikkerhetsstyring ikke er mulig.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
3.	Taushetsplikten etterleves ikke iht. Normen fordi medarbeidere ikke er informert om sin taushetsplikt og klar over dens innhold og omfang og konsekvenser ved brudd på taushetsplikten.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
4.	Bruk av minnepinne (innebærer f.eks. risiko for ondsinnet programvare og helse- og personopplysninger på avveie).	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
5.	Risiko knyttet til bortlåning av ID og passord og dermed feil ved signering av journaler	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
6.	Uautorisert tilgang til og bruk av informasjonssystemet (for eksempel ved manglende eller for svake passord)	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja	Innføre eget brukernavn og passord for alle brukere. Sikre godkjent kvalitet på passord.	Bestille av leverandør oppsett av passord-systemet og innføre ny prosedyre for alle medarbeidere	
7.	Helse- og personopplysninger blir utlevert på e-post med fare for brudd på taushetsplikt og krav til konfidensialitet.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			

Forhold som er vurdert (uønsket hendelse / senario)		Sannsynlighet	Konsekvens	Risiko (sannsynlighet x konsekvens)	Tiltak? Alltid Ja på høy	Beskrivelse av tiltak	Betydning/ kommentar	Dato for gjennomført tiltak
8.	Informasjonssystemene driftes utenfor Normens og virksomhetens sikkerhetskrav (f.eks. pga manglende, prosedyrer, kompetanse og informasjon) med fare for brudd på virksomhetens styringssystem og Normens krav.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
9.	Styrende, gjennomførende og kontrollerende dokumenter, resultater fra sikkerhetsrevisjoner – risikovurderinger, avviksbehandling, ledelsens gjennomgang, autorisasjoner og avtaler med partnere, databehandlere og leverandører blir ikke oppbevart minimum 5 år fra det tidspunktet dokumentet ble erstattet med en ny gjeldende utgave med fare for å ikke kunne spore gjeldene prosedyrer, resultater og avtaler tilbake i tid.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
10.	Helse- og personopplysninger deles med personell uten autorisasjon for tilgang (for eksempel mangler betryggende prosedyrer) med fare for brudd på taushetsplikten.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
11.	En brukerkonto eller fellesbruker benyttes av andre en den som er autorisert med konsekvens at prinsippet med individuell tilgangsstyring ikke er mulig samt at personlige kriterier ift roller ikke kan ivaretas. Videre at journal ikke signeres av det helsepersonellet som utførte den enkelte behandling.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
12.	Helse- og personopplysninger utleveres til andre uten at pasienten har samtykket med fare for brudd på taushetsplikten.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			

Forhold som er vurdert (uønsket hendelse / senario)		Sannsynlighet	Konsekvens	Risiko (sannsynlighet x konsekvens)	Tiltak? Alltid Ja på høy	Beskrivelse av tiltak	Betydning/ kommentar	Dato for gjennomført tiltak
13.	Uautoriserte får tilgang til helse- og personopplysninger gjennom lagringsmedia som er faset ut og kommer på avveie. (f.eks pga manglende merking, sletting, prosedyrer for avhending mv.) med fare for brudd på konfidensialitet.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
14.	Papirutskrifter kommer uautoriserte i hende fordi det mangler prosedyrer og fysiske tiltak med fare for brudd på taushetsplikten og den registertes personvern.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
15.	Uautoriserte får adgang til fysiske områder (manglende kontroll på nøkler, innlåsing, skjerming for innsyn) med fare for innsyn i helse- og personopplysninger, tyveri og ødeleggelse.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
16.	Virksomheten er klar over sitt risikonivå iht. gjennomført risikovurdering, men tiltak blir ikke fulgt opp med fare for at opplysningene behandles under ikke akseptabel risiko.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
17.	Tilgang til en brukerkonto er kjent for mange fordi det er manglende passord, svake passord eller lite hemmelighold med fare for uautorisert tilgang til helse- og personopplysninger	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
18.	Medisinsk teknisk utstyr som behandler helse- og personopplysninger er ikke inkludert i virksomhetens arbeid med informasjonssikkerhet, herunder i risikovurderinger, tilgangsstyring og prosedyrer for bruk, på linje med andre informasjonssystemer med fare for at	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			

Forhold som er vurdert (uønsket hendelse / senario)		Sannsynlighet	Konsekvens	Risiko (sannsynlighet x konsekvens)	Tiltak? Alltid Ja på høy	Beskrivelse av tiltak	Betydning/ kommentar	Dato for gjennomført tiltak
	dette utstyret nedgraderer etablert informasjonssikkerhet etter Normen.							
19.	Pasienter får ikke behandling pga nedetid på informasjonssystemene (f.eks. det mangler reserveløsninger, årlig test og verifikasjon av nødprosedyrer) med fare for brudd på tilgjengelighet.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
20.	Det er ikke mulig å verifisere om sikkerhetstiltakene fungerer eller etterleves fordi det ikke gjennomføres jevnlig (årlig) sikkerhetsrevisjon. Sikkerhetsrevisjoner dokumenteres ikke og følges ikke opp med fare for at sikkerhetsbrudd oppstår og regulatoriske krav brytes.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
21.	SMS -løsning er ikke etablert med skille fra eksterne nettverk iht Normens krav med fare for uautorisert tilgang til helse- og personopplysninger.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			
22.	Timebestilling på nett inneholder helseopplysninger.	☐☐☐☐ 1 2 3 4	☐☐☐☐ 1 2 3 4	☐ 1-4: Lavt ☐ 6-8: Middels ☐ 9-16: Høy	☐ Nei, ikke nødvendig. ☐ Ja			

4.6 Mal for styringssystem

Styringssystemet for <virksomhet> som skal sikre at krav til personvern og informasjonssikkerhet er tilstrekkelig. Databehandlingsansvarlig skal sikre at styringssystemet er à jour og at det oppdateres årlig i samråd med databehandler. Det er databehandler som skal besitte den tekniske kompetansen for å sikre at databehandlingsansvarlig kan forvalte sitt overordnede ansvar. Databehandler har derfor ansvar for at det foreligger nødvendige prosedyrer og oversikt over systemer for å ivareta et akseptabelt risikonivå som databehandlingsansvarlig har definert. Databehandlingsansvarlig kan velge å ivareta alle oppgavene databehandler kan utføre, forutsatt at kompetansen og kapasitet er tilstrekkelig.

Dersom virksomheten ikke benytter en databehandler og dermed drifter sitt eget utstyr henvises virksomheten til Mal for internkontroll på legekontor som finnes på www.normen.no.

4.6.1 Oppgaver databehandlingsansvarlig skal ivareta

DBA = Databehandlingsansvarlig
DB = Databehandler

Sikkerhetsorganisering og ansvarsfordeling		**Ansvar DBA eller DB**		
Ansvarsområde	**Ansvarlig (Navn/leverandør)**	**Skisse 1**	**Skisse 2**	**Skisse 3**
Databehandlingsansvarlig (har det endelige ansvaret for at personvern og informasjonssikkerhet er ivaretatt)	<navn på databehandlingsansvarlig/leder i virksomhet>	DBA	DBA	DBA og DB
Tilgangsstyring, autorisasjon og autentisering	<navn på databehandler eller navn på en i virksomheten>	DBA	DBA	DBA og DB
Fysisk sikring av områder og utstyr	<navn på databehandler>	DBA	DBA	DBA og DB
Sikkerhet i nettverket og datautstyret og tekniske krav	<navn på databehandler>	DBA	DBA	DB
Hendelsesregistrering	<navn på databehandler>	DBA	DBA	DB
Hjemmekontor og mobilt utstyr	<navn på databehandler>	DBA	DBA	DBA og DB
Elektronisk kommunikasjon som e-post og SMS	<navn på databehandler>	DBA	DBA	DBA og DB
<eventuelt andre områder som er avtalt med databehandler>	<navn på databehandler>			DBA
Sikkerhetsmål,- strategi og risikohåndtering				
Sikkerhetsmål	– <list opp mål iht kap. 2.1.1>	DBA	DBA	DBA
Sikkerhetsstrategi	– <list opp strategiske valg iht kap. 2.1.2>	DBA	DBA	DBA
Nivå for akseptabel risiko	– <list opp fastsatt nivå for akseptabel risiko iht kap. 2.1.3>	DBA	DBA	DBA

Oversikt over behandlinger av personopplysninger

Behandling (innsamling, registrering, osv)	**Formål med behandlingen av opplysningene og type informasjon**	**Hjemmel**	**Kategorier av opplysninger**	**Melding** **Meldingen skal fornyes hvert 3 år.**	**Databehandler**
Føre pasientjournal, dokumentasjon og sending av henvisning og behandlerkrav, mottak av epikrise	Plikt til å føre pasientjournal for den som yter helsehjelp. Timebok, fakturering og rapportering. Innehente betaling fra pasienter og behandlerkrav fra HELFO.	Helsepersonellovens §§ 39 og 40.	☒ Sensitive ☐ Ikke sensitive ☒ Administrative	☐Nei, unntatt meldeplikt ☒ Ja, meldepliktig Melding ble sendt: den 30/04/2014 <eksempel>	☐ Ja ☒ Nei Databehandler navn: Databehandleravtale inngått dato: __/__/__
<Eventuell forskning>			☐ Sensitive ☐ Ikke sensitive ☐ Administrative	☐Nei, unntatt meldeplikt ☐ Ja, meldepliktig Melding ble sendt: den __/__/__	☐ Ja ☐ Nei Databehandler navn: Databehandleravtale inngått dato: __/__/__

4.6.2 Databehandlingsansvarliges oppfølging av oppgaver som helt eller delvis kan ivaretas av databehandler

I tabellen nedenfor er det en oversikt over faktaark fra Normen som beskriver relevante prosedyrer. Det er databehandlingsansvarlig som skal fastsette hva som skal følges opp gjennom gjennomførende og kontrollerende prosedyrer.

Oppgaver som helt eller delvis utføres av databehandler	**Referanse til faktaark eller veileder**	**Status og risikovurdering**	**Dato for DBA gjennomgang med DB**
Tilgangsstyring, autorisasjon og autentisering	14 - Tilgangsstyring 31 - Passord og passordhåndtering 47 - Autorisasjonsregister	Status: • Risiko: • Eventuelle tiltak som må gjennomføres: •	Dato for gjennomgang: __/__/____ Dato for utbedring av eventuelle tiltak: __/__/____
Fysisk sikring av områder og utstyr	17 - Fysisk sikring av områder og utstyr	Status: • Risiko: • Eventuelle tiltak som må gjennomføres: •	Dato for gjennomgang: __/__/____ Dato for utbedring av eventuelle tiltak: __/__/____

Oppgaver som helt eller delvis utføres av databehandler	**Referanse til faktaark eller veileder**	**Status og risikovurdering**	**Dato for DBA gjennomgang med DB**
Sikkerhet i nettverket, datautstyret og tekniske krav	19 - Tiltak for å hindre ondsinnet programvare 21 - Sikkerhetskopiering (backup) 25 - Lagringstid og sletting av helse- og personopplysninger 28 - Alternative tekniske løsninger for primærhelsetjenesten 34 - Håndtering av lagringsmedia	Status: • Risiko: • Eventuelle tiltak som må gjennomføres: •	Dato for gjennomgang: __/__/____ Dato for utbedring av eventuelle tiltak: __/__/____
Hendelsesregistrering	15 - Hendelsesregistrering og oppfølging	Status: • Risiko: • Eventuelle tiltak som må gjennomføres: •	Dato for gjennomgang: __/__/____ Dato for utbedring av eventuelle tiltak: __/__/____
Hjemmekontor og mobilt utstyr	22 - Kontroll og sikring av ekstern tilgang 29 - Hjemmekontor 20 - Sikkerhets- og samhandlingsarkitektur	Status: • Risiko: • Eventuelle tiltak som må gjennomføres: •	Dato for gjennomgang: __/__/____ Dato for utbedring av eventuelle tiltak: __/__/____
Opplæring og kompetanse	9 - Opplæring av ledere og medarbeidere	Status: • Risiko: • Eventuelle tiltak som må gjennomføres: •	Dato for gjennomgang: __/__/____ Dato for utbedring av eventuelle tiltak: __/__/____
Elektronisk kommunikasjon som e-post, portal og SMS	Veileder i bruk av portalløsninger, SMS og e-post	Status: • Risiko: • Eventuelle tiltak som må gjennomføres: •	Dato for gjennomgang: __/__/____ Dato for utbedring av eventuelle tiltak: __/__/____

4.6.3 Oppfølging av informasjonssikkerheten

Oppgavene skal databehandlingsansvarlig utføre for å påse at behandlingen av helse- og personopplysninger er iht sikkerhetsmålene, sikkerhetsstrategien og vedtatte prosedyrer.

Revisjon og vurdering av styringssystemet		
Område	**Beskrivelse**	
Overordnet status og oppfølgning	Ansvarlig for sikkerhetsrevisjon	<hvem gjennomførte siste sikkerhetsrevisjon>
	Siste sikkerhetsrevisjon (årlig aktivitet)	<dato for siste og neste sikkerhetsrevisjon>
	Status fra siste sikkerhetsrevisjon	<Beskrivelse av status og antall avvik som ikke er lukket. Sikkerhetsrevisjonen må som et minimum omfatte en vurdering av virksomhetens organisering, sikkerhetstiltak og bruken av kommunikasjonspartnere og leverandører>
	Plan for sikkerhetsrevisjonen	<når og hvem skal gjennomføre sikkerhetsrevisjoner det neste året>
	Ledelsens gjennomgang (gjennomføres minimum årlig)	<dato for siste gjennomgang og oppsummering av status>
Revisjon av avtaler og prosesser	Revisjon av gjeldende databehandleravtaler	<for eksempel: avtaler med databehandler ivaretar behov for tydelig ansvarsfordeling og sikkerhetsansvar>
	Revisjon av gjeldende leverandøravtaler (øvrige leverandører)	<for eksempel: avtaler med øvrige leverandører ivaretar behov for tydelig ansvarsfordeling og sikkerhetsansvar>
	Prosedyre for retting og sletting av pasient-opplysninger, herunder oppbevaring av pasientjournal	<for eksempel: prosedyre for retting og sletting er iht. til lovverket og understøttes av tekniske løsninger>
	Prosedyre for pasientens innsyn i registrerte opplysninger	<for eksempel: prosedyre for innsyn er iht. til lovverket og understøttes av tekniske løsninger>

Kontroll av oppgaver som helt eller delvis er ivaretatt av databehandler		
Område som skal være dekket	**Hvordan området er ivaretatt**	**Avvik, hendelser med tiltak**
Tilgangsstyring, autorisasjon og autentisering	<for eksempel: Databehandler har tilfredsstillende prosedyrer for tilgangskontroll, risiko er akseptabel>	<for eksempel: Det har ikke vært avvik og alle tiltak er lukket>
Innsynsrett i helse-personopplysninger		

Kontroll av oppgaver som helt eller delvis er ivaretatt av databehandler		
Område som skal være dekket	**Hvordan området er ivaretatt**	**Avvik, hendelser med tiltak**
Retting og sletting av pasientopplysninger, herunder oppbevaring av pasientjournal		
Fysisk sikring av områder og utstyr		
Sikkerhet i nettverket og datautstyret og tekniske krav		
Hendelsesregistrering		
Hjemmekontor og mobil arbeidsplass		
Elektronisk kommunikasjon som e-post og SMS		
<andre områder>		

4.6.4 Databehandlingsansvarliges sjekkliste for ivaretakelse av Normen

Sjekklisten inneholder kravene i Normen slik at databehandlingsansvarlig på en enkel måte kan sjekke at virksomheten følger Normens krav til informasjonssikkerhet. Dersom alle spørsmålene i sjekklisten besvares med "Ja" har databehandlingsansvarlig dokumentasjon ved et tilsyn fra Datatilsynet. Dersom noen av punktene besvares med "Nei" må nødvendig tiltak iverksettes for å kunne dekke alle Normens krav. Sjekklisten beskriver hva databehandlingsansvarlig kan gjøre for at hvert punkt skal bli oppfylt.

Sjekkliste for databehandlingsansvarlig – Personvern og informasjonssikkerhet					
Nr	**Krav**	**Kap. i veileder**	**Er kravet ivaretatt i din virksomhet?**		
			Ja	**Nei**	**Hvis nei, utfør følgende aktivitet**
Kapittel 1 - Innledning					
Ansvar					
1.	Er det besluttet og fylt ut informasjon om hvem som er databehandlingsansvarlig(e)?	1.1			Fyll ut informasjonen i kap. 4.6 Mal for styringssystem - sikkerhetsorganisering og ansvarsforhold
2.	Er det fastsatt og fylt ut informasjon om hvem som er databehandler?	1.1			Fyll ut informasjonen i kap. 4.6 Mal for styringssystem – sikkerhetsorganisering og ansvarsforhold
3.	Dersom virksomheten benytter databehandler, er det signert en databehandlingsavtale?	1.1			Fyll ut databehandlingsavtale, eksempel til avtaletekst finnes på www.normen.no
Oversikt over sentrale lovverk					
4.	Har databehandlingsansvarlig oversikt over relevante lover for personvern og informasjonssikkerhet?	4.2			Les kapittel 4.2 Oversikt over sentrale lovregler i veilederen

Sjekkliste for databehandlingsansvarlig – Personvern og informasjonssikkerhet

Nr	Krav	Kap. i veileder	Er kravet ivaretatt i din virksomhet? Ja	Nei	Hvis nei, utfør følgende aktivitet
Kapittel 2 – Oppgaver databehandlingsansvarlig skal ivareta					
Krav til informasjonssystemet ved behandling av helse- og personopplysninger					
5.	Er det fastsatt og fylt ut sikkerhetsmål for virksomheten?	2.1.1			Fyll ut sikkerhetsmålene i kap. 4.6 Mal for styringssystem
6.	Er det utarbeidet og beskrevet en sikkerhetsstrategi for å nå sikkerhetsmålene?	2.1.2			Fyll ut sikkerhetsstrategien i kap. 4.6 Mal for styringssystem
7.	Er det fastsatt og beskrevet nivå for akseptabel risiko?	2.1.3			Fyll ut nivå for akseptabel risiko i kap. 4.6 Mal for styringssystem
8.	Er det utarbeidet en oversikt over hvilke behandlinger av helse- og personopplysninger som skjer i virksomheten?	2.1.4			Fyll ut oversikt over behandlinger av personopplysninger i kap. 4.6 Mal for styringssystem
9.	Er alle behandlinger av helse- og personopplysninger meldt til Datatilsynet?	2.1.4			Send melding til Datatilsynet gjennom deres nettsider: Melding om behandling av personopplysninger
Oppgaver ved behandling av helse- og personopplysninger					
10.	Er det utarbeidet en oversikt som viser hvem som har tilgang til virksomhetens helse- og personopplysninger?	2.2.1			Se kapittel 3.2.1 Tilgangsstyring, autorisasjon og autentisering i Mal for internkontroll – legekontor. Malen kan hentes på www.normen.no
11.	Er det etablert rutiner som sikrer en oversikt med tildelte tilganger per rolle?	2.2.1			Fyll ut tabell i kapittel 3.2.1 Tilgangsstyring, autorisasjon og autentisering i Mal for internkontroll – legekontor. Malen kan hentes på www.normen.no
12.	Er det etablert et autorisasjonsregister?	2.2.1			Fyll ut tabell i kapittel 3.2.1 Tilgangsstyring, autorisasjon og autentisering i Mal for internkontroll – legekontor. Malen kan hentes på www.normen.no
13.	Lagres oppføringene i autorisasjonsregisteret i minimum 5 år fra det tidspunkt autorisasjonen ble tatt ut av bruk	2.2.1			Se Faktaark 47 – Autorisasjonsregister, for krav til innhold og oppbevaring av autorisasjonsregisteret
14.	Inngår tilgangsstyring, autorisasjon og autentisering i virksomhetens risikovurdering?	2.2.1			Fyll ut risikovurderingen i kap. 4.6 Mal for styringssystem
15.	Er det innhentet signert taushetserklæring fra alle som får tilgang til fortrolige opplysninger om virksomheten eller virksomhetens pasienter?	2.2.1.1			Fyll ut taushetserklæring, eksempel til avtaletekst finnes på www.normen.no
16.	Er det etablert rutiner og en holdninger som forhindrer at helse- og personopplysninger ikke kommer på avvei, enten via IT-utstyr eller utskrifter (PC og mobil, skriver, Internett og trådløst nettverk)?	2.2.2			Fyll ut informasjonen om fysisk sikring av i kap. 4.6 Mal for styringssystem
17.	Er det inngått skriftlig avtale ved bruk av ekstern leverandør som spesifiserer ansvar og oppgavefordeling?	2.2.3			Fyll ut leverandøravtale, eksempel til avtaletekst finnes på www.normen.no

Sjekkliste for databehandlingsansvarlig – Personvern og informasjonssikkerhet

Nr	Krav	Kap. i veileder	Er kravet ivaretatt i din virksomhet?		
			Ja	Nei	Hvis nei, utfør følgende aktivitet
18.	Er det fastsatt rutiner for opplæring og kompetanseheving i virksomheten?	2.2.4			Se kapittel 3.2.11 Opplæring og kompetanse i Mal for internkontroll – legekontor. Malen kan hentes på www.normen.no
19.	Gis pasienten informasjon om sine rettigheter knyttet til samtykke, reservasjon, innsyn, retting og sletting?	2.2.5			Se forslag til informasjonsplakat kapittel 4.4 Informasjonsplakat i veilederen
20.	Gis pasientene mulighet til innsyn i egen journal?	2.2.6			Fyll ut innsynsprosedyrer i kap. 4.6.3 Mal for styringssystem
21.	Er det etablert rutiner for utlevering og sammenstilling av pasientens journal?	2.2.7			Se kapittel 4.1.4
22.	Er pasientens rettigheter til retting/sletting av helse- og personopplysninger ivaretatt?	2.2.8			Fyll ut prosedyre for retting og sletting av pasientopplysninger, herunder oppbevaring av pasientjournal i kap. 4.6.3 Mal for styringssystem
23.	Ved overføring av helse- og personopplysninger til utlandet, er reglene for dette fulgt?	2.2.9			Se kap 3.2.16 Overføring av helse- og personopplysninger til utlandet i Mal for internkontroll – legekontor. Malen kan hentes på www.normen.no
Oppfølging av informasjonssikkerheten					
24.	Er det utarbeidet en plan for sikkerhetsrevisjon?	2.3.1			Fyll ut dato og hvem som skal gjennomføre sikkerhetsrevisjon det neste året i kap. 4.6 Mal for styringssystem
25.	Har databehandlingsansvarlig gjennomført årlig sikkerhetsrevisjon?	2.3.1			Fyll ut skjema for sikkerhetsrevisjon i kap 4.3 i Mal for internkontroll – legekontor. Fyll ut dato for siste gjennomførte sikkerhetsrevisjon i kap. 4.6 Mal for styringssystem
26.	Er resultatene fra sikkerhetsrevisjonen dokumentert?	2.3.1			Fyll ut status fra sikkerhetsrevisjonene i kap. 4.6 Mal for styringssystem
27.	Fornyes meldinger til Datatilsynet hvert tredje år?	4.1.1 og 2.1.4			Fornyelse av melding til Datatilsynet gjennom deres nettsider www.datatilsynet.no. Oppdater tabellen i kapittel 4.6.1 Mal for styringssystem
28.	Er det gjennomført kontroll siden forrige ledelsens gjennomgang?	2.3.3			Fyll ut Mal for styringssystem – Kontroll av Oppgaver som helt eller delvis er ivaretatt av databehandler (Kap 4.6.3)
29.	Har databehandlingsansvarlig gjennomgått og kontrollert at oppgaver og tiltak er gjennomført av databehandler?	2.3.3			Fyll ut tabell i kap. 4.6.2 Databehandlingsansvarligs oppfølging av oppgaver som helt eller delvis kan ivaretas av databehandler i veilederen
30.	Er det etablert prosedyrer for håndtering av avvik?	2.3.4			Fyll ut avviksskjema. Eksempel på avviksskjema i kap. 2.3.4
31.	Gjennomgås, minimum årlig, virksomhetens sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene?	2.3.5			Fyll ut dato og oppsummering av ledelsens gjennomgang i kap. 4.6 Mal for styringssystem
Kapittel 3 – Oppgaver som helt eller delvis kan ivaretas av databehandler					
Fysisk sikring av områder og utstyr					
32.	Er det utarbeidet prosedyrer for fysisk sikring av områder og utstyr?	3.1			Se kap. 3.2.5 Fysisk sikring av områder og utstyr i Mal for internkontroll – legekontor på www.normen.no.

Sjekkliste for databehandlingsansvarlig – Personvern og informasjonssikkerhet

Nr	Krav	Kap. i veileder	Er kravet ivaretatt i din virksomhet?		
			Ja	Nei	Hvis nei, utfør følgende aktivitet
33.	Inngår fysisk sikring av områder og utstyr i virksomhetens risikovurdering?	3.1			Fyll ut risikovurderingen i kap. 4.6 Mal for styringssystem
Sikkerhet i nettverket, datautstyret og tekniske krav					
34.	Er det utarbeidet prosedyrer som sikrer korrekt gjennomføring av konfigurasjonskontroll?	3.2			Se kap. 3.2.6 Sikkerhet i nettverket og datautstyret i Mal for internkontroll – legekontor på www.normen.no
35.	Er det utarbeidet prosedyrer som sikrer nødvendig sikkerhetskopiering av helse- og personopplysninger?	3.2			Se kap. 3.2.6 Sikkerhet i nettverket og datautstyret i Mal for internkontroll – legekontor på www.normen.no
36.	Er det utarbeidet prosedyrer for å hindre ondsinnet programvare?	3.2			Se kap. 3.2.6 Sikkerhet i nettverket og datautstyret i Mal for internkontroll – legekontor på www.normen.no
37.	Er det utarbeidet prosedyrer for å sikre korrekt behandling av helse- og personopplysninger ved utfasing av utstyr?	3.2			Se kap. 3.2.6 Sikkerhet i nettverket og datautstyret i Mal for internkontroll – legekontor på www.normen.no
38.	I tilfeller der virksomheten har inngått avtale med leverandør om sletting av opplysninger, er det undertegnet en avtale mellom virksomheten og leverandør?	3.2			Fyll ut leverandøravtale, eksempel til avtaletekst finnes på www.normen.no
39.	Inngår sikkerhet i nettverket, datautstyret og tekniske krav i virksomhetens risikovurdering?	3.2			Fyll ut risikovurderingen i kap. 4.6 Mal for styringssystem
Hendelsesregistrering					
40.	Er det etablert prosedyrer for hendelsesregistrering?	3.3			Se kap. 3.2.7 Hendelsesregistrering i Mal for internkontroll – legekontor på www.normen.no
41.	Har virksomheten hendelsesregister?	3.3			Fyll ut tabell i kap. 3.2.7 Hendelsesregistrering i Mal for internkontroll – legekontor på www.normen.no
42.	Er det etablert prosedyrer for kontroll av hendelsesregistre?	3.3			Se kap. 3.2.7 Hendelsesregistrering i Mal for internkontroll – legekontor på www.normen.no
43.	Inngår vurdering av hendelsesregistreringen i virksomhetens risikovurdering?	3.3			Fyll ut risikovurderingen i kap. 4.4 Mal for styringssystem – Risikovurdering og internkontroll av oppgaver som helt eller delvis er ivaretatt av databehandler
Hjemmekontor og mobilt utstyr					
44.	Har databehandlingsansvarlig fastsatt prosedyrer for sikker bruk av hjemmekontor og mobilt utstyr?	3.4			Se kap. 3.2.9 Hjemmekontor i Mal for internkontroll – legekontor på www.normen.no.
45.	Inngår bruk av hjemmekontor og mobilt utstyr i virksomhetens risikovurdering?	3.4			Fyll ut risikovurderingen i kap. 4.6 Mal for styringssystem
Elektronisk kommunikasjon som e-post og SMS					
46.	Dersom virksomheten benytter elektronisk kommunikasjon til pasient, er løsningen i tråd med kravet til personvern og informasjonssikkerhet?	3.5			Se veileder i bruk av portalløsninger, SMS og e-post på www.normen.no.

Sjekkliste for databehandlingsansvarlig – Personvern og informasjonssikkerhet

Nr	Krav	Kap. i veileder	Er kravet ivaretatt i din virksomhet?		
			Ja	Nei	Hvis nei, utfør følgende aktivitet
47.	Inngår bruk av elektronisk kommunikasjon som e-post og SMS i virksomhetens risikovurdering?	3.5			Fyll ut risikovurderingen i kap. 4.4 Mal for styringssystem – Risikovurdering og internkontroll av oppgaver som helt eller delvis er ivaretatt av databehandler

4.7 Referanser

Relevante nettsteder og dokumenter:

- Hjemmeside til *Normen*: www.normen.no
- Hjemmeside til Datatilsynet: www.datatilsynet.no
- Hjemmeside til Helsetilsynet: www.helsetilsynet.no
- Hjemmeside til Norsk Helsenett: www.nhn.no
- Hjemmeside til Lovdata: www.lovdata.no

5 DELTAGERE I UTARBEIDELSE AV VEILEDEREN

Navn	Organisasjon	Tittel
Tor Ottersen	Helsedirektoratet	Seniorrådgiver, leder for sekretariatet for Normen
Jan Gunnar Broch	Helsedirektoratet	Seniorrådgiver
Holmar Ø. Finnsson	Helsedirektoratet	Seniorrådgiver
Ida Martinussen	Helsedirektoratet	Seniorrådgiver
Jan Henriksen	Helsedirektoratet	Seniorrådgiver
Nina Cecilie Carlsen	Helsedirektoratet	Seniorrådgiver
Ole Jørgen Grannes	Helsedirektoratet	Seniorrådgiver
Braar Larsen	Datatilsynet	Senioringeniør
Olga Rugsland	Norsk Fysioterapeutforbund	Fysioterapeut
Joachim T. Andersen	Norsk Kiropraktorforening	Kiropraktor
Jostein Stensland	Norsk Manuellterapeutforening	Manuellterapeut
Peter C. Lehne	Norsk Manuellterapeutforening	Manuellterapeut
Julius Okkenhaug	Norsk Psykologforening	Spesialrådgiver
Andreas Høstmælingen	Norsk Psykologforening	Spesialrådgiver
Dag Helge Haslekås	ASPIT AS	Daglig leder
Thore Farmen	Unisoft IKT AS	Daglig leder
Kim Saxvik	KPMG	Senior konsulent
Nora Henriksen	KPMG	Junior konsulent