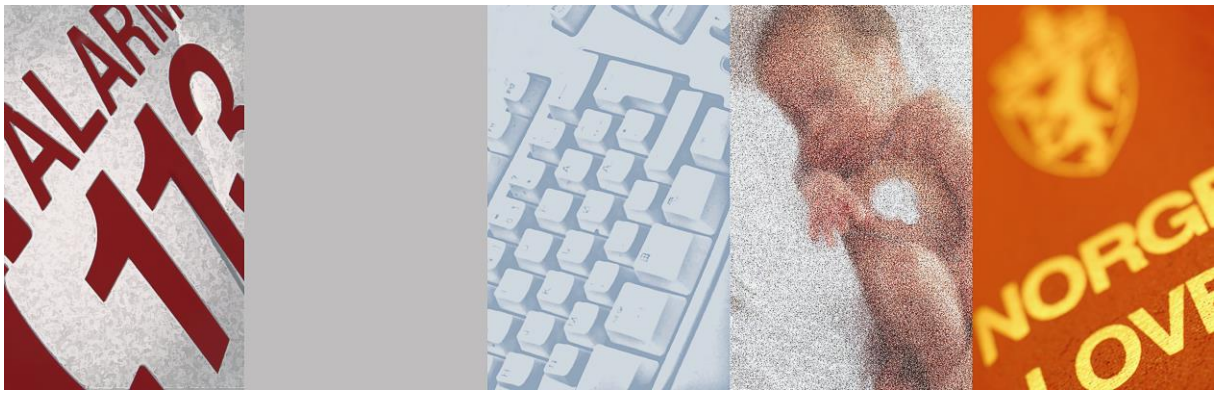
Personvern og informasjonssikkerhet for virksomheter i tannhelsetjenesten

- en veileder

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

Endringshistorikk for og godkjenning av dokumentet

Versjon	Endringer	Godkjent av styringsgruppen for Normen (dato)
1.0	Første utgave av veilederen	Februar 2010
1.1	Etter innspill fra instruktørkurset	Sekretariatet Mai 2010
1.2	Oppdatering av terminologi og referanser	Sekretariatet Jan. 2011
1.3	Oppdatert referanser i definisjon "taushetsplikt"	Sekretariatet 6.jun 2013
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 Bakgrunn

Stor dynamikk, økt samhandling, høy grad av elektronisk registrering og bruk av IT-systemer for dokumentasjon preger arbeidsdagen i de ulike delene av tannhelsetjenesten, både i det offentlige og i det private.

Norsk Helsenett (helsenettet) er den elektroniske samhandlingsarenaen for helse- og omsorgssektoren (se www.nhn.no). Nytteverdien er stor, og mange *virksomheter* vil knytte seg til helsenettet. Dette gir en enklere og sikrere samhandling med andre *virksomheter*.

Det er sentralt at *virksomheter* innen tannhelsetjenesten følger lovpålagte krav til personvern og informasjonssikkerhet.

På denne bakgrunn er det behov for en veileder i personvern og informasjonssikkerhet som er rettet spesielt mot tannhelsetjenesten.

Hensikten med veilederen er i første rekke å gi *virksomheter* i tannhelsetjenesten et praktisk verktøy i arbeidet med å ivareta gjeldende personvern- og informasjonssikkerhetskrav. Målsetningen er at *virksomhetene* ivaretar gjeldende lovkrav ved å følge anbefalingene i veilederen.

Med veilederen følger det en mal for internkontroll med oversiktlige prosedyrer, konkrete maler og sjekklister. Disse beskriver sikkerhetskrav og prosedyrer *virksomheten* må etablere som et minimum og kan legges til grunn i det daglige arbeidet med informasjonssikkerhet.

Når dette er etablert, vil det utgjøre *virksomhetens* eget styringssystem for informasjonssikkerhet. Samtidig vil kravet til skriftlig dokumentasjon være ivaretatt.

Veilederen vil gi en enklere hverdag for *virksomhetene* i arbeidet med å ivareta lovpålagte krav til personvern og informasjonssikkerhet.

Veilederen er bygget opp slik:

- Kapittel 1 inneholder bakgrunnsinformasjon og definisjoner
- Kapittel 2 gir en kort redegjørelse for kravene til personvern og informasjonssikkerhet i tannhelsetjenesten mer generelt
- Kapittel 3 er selve veiledningen i informasjonssikkerhet
- Kapittel 4 inneholder referanser til nyttige linker og ytterligere dokumentasjon

Veilederen dekker ikke forskning. For forskning vises det til veileder til *Normen*: ”Personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren”.

Veilederen er utarbeidet for styringsgruppen for *Normen* med støtte fra Helsedirektoratet av selskapene Advokatfirmaet Wiegaard, INCERTUS og INFOSEC og kvalitetssikret av Pharos, i samarbeid med tannhelsetjenesten (se kapittel 4.4).

1.2 Om Normen

Norm for informasjonssikkerhet (*Normen*) ble lansert i august 2006. *Normen* skal bidra til tilfredsstillende informasjonssikkerhet hos den enkelte *virksomhet*, og i helsesektoren generelt. I tillegg skal *Normen* bidra til å harmonisere informasjonssikkerheten, slik at *virksomhetene* kan ha gjensidig tillit til hverandre.

Normen bygger på gjeldende bestemmelser om personvern og informasjonssikkerhet, bl.a. reglene i personopplysningsloven og helseregisterloven.

Kravene i *Normen* er derfor basert på gjeldende regler på personvern- og informasjonssikkerhetsområdet. Enhver *virksomhet* som etterlever *Normen* vil tilfredsstille alle krav i lovverket til informasjonssikkerhet. Alle som knytter seg til helsenettet er - gjennom avtalen om tilknytning - forpliktet til å følge *Normen*.

1.3 Målgruppe

Målgruppen for veilederen er private *virksomheter* innen tannhelsetjenesten og den fylkeskommunale tannhelsetjenesten.

Denne veilederen er primært rettet mot personell med ansvar, oppgaver og roller i forbindelse med personvern og informasjonssikkerhet i *virksomhetene*. Eksempler på slikt personell er:

Innen det private
- Leder for den enkelte, private *virksomhet* i tannhelsetjenesten (den ansvarlige eieren av praksisen/tannklinikken)
- Assistenttannlege
- Kontraktørtannlege

Innen det offentlige
- Fylkesordfører, fylkesrådmann (som overordnet ansvarlig for den fylkeskommunale tannhelsetjenesten)
- Ledere innen den fylkeskommunale tannhelsetjenesten
- Personell ved de odontologiske fakultetene og høyskolene
- Personell i forsvaret

Andre som kan ha nytte av veilederen
- Det enkelte helsepersonell (f.eks. tannlege i privat og offentlig sektor, tannpleier, tannhelsesekretær, tanntekniker)
- Tannlegesekretær (uten autorisasjon)
- *Databehandlere*
- *EPJ-leverandører*
- Røntgenleverandører
- IKT-*leverandører*
- Sikkerhetskoordinatorer
- Spesialisthelsetjenesten

1.4 Veilederens forhold til andre dokumenter og veiledere

Dokument (for pekere, se pkt. 4.3)	**Forhold til denne veilederen**
Norm for informasjonssikkerhet (*Normen*)	Overordnet dokument, bindende ved avtale.
Støttedokumenter til *Normen*: Faktaark og veiledere (herunder denne veilederen)	Gir utfyllende veiledning på ulike tematiske områder. Er underordnet *Normen*, og ikke bindende.
Veileder i informasjonssikkerhet ved tilknytning mellom kommuner, fylkeskommuner og helsenettet	Presiserer krav og gir anbefalinger når kommuner og fylkeskommuner skal tilknyttes helsenettet.
Veileder for fjernaksess mellom leverandør og virksomhet	Presiserer krav og gir anbefalinger om *fjernaksess*
En veiledning om internkontroll og informasjonssikkerhet	Datatilsynets veileder i internkontroll
Databehandleravtaler etter personopplysningsloven og helseregisterloven	Datatilsynets veileder i utarbeidelse av databehandleravtaler

1.5 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* (av feb.2015)

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 "***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.

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

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.

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*.

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 "***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 a) og pasientjournalloven § 2 a).*

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 a) og pasientjournalloven § 2 a).

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*.

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 "***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.

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.

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.

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- og personopplysninger*, og dette ut fra de foreliggende omstendigheter må vurderes som rettmessig.

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.

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

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

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, helseregisterloven § 17, pasientjournalloven § 15, helse- og omsorgstjenesteloven § 12-1, spesialisthelsetjenesteloven § 6-1 og forvaltningsloven §§ 13 til 13e, samt annen informasjon med betydning for informasjonssikkerheten, jf. personopplysningsforskriften § 2-9. *Taushetsplikt* innbefatter både en passiv plikt til å tie og en plikt til aktivt å hindre uvedkommende i å få kunnskap om taushetsbelagte opplysninger.

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

Nye definisjoner

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

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.

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.*

2 OVERSIKT OVER SENTRALE LOVREGLER OG TILSYNSMYNDIGHETENS ROLLE

2.1 Helsepersonelloven

Etter helsepersonelloven (§ 48) er tannlege, tannpleier, tannhelsesekretær og tanntekniker autorisert helsepersonell. Den som yter helsehjelp har plikt til å føre journal (§ 39).

Loven gir regler om *taushetsplikt*. Helsepersonell har som hovedregel *taushetsplikt* om pasientforhold (§ 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 innenfor tannhelsetjenesten. Imidlertid har pasienten reservasjonsrett, dvs. rett til å motsette seg at opplysninger gis til samarbeidende personell (§ 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 føres hos en *databehandler*, 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.

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

2.2 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.

Det heter i loven (§ 3-6) at opplysninger om sykdomsforhold - og andre personlige opplysninger - skal *behandles* i samsvar med *taushetsplikten*. At *helse- og personopplysninger* skal *behandles* med varsomhet og respekt for integriteten til den opplysningene gjelder, er derfor både en plikt for helsepersonellet og en rettighet for pasienten. 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 (§ 5-3). Pasientrettighetsloven slår fast at pasienten som hovedregel har rett til innsyn i sin egen journal (§ 5-1).

2.3 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 fast forbudet mot snoking i pasientjournaler, presisert på den måten 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 til pasienten, administrasjon av helsehjelp, internkontroll, kvalitetssikringen av helsehjelpen eller har særskilt hjemmel i lov.

2.4 Personopplysningsloven

Personopplysningsloven gir grunnleggende regler og definisjoner innen personvern og informasjonssikkerhet. Som nevnt under pkt. 1.2, bygger *Normen* bl.a. på reglene i personopplysningsloven. Definisjoner brukt i denne veilederen er i stor grad hentet fra personopplysningsloven , se pkt. 1.5.

Etter loven har en *virksomhet* i tannhelsetjenesten *meldeplikt* til Datatilsynet for sine *behandlinger* av *helse- og personopplysninger*. *Meldeplikten* gjennomføres ved å fylle ut og sende elektronisk skjema via www.datatilsynet.no. Meldingen skal fornyes hvert tredje år.

2.5 Spesielt om straffeansvar

Brudd på regler om *taushetsplikt* og informasjonssikkerhet mv. kan medføre straffeansvar for *virksomheten* (foretaksstraff) eller det enkelte personell.

2.6 Tilsynsmyndigheters rolle og ansvar

Etter helsepersonelloven har tannlegene og annet autorisert helsepersonell plikt til å føre journal. Etter tannhelsetjenesteloven er det Statens helsetilsyn som skal føre tilsyn med journalen og *helse- og personopplysningene* i den. Etter personopplysningsloven og helseregisterloven skal Datatilsynet føre tilsyn med hvordan *helse- og personopplysninger behandles* og sikkerheten rundt dem.

3 VEILEDNING I ARBEIDET MED INFORMASJONSSIKKERHET

Dette kapittelet gir en oversikt over og en veiledning i nødvendige sikkerhetstiltak for *virksomheten*. Det er gitt en forklaring for hvert enkelt sikkerhetstiltak. På denne måten vil leseren få en forståelse av tiltaket før det konkret iverksettes.

Kapittelet er delt i en styrende del, en gjennomførende del og en kontrollerende del.

Hver del inneholder de viktigste sikkerhetstiltakene *virksomheten* må gjennomføre for å ivareta kravene.

Vær oppmerksom på at ingen *virksomhet* er lik den annen - de skiller seg fra hverandre i størrelse og type. Omfanget på tiltakene må derfor tilpasses den enkelte *virksomhet*. Ikke alle tiltakene er like relevante for alle *virksomheter*.

For hvert av tiltakene er det utarbeidet en konkret prosedyre, som kan implementeres i *virksomheten*. Disse prosedyrene finnes samlet i en egen mal for internkontroll. Malen kan lastes ned fra nettstedet www.normen.no.

Alle avsnittene i dette kapittelet korresponderer med tilsvarende avsnitt i malen for internkontroll.

Når malen for internkontroll er utfylt og på plass, har *virksomheten* et styringssystem for informasjonssikkerhet. Styringssystemet er således basert på prinsipper om internkontroll. Dokumentasjonen kan derfor - med fordel - inngå som en del av *virksomhetens* øvrige dokumentasjon for internkontroll (HMS mv.).

3.1 STYRENDE DEL

I styrende del skal alle prinsipper for gjennomførende og kontrollerende informasjonssikkerhetstiltak beskrives.

I styrende del skal det fremkomme hva som er *virksomhetens* sikkerhetsmål og sikkerhetsstrategi og *virksomheten* skal utarbeide oversikt over *behandlinger* av *helse- og personopplysninger*. *Virksomheten* skal videre fastsette nivå for akseptabel risiko.

3.1.1 Ansvar

Det er *virksomhetens* ledelse som er ansvarlig for informasjonssikkerheten.

Det daglige ansvaret ligger som oftest hos daglig leder i *virksomheten*. Den som har det daglige ansvaret for informasjonssikkerheten, kan delegere oppgaver til egne ansatte.

Oppgaver kan også delegeres til eksterne, f.eks. kan man delegere oppgaver til *leverandører*. Dette må gjøres i form av skriftlige avtaler.

Uansett om oppgaver er delegert eller ikke, ligger det juridiske ansvaret hos *databehandlingsansvarlig* (for eksempel leder for den enkelte private *virksomhet* i tannhelsetjenesten - den ansvarlige eieren av praksisen/tannklinikken, assistenttannlege, kontraktørtannlege).

Virksomheter innen tannhelsetjenesten er organisert på ulike måter.

Innen fylkeskommunen og offentlige tannklinikker har fylkesrådmannen det øverste formelle ansvaret (*databehandlingsansvarlig*), men oppgavene vil i det daglige ofte være delegert til leder i den fylkeskommunale tannhelsetjenesten.

I privat tannhelsetjeneste vil det formelle ansvaret (*databehandlingsansvarlig*) avhenge av organisasjonsform.

Aktuelle organisasjonsformer er:

- aksjeselskap med databehandlingsansvar. Styret ved styreleder skal forvalte ansvaret på vegne av selskapet, men i det daglige vil ansvaret normalt være delegert til daglig leder, om *virksomheten* har daglig leder
- enkeltpersonforetak. Eieren er *databehandlingsansvarlig*

I mange *virksomheter* benyttes en kontraktørmodell ved at *virksomheten* kjøper tannhelsetjenester av et autorisert helsepersonell, i praksis en tannlege eller tannpleier. I informasjonssikkerhetssammenheng er det *virksomheten* og ikke det innleide personellet som har ansvaret.

En annen modell som benyttes er ordningen med assistenttannlege, hvor en tannlege leier seg inn i *virksomheten*. Assistenttannlegen har et selvstendig ansvar (*databehandlingsansvarlig).*

Gjennom avtaler *virksomheten* har med andre *virksomheter*, kontraktør eller assistenttannlege, må ansvaret tydeliggjøres.

Det skal angis i meldingen til Datatilsynet - jfr. pkt. 2.4 - hvilken stilling som har det daglige ansvaret for oppfyllelse av *virksomhetens* plikter, herunder for informasjonssikkerheten.

3.1.2 Styringssystem for informasjonssikkerhet

Etter *Normen* plikter *virksomheten* å etablere et styringssystem for informasjonssikkerhet. Et styringssystem angir aktiviteter for å rettlede og styre *virksomheten* og er basert på alminnelige internkontrollprinsipper. Kravene og anbefalingene som er angitt i kapittel 3 er normalt en del av dette styringssystemet.

3.1.3 Sikkerhetsmål

Virksomheten skal ha utarbeidet sikkerhetsmål. *Behandling*en av *helse- og personopplysninger* og *virksomhetens* sikkerhetstiltak skal gjennomføres i tråd med disse.

Sikkerhetsmålene er *virksomhetens* overordnede føringer for *behandling* av *helse- og personopplysninger*.

Sikkerhetsmålene bør være konkrete, målbare og lett å operasjonalisere i en sikkerhetsstrategi.

3.1.4 Sikkerhetsstrategi

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

Sikkerhetsstrategien skal være så klar at *virksomheten* ut fra den kan utarbeide prosedyrer i sitt styringssystem for informasjonssikkerhet.

3.1.5 Nivå for akseptabel risiko

Virksomheten skal ha fastsatt nivå for akseptabel risiko. Med "akseptabel risiko" menes hvor stor risiko *virksomheten* kan akseptere for at det inntreffer en hendelse som kan forårsake brudd på *konfidensialitet*, *tilgjengelighet* eller *integritet* for *helse- og personopplysninger*.

3.1.6 Oversikt over behandlinger av helse- og personopplysninger

Virksomheten skal til enhver tid ha oversikt over hvilke *behandlinger* av *helse- og personopplysninger* som skjer i *virksomheten.*

Oversikten over *behandlinger* bør inneholde følgende informasjon:

- formålene med *behandlingen* (overordnet, for eksempel: timeliste, regnskap, diagnostikk, helsehjelp, plikt til å føre journal mv.)
- kategorier av *helse- og personopplysninger* (sensitive/ikke-sensitive)
- daglig ansvar (person i *virksomheten* som har ansvaret eller som har fått oppgaver delegert til seg)
- navn på *fagsystem*/typebetegnelse (leverandørnavn mv.) som benyttes til *behandlingen*
- *meldeplikt* (utført/ikke-utført, informasjon om fornyelse hvert tredje år, ansvar mv.)
- evt. *databehandler* (navn, kontaktinformasjon, avtaleforhold mv.)

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

Nærmere om *meldeplikten*
I tannhelsetjenesten skal alle *behandlinger* av *helse- og personopplysninger* meldes til Datatilsynet før *behandlingen* tar til. Når det skjer endringer i behandlingsmåten, skal det sendes en endringsmelding. Innsendte meldinger skal fornyes etter 3 år.

Alle meldinger sendes inn via Datatilsynets nettsted, www.datatilsynet.no.

Det er *databehandlingsansvarlig* som har ansvaret for å melde (jfr. avsnitt 3.1.1 - Ansvar).

3.2 GJENNOMFØRENDE DEL

3.2.1 Tilgangsstyring, autorisasjon og autentisering

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

Tilgang skal tildeles medarbeiderne etter hvilke roller og arbeidsoppgaver de har. Medarbeiderens rolle skal ikke alene gi *tilgang* til *helse- og personopplysninger* og bruk av *informasjonssystemene*. *Tilgangen* som gis skal være basert på et konkret tjenstlig behov (arbeidsoppgaver).

Tilgangsstyringen må derfor ta utgangspunkt i hvordan den enkelte *virksomheten* konkret er organisert (jfr. avsnitt 3.1.1), og *tilgangen* må avpasses etter forholdene i *virksomheten*. F.eks. må sekretæren til tannlegen ofte håndtere røntgenbilder, lese eller på annen måte fremskaffe informasjon i løpet av en behandlingsseanse. Tannlegen kan også la sekretæren føre journal etter diktat under behandlingsseansen. Prosedyrene som beskriver tilgangsrettighetene skal speile denne praksisen i *virksomheten*.

Virksomhetene har vide muligheter til å organisere seg i tråd med egne forutsetninger og behov. Momenter som vil kunne påvirke den konkrete tilgangsstyringen er bl.a.:

- størrelsen på praksisen (mange tannlegepraksiser er på 3-5 tannleger med tillegg av hjelpepersonell, men det finnes en del praksiser med én tannlege og én sekretær, og kanskje bare én PC)
- organisasjonsform (jfr. 3.1.1)
- bruk av *databehandler*, f.eks. ved at en tredjepart drifter og lagrer journalopplysninger
- *leverandør* av journalsystem, der *leverandøren* har *fjernaksess*
- *nødrettstilgang*

Autentiseringen skal uansett være forholdsmessig ut fra *virksomhetens* størrelse og virkefelt. Hvilke interne prosedyrer for *autentisering virksomheten* etablerer, bør være basert på en risikovurdering på en slik måte at risikovurderingen viser begrunnelsen for den etablerte tilgangstyringen. *Virksomheten* bør utarbeide en oversikt som viser *tilgangene* per rolle.

Tabellen nedenfor viser et eksempel på *tilganger* per rolle.

	Opprette pasientjournal	Full lese/skrive *tilgang* for egen pasient	Redigere timebok	Sende og motta SMS	Tidsavgrenset *tilgang* til en pasients journal	*Tilgang* til å sperre journal på en pasient	Registrere grunnlag for å gi an annen tannlege *tilgang*	Registre røntgenbilder
Tannlege	X	X	X	X	X	X	X	X
Assistenttannlege	X	X	X	X	X	X	X	X
Kontraktørtannlege	X	X	X	X				X
Tannpleier	X		X	X	X			X
Tannhelsesekretær	X		X	X				X
Tannlegesekretær			X					

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.

For å motvirke at en *tilgang* til informasjonssystemet misbrukes, skal den enkelte bruker *autentiseres*, i praksis ved hjelp av passord eller *PKI*.

I utgangspunktet tillater ikke pasientjournalloven at personell utenfor *virksomhetens* (*den databehandlingsansvarliges*) instruksjonsmyndighet har *tilgang* til *virksomhetens helse- og personopplysninger*. Loven åpner imidlertid for at to eller flere virksomheter kan inngå avtale om føring av felles journal. Det er da viktig å merke seg at loven oppstiller visse krav til avtalens innhold og at den felles journalen erstatter den virksomhetsinterne journalen.

Pasientjournalloven og helsepersonelloven slår fast forbudet mot snoking i pasientjournalen, presisert på den måten 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.

3.2.2 Pasientinformasjon og informert samtykke

Når *virksomheten* registrerer *helse- og personopplysninger* skal *den registrerte* være informert om at registreringen skjer. Bare ved å være informert om registreringen, vil *den registrerte* være i stand til å ivareta sine rettigheter. *Den registrerte* skal ha informasjon om sine rettigheter knyttet til samtykke, reservasjon, innsyn, retting og sletting.

Virksomheten kan gi informasjonen ved oppslag på kontoret, i brev til pasienten eller i en brosjyre.

Virksomheten har som hovedregel bare rett til å behandle opplysninger dersom *den registrerte* samtykker til det. Det kreves ikke samtykke for å opprette en pasientjournal.

Likevel følger det av en rekke rettsregler at *virksomheten* kan behandle *helse- og personopplysninger* uten samtykke. *Virksomheten* skal behandle *helse- og personopplysninger* uten samtykke når det føres pasientjournal. *Den registrerte* kan ikke motsette seg at *helse- og personopplysninger* blir journalført hvis helsehjelpen mottas; personellets journalføringsplikt går foran den enkeltes individuelle rett til å samtykke til eller nekte registreringen.

I andre situasjoner enn ved føring enn pasientjournal, er det krav til informert samtykke (for eksempel utplukk av pasienter for vaksine, forskning mv).

Ofte vil samtykket være stilletiende. At pasienten oppsøker *virksomheten* vil bli oppfattet som at vedkommende godtar at de opplysningene som er nødvendig kan registreres.

At samtykket er "informert" betyr at det foreligger en frivillig, uttrykkelig og informert erklæring fra *den registrerte* om at han eller hun godtar *behandling* av opplysninger om seg selv. Loven stiller ikke noe krav om at et informert samtykke skal foreligge skriftlig.

I enkelte sammenhenger, spesielt der *den registrerte* mangler samtykkekompetanse, er det de pårørende eller verge/hjelpeverge som må samtykke på vegne av *den registrerte*.

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

3.2.3 Innsynsretten

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

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, legemiddel- og cardexkort, pleieplaner og andre skriftlige nedtegnelser. Alle former for journal omfattes av innsynsretten, både papir- og IKT-baserte journaler (*EPJ*).

3.2.4 Retting og sletting av pasientopplysninger, herunder oppbevaring av pasientjournal

Den registrerte kan i en rekke sammenhenger kreve at feil i *helse- og personopplysningene* om vedkommende, blir rettet eller slettet. F.eks. følger det av pasient- og brukerrettighetsloven at *den registrerte* kan 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, skal opplysningen korrigeres evt. supplert med ny journalføring slik at informasjonen samlet sett gir et mest mulig riktig bilde. Retting kan ikke skje ved at opplysninger slettes. Etter gitte vilkår kan opplysningene slettes. Utfyllende regler om retting og sletting finnes i pasientjournalforskriften.

3.2.5 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 med *helse- og personopplysninger* mv.). Sikringen har som formål å hindre at uautoriserte får *tilgang*.

Konkret bør *virksomheten* utarbeide prosedyrer for daglig sikring av kontordører/-vinduer (låsing, alarmsystemer), resepsjonsområde, PC-er, printere, telefakser, kopimaskiner, bærbare datamaskiner mv. *Virksomheten* skal sikre at utskrifter ikke kommer på avveie. Dokumenter som inneholder *helse- og personopplysninger*, og som ikke skal tas vare på, skal slettes fullstendig, helst ved makulering.

3.2.6 Sikkerhet i nettverket og datautstyret

Konfigurasjonskontroll
Virksomheten skal gjennom konfigurasjonskontroll ha oversikt over alt utstyr og programvare som benyttes i *behandlingen* av *helse- og personopplysninger*.

Dokumentasjonen skal inneholde et konfigurasjonskart / tekstlig beskrivelse med:

- sikkerhetsbarrierer (for eksempel brannmur)
- hvor eventuelle servere er plassert
- hvor *EPJ-systemet* / røntgensystemet er plassert
- plassering av arbeidsstasjoner og skrivere
- plassering av betalingsterminal(er)
- Internettilknytning (gitt at gjeldende sikkerhetskrav ivaretas)
- eventuell tilknytning til helsenettet

Konfigurasjonsendringer, dvs. endringer i utstyr og/eller programvare, skal ikke settes i drift før følgende tiltak er gjennomført:

- risikovurdering som viser at nivå for akseptabel risiko oppfylles
- 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

Sikkerhetskopiering

Virksomheten skal sikkerhetskopiere *helse- og personopplysninger* etter en fastsatt prosedyre. I tillegg skal oppsett av *EPJ-systemet*, røntgensystemet, servere mv. sikkerhetskopieres jevnlig slik at hele informasjonssystemet kan tilbakekopieres.

Sikkerhetskopiene bør oppbevares adskilt fra det utstyret som er sikkerhetskopiert, og skal én gang i uken bringes fysisk ut av *virksomheten* og oppbevares sikret (safe, bankboks, låsbart skap).

Beskyttelse mot ondsinnet programvare

Virksomheten skal sørge for at datamaskinene i *virksomheten* har installert en løsning for å hindre ondsinnet programvare.

Programvaren skal være 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*.

Lagres *helse- og personopplysninger* på fysisk adskilt utstyr er behovet for sikring mot ondsinnet programvare mindre.

Mobilt utstyr

Eksempler på mobilt utstyr er PC, PDA, mobiltelefoner mv. Om det lagres *helse- og personopplysninger* på det mobile utstyret skal data krypteres iht. gjeldende krav.

Det mobile utstyret skal sikres med *autentisering* (for eksempel passord) for å hindre uautorisert *tilgang* mv. på samme måte som stasjonært utstyr i *virksomheten*.

Utfasing av utstyr

Ved utfasing av utstyr (for eksempel kopimaskin, telefaks, multifunksjonsskriver, PC, server mv.) skal *virksomheten* påse at *helse- og personopplysninger* blir slettet slik at opplysningene ikke kan gjenskapes. Vanlig sletting av datafiler og formatering er ikke tilstrekkelig. Et godkjent sletteprogram skal benyttes, alternativt kan lagringsmediene ødelegges fysisk.

Oversikt over godkjente sletteprogram finnes på hjemmesiden til Nasjonal sikkerhetsmyndighet www.nsm.stat.no.

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

3.2.7 Hendelsesregistrering

Virksomheten skal ha etablert *hendelsesregistrering* og prosedyre for kontroll av *hendelsesregistre*, slik at den har kontroll med aktiviteten i informasjonssystemet. Dermed kan *avvik* oppdages. Følgende hendelser skal som et minimum registreres:

- tildeling av *tilganger*
- bruk av *tilganger*
- uautorisert eller forsøk på uautorisert bruk av *tilganger*
- bruk av *nødrettstilgang* (blålysfunksjon)

Det skal etableres prosedyrer for å analysere *hendelsesregistrene* slik at hendelser oppdages før de får alvorlige konsekvenser, og fortrinnsvis innen 1 uke.

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

3.2.8 Hjemmekontor

Med *hjemmekontor* menes teknisk løsning 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.

Det anbefales følgende tekniske krav til den tekniske løsningen:
- Terminalserverløsning er anbefalt og skal fortrinnsvis benyttes, fordi kravet til at data ikke skal lagres lokalt på PC-en automatisk da blir ivaretatt
- Kommunikasjonen skal være kryptert.
- Ved bruk av VPN må hjemme-PC/utstyr og kommunikasjonspart i andre enden konfigureres slik at begge parter er den som de gir seg ut for å være
- VPN-løsning uten bruk av terminalserver kan benyttes men er ikke anbefalt. Hvis dette likevel benyttes skal utstyr konfigureres og nødvendige mekanismer iverksettes for å sikre at lokal lagring av *helse- og personopplysninger* ikke er mulig

3.2.9 Opplæring og kompetanse

Virksomhetens ledelse 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 kompetanse slik at de kan ivareta et godt og hensiktsmessig personvern etter gjeldene krav. Gode opplæringstiltak vil bl.a. bidra til at ledere og medarbeiderne:

- forstår hensikten med og blir i stand til å sikre personvernet
- blir bevisste på krav i *Normen* og i denne veilederen (inkludert malen for internkontroll)

- blir oppmerksom på ansvarsforhold med hensyn til informasjonssikkerhet

3.2.10 Tekniske løsninger for ekstern datakommunikasjon

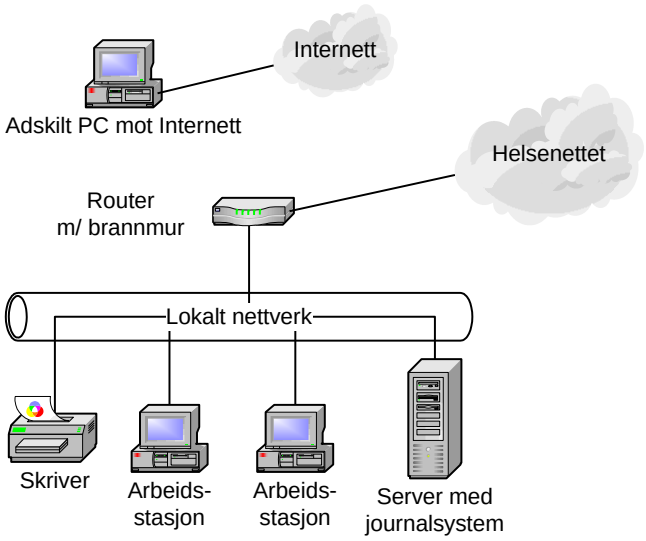
Tilkobling til eksterne datanettverk skal sikres med to uavhengige tekniske virkemidler der det er *helse- og personopplysninger*. Nedenfor vises fire ulike eksempler på tekniske løsninger.

1. Lokalt nettverk med tilkobling til helsenettet for å sende rekvisisjoner og henvisninger og motta laboratoriesvar. Adskilt PC for tilgang til Internett.

Journal- og pasientadministrative systemer driftes lokalt på eget nettverk (server) og det er kun behov for ekstern kommunikasjon for å motta laboratoriesvar via helsenettet. Løsningen har lav risiko og krever få tekniske sikkerhetstiltak. Ofte er det tilstrekkelig med sikkerhetsløsning levert av maskin- og programvareleverandør inklusive sikkerhetskopiering og løsning for tilkobling til helsenettet. *Tilgang* til Internett er løst med en adskilt PC.

Fordeler: Ingen trusler utenfra. Er det tillatt med minnepinner etc., er det nødvendig med antivirus-program.

Ulemper: To tekniske løsninger som krever forskjellig vedlikehold.

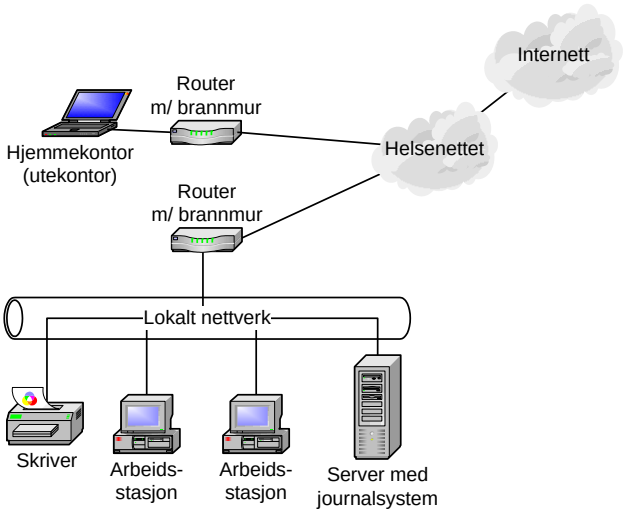


2. Som 1, men tilkoblet Internett via helsenettet og *hjemmekontor* (mobilt kontor) via helsenettet

Som eksempel 1, men nettverket er i tillegg koblet til helsenettet med Internett og *hjemmekontor* (mobilt kontor). Løsningen har høyere risiko og krever sikring slik at det ikke opprettes gjennomgående forbindelser fra Internett ved at det er to uavhengige sikkerhetsbarrierer mellom nettverk og Internett, at all kommunikasjon initieres innenfra og ut og at trafikken overvåkes. Det må etableres teknisk løsning for *tilgang* til Internett som hindrer uautorisert utlevering av *helse- og personopplysninger* (for eksempel ved bruk av tynne klienter og terminalserver).

Fordeler: Mulig å kommunisere med eksterne *virksomheter*.

Ulemper: Krever kompetent bistand for oppsett og drift av løsningen.

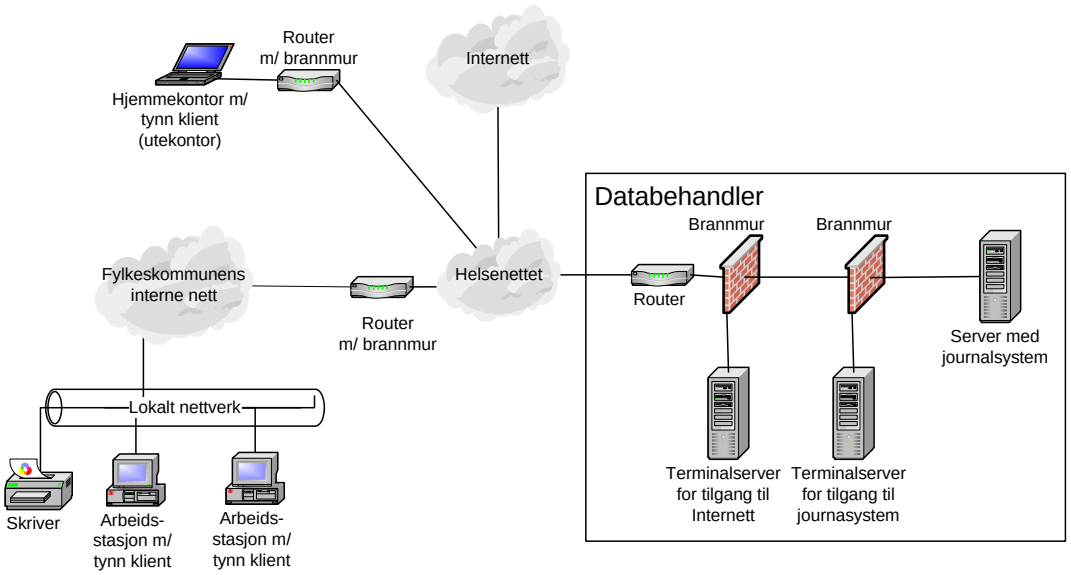


3. Servere plassert hos *leverandør* og all kommunikasjon går via helsenettet. Internett nås via helsenettet

Virksomheten benytter *databehandler* for drift av servere. All kommunikasjon går via helsenettet inklusive *hjemmekontor* (mobilt kontor) og Internett. Helsenettet tilbyr kontrollerte tjenester (Internett-*tilgang*, viruskontroll) og sikkerhetsmekanismer i helsenettet kan ses på som en sikkerhetsbarriere mot eksterne nettverk. Ved at *virksomheten* oppretter en egen barriere er kravet til to uavhengige barrierer ivaretatt.

Fordeler: Kun én kommunikasjonspart å forholde seg til.

Ulemper: Krever kompetent bistand for oppsett og drift av løsningen. Avhengig av helsenettet for å nå egne systemer.

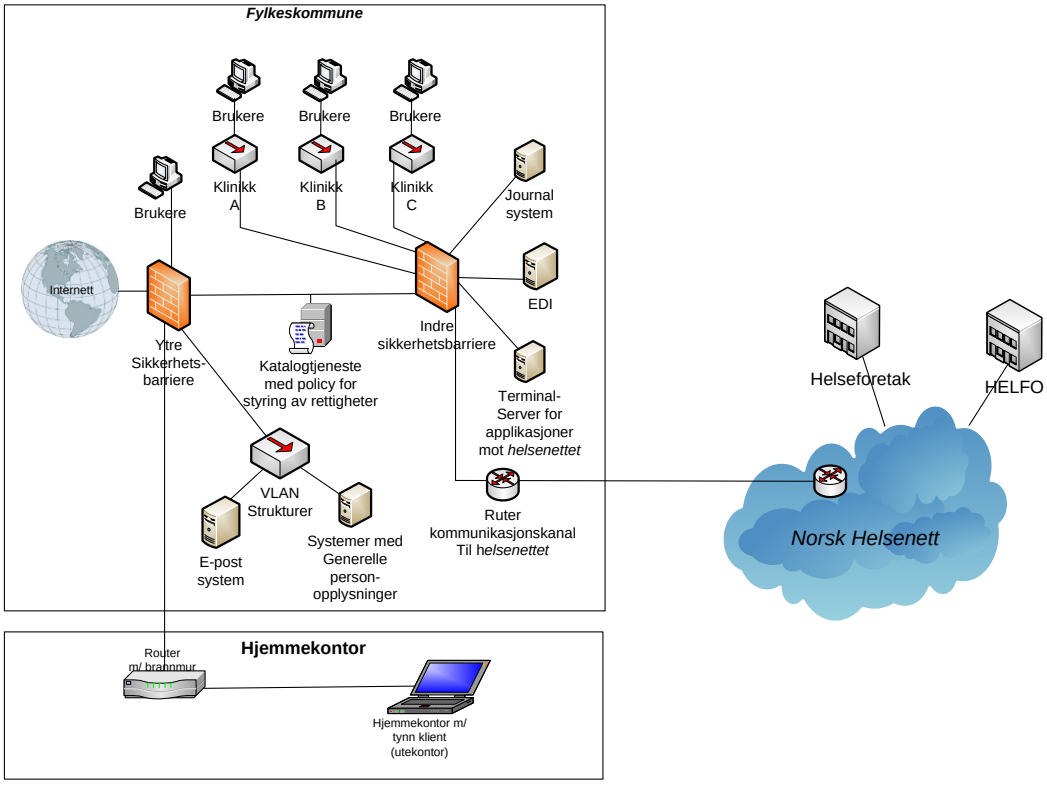


4. Alle løsningene er plassert i og håndteres av virksomheten

Virksomheten står selv for drift av alle sikkerhetsløsninger, nettverk og servere. Helsenettet benyttes til meldingsformidling.

Fordeler: Større *virksomheter* har kompetanse og omfang tilstrekkelig til å ivareta all sikkerhet selv.

Ulemper: Krever kompetent bistand for oppsett og drift av løsningen.



3.2.11 Bruk av SMS og e-post

SMS kan benyttes i kommunikasjonen mellom pasient og *virksomheten*, særlig i forbindelse med innkalling til / påminnelse om konsultasjoner. I den anledning er det viktig å etablere løsninger som ikke benyttes til overføring av informasjon som bryter med kravet til personvern og informasjonssikkerhet.

Det kan være hensiktsmessig å innkalle *den registrerte* til time etc. ved hjelp av SMS eller e-post. Meldingen skal ikke inneholde:

- fødselsnummer (11 siffer)
- helseopplysninger
- reseptinformasjon

Virksomheten som benytter løsningen er ansvarlig og skal påse at krav til informasjonssikkerhet ivaretas. *Leverandør* og eventuell tjenesteyter er kun ansvarlig for at deres løsning fungerer som avtalt.

Virksomheten skal ikke bruke e-post til overføring av *helseopplysninger*.

Om *virksomheten* benytter e-post til bestilling av for eksempel tannteknisk arbeid fra *leverandør* skal pasienten identifiseres med for eksempel journalnummer eller et løpenummer.

3.2.12 Avtaler

Virksomheten må inngå og administrere de avtaler som er nødvendige i sammenheng med informasjonssikkerheten.

Databehandler
Hvis *virksomheten* benytter en *databehandler*, er det lovpålagt at partene innegår en skriftlig avtale (databehandleravtale). Det må klargjøres hvem som er *databehandlingsansvarlig* og hvem som er *databehandler*. Utgangspunkt for en slik avtale finnes i malen for internkontroll til denne veilederen, og på www.datatilsynet.no.

Øvrige *leverandører*
Hvilke *leverandører virksomheten* inngår avtale med, avhenger av spesialisering, hvilket marked *virksomheten* retter seg mot, *virksomhetens* interne kompetanse mv. Følgende kan være aktuelle avtaler, og *virksomheten* må oppfylle informasjonssikkerhetskravene i sammenheng med dem:

- *leverandør* av *EPJ-system* og pasientadministrative systemer
- kjøp / bestilling av tannteknisk arbeid (både fra *leverandører* i Norge og i utlandet (i og utenfor EU-/EØS-området)).
- avtaler om *fjernaksess* for sikkerhetsleverandører (jfr. "Veileder for fjernaksess for vedlikehold og oppdateringer mellom *leverandør* og helsevirksomhet")
- avtaler med eksterne røntgenleverandører

3.2.13 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 ratifisert EUs personverndirektiv. Opplysninger om dette finnes på www.datatilsynet.no.

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

3.3 KONTROLLERENDE DEL

I kontrollerende del beskrives ulike kontrolltiltak for å verifisere at etablert informasjonssikkerhet virker etter hensikten.

3.3.1 Sikkerhetsrevisjon

Arbeidet med informasjonssikkerheten i *virksomheten* er en kontinuerlig prosess. For å sikre at *virksomheten* er på høyde i informasjonssikkerhetssammenheng, er det stilt krav om at *virksomheten* jevnlig, og minimum årlig, skal gjennomføre en sikkerhetsrevisjon.

Omfanget av sikkerhetsrevisjonen må tilpasses *virksomhetens* størrelse og behov. Sikkerhetsrevisjonen må likevel, som et minimum, omfatte en vurdering av organiseringen i *virksomheten*, sikkerhetstiltakene og bruken av kommunikasjonspartnere og *leverandører*.

Formålet med å gjennomføre sikkerhetsrevisjon er å:

- 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

3.3.2 Fornyelse av meldeplikten

Det er krav om at de meldingene som *virksomheten* er pliktige til å sende til Datatilsynet, skal fornyes hvert tredje år. Fornyelsesmeldingen sendes via Datatilsynets hjemmeside (på samme måte som den opprinnelige meldingen), www.datatilsynet.no. *Virksomhetens* ledelse må påse at slik fornyelse finner sted, gjerne ved at meldinger legges inn som et fast punkt i sikkerhetsrevisjonen (se pkt. 3.3.1).

3.3.3 Risikovurdering

Behandlingene og informasjonssystemene skal risikovurderes opp mot nivå for akseptabel risiko. Om risikovurderingen viser uakseptabel risiko, skal *behandlingen* ikke gjennomføres før risikoreduserende tiltak er iverksatt**.**

Gjennom risikovurderingen må *virksomheten* vurdere hensynet til personvernet 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. Ut fra risikovurderingen må *virksomheten* iverksette tiltak ut fra prinsippene om forholdsmessig sikring.

Med utgangspunkt i nivå for akseptabel risiko skal *virksomheten* gjennomføre en risikovurdering før informasjonssystemet tas i bruk, ved større endringer eller om det oppstår vesentlige *avvik*.

Følgende momenter kan være aktuelle å risikovurdere*:*

- uautorisert *tilgang* til og bruk av informasjonssystemet (for eksempel ved manglende eller for svake passord)
- tilgangsstyringen er for svak slik at uautoriserte får *innsyn* i journaler
- manglende tilgangsstyring i røntgensystemet
- uautoriserte (for eksempel pasienter) får innsyn i *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 bortlåning av ID 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

Se eksempel på en risikovurdering i kapittel 4.2.

3.3.4 Avvikshåndtering

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

Formålet med avviksbehandling er å:

- håndtere sikkerhetsbrudd på en systematisk måte
- gjenopprette normaltilstanden etter et sikkerhetsbrudd
- vurdere endringer i sikkerhetsarbeidet for å hindre framtidige sikkerhetsbrudd
- sikre at Datatilsynet varsles ved uautorisert utlevering av *helse- og personopplysninger*

3.3.5 Ledelsens gjennomgang

Fordi personvern og informasjonssikkerhet er et ledelsesansvar, er det stilt krav om at ledelsen jevnlig, og minimum årlig, gjennomgår sentrale forhold som angår sikkerheten i *virksomheten*.

Ledelsens gjennomgang kan med fordel gjennomføres i sammenheng med kvartalsvis/halvårlig/årlig økonomi- eller virksomhetsplanlegging. Ledelsens gjennomgang skal gjennomføres i henhold til en møteplan som er utarbeidet på forhånd. Formålet med ledelsens gjennomgang er å avdekke om sikkerheten ivaretas i henhold til mål, strategier og prosedyrer og beslutte handlingsplaner for det videre sikkerhetsarbeidet.

4 VEDLEGG

4.1 Tabell med referanse kapittel og faktaark

Kapittel Nr		Faktaark
	Styrende del	
3.1.1	Ansvar	1
3.1.2	Styringssystem for informasjonssikkerhet	2 og 3
3.1.3	Sikkerhetsmål	
3.1.4	Sikkerhetsstrategi	
3.1.5	Nivå for akseptabel risiko	5
3.1.6	Oversikt over behandlinger av helse- og personopplysninger	4
	Gjennomførende del	
3.2.1	Tilgangsstyring, autorisasjon og autentisering	14 og 31
3.2.2	Pasientinformasjon og informert samtykke	
3.2.3	Innsynsretten	
3.2.4	Retting og sletting av pasientopplysninger, herunder oppbevaring av pasientjournaler	25
3.2.5	Fysisk sikring av områder og utstyr	17
3.2.6	Sikkerhet i nettverket og datautstyret	19, 21, 30 og 34
3.2.7	Hendelsesregistrering	15
3.2.8	Hjemmekontor	29
3.2.9	Opplæring og kompetanse	9
3.2.10	Tekniske løsninger for ekstern datakommunikasjon	26, 28 og 36
3.2.11	Bruk av SMS og e-post	
3.2.12	Avtaler	10
3.2.13	Overføring av helse- og personopplysninger til utlandet	
	Kontrollerende del	
3.3.1	Sikkerhetsrevisjon	6
3.3.2	Fornyelse av meldeplikten	
3.3.3	Risikovurdering	7
3.3.4	Avvikshåndtering	8
3.3.5	Ledelsens gjennomgang	

4.2 Eksempel på risikovurdering

EKSEMPEL PÅ RISIKOVURDERING

Virksomhet: Tannhelse DA	
Vurdert av: **Ola Norman**	**Dato: 4.10.2009**
Formålet med risikovurderingen:	Etablering av nytt EPJ-system

	Forhold som er vurdert (uønsket hendelse / senario)	**Sannsynlighet**				**Konsekvens**				**Risikonivå**	**Tiltak Alltid Ja på Høy**
		1 = Usannsynlig	2 = Mindre Sannsynlig	3 = Mulig	4 = Sannsynlig	1 = Ubetydelig	2 = Moderat	3 = Alvorlig	4 = Kritisk		
1.	*Uautorisert tilgang* til og bruk av informasjonssystemet (for eksempel ved manglende eller for svake passord)	☐ 1	☐ 2	☒ 3	☐ 4	☐ 1	☐ 2	☒ 3	☐ 4	☐Lavt ☐Middels ☒Høy	☒Ja ☐Nei
2.	Tilgangsstyringen er for svak slik at ikke *autoriserte* får innsyn og kan gjøre endringer i journaler	☐ 1	☒ 2	☐ 3	☐ 4	☐ 1	☒ 2	☐ 3	☐ 4	☒Lavt ☐Middels ☐Høy	☐Ja ☒Nei
3.	Uautoriserte (for eksempel pasienter) får innsyn i *helse- og personopplysninger* fra skjermer eller utskrifter	☐ 1	☐ 2	☐ 3	☒ 4	☐ 1	☐ 2	☒ 3	☐ 4	☐Lavt ☐Middels ☒Høy	☒Ja ☐Nei
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	☐Lavt ☒Middels ☐Høy	☐Ja ☒Nei
5.	Risiko knyttet til bortlåning av ID og passord og dermed feil ved signering av journaler	☐ 1	☒ 2	☐ 3	☐ 4	☒ 1	☐ 2	☐ 3	☐ 4	☒Lavt ☐Middels ☐Høy	☐Ja ☒Nei
6.	At data kan tilbakekopieres fra sikkerhetskopier om data blir slettet eller blir inkonsistente	☐ 1	☐ 2	☐ 3	☒ 4	☐ 1	☐ 2	☒ 3	☐ 4	☐Lavt ☐Middels ☒Høy	☒Ja ☐Nei

	Beskrivelse av tiltak *(Nr 1 har høyest prioritet)*	**Betydning/ Kommentar**	**Ref linje nr over**
1.	Etablere løsning for daglig sikkerhetskopi med kontroll av at sikkerhetskopiering er gjennomført. Bringe sikkerhetskopier til et sikkert sted	Bestille løsning hos *leverandør* med oppsatt av en daglig prosedyre	6
2.	Plassere skjermer og skrivere slik at pasienter ikke får innsyn fra venterommet og når de skal betale i skranke	Ommøblering	3
3.	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	1

4.3 Referanser

Relevante nettsteder og dokumenter:

- Hjemmeside til *Normen*: www.normen.no
- Hjemmeside til Den norske tannlegeforening: www.tannlegeforeningen.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

4.4 Deltagere i utarbeidelse av veilederen

Navn	Rolle / stilling	Virksomhet
Helle Nyhuus	Tannlege	ADB Oslo Private tannlegevakt AS
Geir Grønlund	Tannlege	Egen virksomhet
Øyvind Asmyhr	Tannlege / rådgiver	Den norske tannlegeforening
Frank Ulfsby Eriksen	Overingeniør	Datatilsynet
Peter Bonne	Rådgiver	Pharos AS
Alf Marcus Wiegaard	Advokat	Advokatfirmaet Wiegaard
Knut Henrik Andersen	Daglig leder	INCERTUS
Jan Henriksen	Rådgiver	INFOSEC Norge AS
Tor Ottersen	Seniorrådgiver	Helsedirektoratet
Anita Lindholt	Ekstern konsulent	Helsedirektoratet
Eirik Mangseth	Seniorrådgiver	Helsedirektoratet