NORMEN

Veileder for små helsevirksomheter

Versjon 1.1

17. september 2020

Utgitt med støtte av:

Direktoratet for e-helse

Endringshistorikk for og godkjenning av dokumentet

Versjon	Endringer	Godkjent av styringsgruppen for *Normen* (dato)
1.0	Første utgave av veilederen	14.november 2019
1.1	Veilederen supplert med gjennomgående eksempel	17.september 2020

Innledning

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) skal gjøre det enklere for dataansvarlige og helsepersonell i små virksomheter å kjenne til og forstå hvilke krav til informasjonssikkerhet og personvern, som gjelder for dem.

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. Normen samler alle krav og plikter til personvern og informasjonssikkerhet (se Normen).

Veiledere er tilpasset ansvarlig ledelse i små helsevirksomheter, med bakgrunn i Normens krav

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

- 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?

Det er virksomhetens ledelse som er dataansvarlig for at informasjonssikkerhet og personvern ivaretas. Det vil si at den dataansvarlige skal sørge for at:

- kravene til konfidensialitet, integritet, tilgjengelighet og robusthet blir ivaretatt
- taushetsplikten ivaretas i virksomheten
- pasientens rettigheter blir ivaretatt

Målgruppe
Små virksomheter og enkeltpersonforetak i helse og omsorgssektoren.
Den er primært rettet mot personell med ansvar, oppgaver og roller i forbindelse med personvern og informasjonssikkerhet

Formål
Bidra til tydeligere og mer tjenestetilpassede krav for små virksomheter i helse og omsorgssektoren
Veilederen skal gi den som har det overordnede ansvaret for virksomheten, et godt verktøy for:

- å kunne ha god systematisk styring og ledelse
- å få hjelp til å prioritere
- å aktivt jobbe kontinuerlig med forbedring
- at krav i helse- og omsorgslovgivningen etterleves.

INNHOLD

1. Om Normen

Normen skal bidra til tilfredsstillende informasjonssikkerhet og personvern 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 og personvern.

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

Normen er til for alle virksomheter som ved avtale har forpliktet seg til å følge Normen – i praksis de fleste av sektorens mer enn titusen virksomheter, deres leverandører og databehandlere

Normen styres av en bredt sammensatt styringsgruppe. Det daglige arbeidet koordineres av sekretariatet, som er plassert i Direktoratet for e-helse med fast representasjon fra Norsk Helsenett

2. Viktige begreper

Se Normens definisjonskapittel for gjeldende definisjoner til slutt i dokumentet.

Dataansvarlig er virksomheten som bestemmer formålet (hva helse- og personopplysningene skal brukes til) med behandlingen, og hvilke hjelpemidler som skal brukes (hvilke systemer som tas i bruk). Ansvaret skal ivaretas av den daglige ledelsen av virksomheten, og virksomheten er pliktsubjekt.

Databehandler er den virksomheten som behandler helse- og personopplysninger på vegne av dataansvarlig.

Helseopplysning
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).

Personopplysning
En personopplysning er enhver opplysning om en identifisert eller identifiserbar person. For eksempel: Navn, personnummer, telefonnummer og adresse.

Sensitive / særlig kategorier personopplysninger
Opplysninger om:

- rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning
- fagforeningsmedlemskap
- genetiske opplysninger
- biometriske opplysninger
- helseopplysninger
- opplysninger om en fysisk persons seksuelle forhold seksuelle orientering

Behandling av personopplysninger
Alt som gjøres med disse, inkludert innsamling, oppbevaring, tilgjengeliggjøring, bruk, endring, utlevering og tilintetgjøring. De fleste personopplysningene små virksomheter i sektoren behandler, vil være lovpålagte behandlinger som følge av helsepersonellovens plikt til å føre journal.

Personvernforordningen - GDPR
EUs nye personvernforordning ble norsk lov i 2018. Regelverket styrker rettighetene til de registrerte (de personene det behandles personopplysninger om) og gir plikter til alle som behandler personopplysninger.

Leverandør
En juridisk enhet som yter tekniske og/eller administrative tjenester til virksomheten. Eksempler er EPJ-leverandør, røntgenleverandør, leverandør av løsning for SMS-meldinger, IT-leverandør m. flere

Virksomhet
Juridisk enhet som helseforetak, kommune, sykehus, legepraksis, tannklinikk, apotek, fysioterapeuter, psykologer, kiropraktorer, røntgeninstitutt m flere.

3. Informasjonssikkerhet og personvern

3.1. Informasjonssikkerhet

Informasjonssikkerhet handler om å håndtere risiko relatert til informasjon og behandling av personopplysninger. Informasjonens integritet, tilgjengelighet og konfidensialitet skal sikres. God informasjonssikkerhet er viktig for å kunne utøve forsvarlige helsetjenester.

- Med integritet menes i Normen at helse- og personopplysninger må være sikret mot utilsiktet eller uautorisert endring eller sletting. Integritet er en forutsetning for god og forsvarlig helsehjelp.
- 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. Tilgjengelig informasjon for helsepersonell er en forutsetning for god og forsvarlig helsehjelp.
- Med konfidensialitet menes i Normen at helse- og personopplysninger må være sikret mot at uvedkommende får kjennskap til opplysningene. Konfidensialitet bidrar til ivaretakelse av taushetsplikt og personvern, noe som er viktig for innbyggernes tillit til helse- og omsorgstjenesten.
- Med robusthet menes i Normen organisasjonens og informasjonssystemenes evne til å gjenopprette normaltilstand etter for eksempel en fysisk eller teknisk hendelse. Dette oppnås gjennom egnede tekniske og organisatoriske tiltak som muliggjør forebygging, deteksjon, skalerbarhet, håndtering og gjenoppretting av personopplysningssikkerheten og informasjonssikkerheten for øvrig

Avvik fra dette kan skade både pasienten direkte og helsepersonellets, virksomhetens og helsevesenets omdømme. Det kan skade tilliten mellom pasienten og virksomheten som behandler vedkommende, som er grunnleggende for å kunne oppnå god pasientbehandling.

3.2. Taushetsplikten i helse og omsorgssektoren

Personell i helse- og omsorgssektoren er pålagt en omfattende taushetsplikt. Taushetsplikten skal verne om pasientens personvern og integritet, sikre befolkningens tillit til helse- og omsorgstjenesten og sikre kvalitet i helse- og omsorgssektoren.

Les mer om taushetsplikt på Helsedirektoratets sider.

3.3. Personvern for små helsevirksomheter

For å gi god og forsvarlig helsehjelp er det nødvendig å håndtere store mengder personopplysninger om enkeltindivider. Disse opplysningene omhandler personlige og sensitive forhold og er avgjørende for helsehjelpens kvalitet.

Å behandle disse personopplysningene om pasienter og brukere på en trygg måte, er avgjørende for å sikre tillit. Helsetjenesten er avhengig av tillit fra både pasienter, brukere, helsepersonell og befolkningen for øvrig. Pasienter, brukere og pårørende må ha tillit for å

våge å gi helsetjenesten sine personopplysninger, av og til svært intim og personlig informasjon. Uten disse kan det ikke gis helsehjelp av god kvalitet.

Tiltak for å sikre personopplysninger har stort fokus i lovgivningen. Tiltakene skal være "egnede". Ved valg av egnede tekniske og organisatoriske tiltak skal virksomheten vurdere tiltakene i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv.

Dette kommer særlig til uttrykk i vurderingen av , arbeidsoppgaver, kontrolloppgaver og tiltak innen informasjonssikkerhet (for eksempel tilgangsstyring, logging, fysisk sikring, beredskap mv.).

Regelverket om beskyttelse av personopplysninger bygger på noen grunnleggende prinsipper for behandling av personopplysninger. Disse kan du lese mer om i kap xx i Normen og på Datatilsynet.no Virksomheten er ansvarlig for å opptre i henhold til personvernprinsippene og dokumentere at virksomheten har gjennomført tiltak for å etterleve personopplysningsregelverket.

Normen har laget en oversikt over noen av de viktigste kravene som skal ivaretas, tilpasset små helsevirksomheter.

Velkommen til Normland Helsesenter!
Helsesenteret består av tre behandlende helsepersonell. Disse er daglig leder Lena, Frank, sykepleier Simen, og de merkantilt ansatte Maren og Morten. Renholder Renate er ansatt i en mindre stillingsbrøk. Det behandlende helsepersonellet er egne juridiske enheter, men bruker helsesenteret som kontorfellesskap der de deler lokaler, sykepleier og merkantilt ansatte. Lena og Frank har felles journalsystem.

Helsesenteret har et enkelt internkontrollsystem basert på Word og Excel, lagret på filserver.

3.4. Oversikt over behandling av helse- og personopplysninger

Alle virksomheter må ha oversikt over hvilke personopplysninger som behandles. Dette er viktig bl.a. for å ha kontroll på om virksomheten faktisk har lov til å behandle opplysningene og for å kunne vise at den har tiltak som er hensiktsmessige for å ivareta det ansvaret virksomheten har.

Som et ledd i å holde oversikt og kontroll med personopplysningene krever loven at virksomheten har en skriftlig oversikt. I personopplysningsloven kalles dette "Protokoll over behandlingsaktiviteter". Oversikten skal inneholde et minimum av opplysninger. ¨

Les mer om dette i protokoll over behandlinger av helse- og personopplysninger i virksomheten (faktaark 13). Faktaarket inneholder også en mal for en slik oversikt.

Normland Helsesenter sin oversikt over behandling av helse- og personopplysninger er basert på eksemplet som finnes som vedlegg til Normens faktaark 13, og er lagret i

internkontrollsystemet. Se også protokoll over behandlinger av helse- og personopplysninger i virksomheten (faktaark 13).

3.5. Lovlig behandling av helse- og personopplysninger

Personopplysninger kan bare behandles når lovgivningen tillater det. Dataansvarlig skal sørge for at personopplysninger skal har et lovlig grunnlag for behandlingen, et behandlingsgrunnlag.

Behandlingsgrunnlag skal identifiseres før behandling av helse og personopplysninger starter, eller ved endringer.

Plikten til å føre journal gir en rettslig forpliktelse til å behandle helse- og personopplysninger. Personopplysningene virksomheten behandler ved ytelse av helsehjelp vil være lovpålagt å behandle som følge av denne plikten. Dette er behandlingsgrunnlaget for denne behandlingen.

Virksomhetens øvrige behandlinger av personopplysninger kan ha andre behandlingsgrunnlag. Eksempler på dette er i arbeidet med å følge opp ansatte, der avtale med den registrerte kan være riktig behandlingsgrunnlag, og dersom virksomheten utfører oppdrag som ikke er helsehjelp kan både samtykke og avtale være riktige behandlingsgrunnlag.

Les mer om de ulike behandlingsgrunnlagene i artikkelen personvern i små helsevirksomheter.

4. Styring og kontroll

4.1. Internkontroll

Med internkontroll menes formalisering av hvordan virksomheten planlegger, gjennomfører, evaluerer/ kontrollerer og korrigerer etterlevelse av relevant regelverk, krav og avtaler.

Den som har det overordnede ansvaret for virksomheten, skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter (internkontroll). Det er et krav at dokumentasjon om dette til enhver tid skal være oppdatert og lett tilgjengelig for alle ansatte.

Det må også etableres rutiner for å sikre at styrende dokumenter til enhver tid er oppdaterte i tråd med krav i gjeldende lovverk, beslutninger, organisatoriske løsninger, rutiner og andre relevante styringsdokumenter.

Informasjonssikkerhet og personvern bør inngå som en del av den totale interkontrollen i virksomheten.

En måte å jobbe med internkontroll er å dele det inn i tre deler; styrende del, gjennomførende del og kontrollerende del. Kort oppsummert:

Styrende del – noen viktige områder

- Definer ansvar, funksjoner og ha en god oversikt over virksomhetens mål, oppgaver og tjenester, organisering og ansvarsfordeling

Oversikt over behandlinger av helse- og personopplysninger (protokoll)Gjennomførende del noen viktige områder

- Tilgangsstyring
- Opplæring og kompetanse
- Avtaler

Kontrollerende del – noen viktige områder

- Scenarioliste over hva galt som kan skje, og risikovurdering
- Avvikshåndtering av uønskede hendelser
- Årlig sikkerhetsprat i virksomheten (som i Normen omtales som ledelsens gjennomgang)

Virksomheten skal ha en oversikt over ansatte, funksjoner og hvilke oppgaver de har ansvar for. Oversikten skal være oppdatert og lett tilgjengelig for alle ansatte

Internkontrollsystemet til Normland Helsesenter inneholder en oversikt over ansatte, samarbeidspartnere, kontraktører, inkludert funksjoner og ansvar. Her fremgår det f.eks at:

- Lena er daglig leder
- Morten er IKT-ansvarlig, noe som omfatter bl.a ansvar for kontakt med IKT-driftspartner, backup og programvareoppdateringer på pc'er, samt holde de delene av internkontrollsystemet som gjelder informasjonssikkerhet oppdatert.

- Hvilke avtaler helsesenteret har med eksterne leverandører, med oppdatert kontaktinfo ved behov for support og andre henvendelser.
- Utfylt sjekkliste sikkerhet

4.2. Sjekkliste for sikkerhet

Denne veilederen samler de viktigste dokumentasjonskravene i en sjekkliste. Sjekklisten gir virksomheten et godt utgangspunkt for oversikt og internkontroll for informasjonssikkerhet og personvern.

Tiltak som gjøres for å sikre helse- og personopplysninger skal som tidligere nevnt være forholdsmessige. Dette gjelder også ved internkontroll.

Sjekklisten ligger som vedlegg til denne veilederen.

4.3. "Sikkerhetspraten" (Ledelsens gjennomgang)

Øverste leder har ansvaret for at virksomheten kontrollerer at oppgaver, tiltak, planer og mål gjennomføres som planlagt.

Status for sikkerhetsarbeidet i virksomheten skal gjennomgås minimum årlig. I lovgivningen og Normen heter dette ledelsens gjennomgang. I en større virksomhet Ledelsens gjennomgang en gjennomgang med ledelsen. I en mindre virksomhet kan dette gjøres som en samtale med alle som jobber i virksomheten. I denne samtalen (sikkerhetspraten) bør virksomheten minimum gå gjennom:

"TA PRATEN"	
Når	• En gang per år som et fast møtepunkt • Om det oppstår alvorlige hendelser
Vurderinger	Følgende bør som minimum gjennomgås: • Gjennomgang av sikkerhetsmalen; er det viktige endringer i oversikter, rutiner og prosedyrer • Avvik, håndtering av avvikene og læringspunkter for at avviket ikke skal skje igjen • Gjennomgang av scenarioer (se kapittel 6.1) over hendelser som kan skje og relevante tiltak for virksomheten • Ansvarsforhold og organisering mht. informasjonssikkerhet • Endringer i oversikten over helse- og personopplysninger som behandles i virksomheten (protokollen) og formålet med behandling av helse- og personopplysninger • Oppfølging av leverandører og databehandleravtaler

"TA PRATEN"	
Tiltak	Dersom gjennomgangen avdekker hendelser eller rutiner som trenger oppfølging, korrigering og nye tiltak, må dette ivaretas. • Tiltaksplaner med plassering av ansvar og tidsfrist

Sikkerhetspraten skal dokumenteres. Dokumentet vil fungere som Ledelsens gjennomgang.

Normland Helsesenter skal gjennomføre sikkerhetspraten / ledelsens gjennomgang for første gang i forbindelse med et møte for de ansatte. Lena leder møtet. Maren lager referat. Hovedpunkter fra møtet:

- Sjekkliste for sikkerhet: Må supplere oversikt over eksterne avtalepartnere med leverandør som håndterer makulering av papirdokumenter. Det mangler rutine for håndtering av elektroniske meldinger. Hva gjør vi hvis vi får feilmeldinger ved sending av f.eks henvisninger?
- Avvik: Det har flere ganger ligget igjen sensitive dokumenter som pasienter har glemt igjen på venterommet. Tiltak er instruks til renholder: Finner man slike dokumenter skal de låses inn på resepsjonskontoret.
- Risiko: Scenarioene gjengitt i kapittel 6 i denne veilederen er gjennomgått. Avdekket et scenario med ikke akseptabel risiko: Papirdokumenter scannes inn på feil pasient. Tiltak: Maren og Morten lager forslag til rutine.
- Oversikter (bl.a. ansvar, funksjoner og oppgaver): Ingen endringer utover makulering som nevnt over
- Oppfølging av leverandører og databehandlere: Dårlig tilgjengelighet på support hos EPJ-tjenesteleverandør. Følges opp av Lena mot kontaktperson.

Maren lagrer referatet i internkontrollsystemet etter at det er godkjent av Lena.

4.4. Hvordan skal virksomheten ivareta kravene i Normen?

Normens faktaark 6b gir en oversikt over alle kravene i Normen som virksomheten skal følge. Journalsystemleverandøren/ driftsleverandøren kan bistå med å fylle ut flere av punktene. De har ofte kunnskap og kompetanse

Faktaark 6b gir en god oversikt. Den er generisk og ikke spesielt tilpasset små virksomheter. Her er det viktig å tenke at virksomheten skal ha tiltakene i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv. Se mer om dette i kapittel 3.

Dersom noen av punktene besvares med ”Nei”, må egnede tiltak iverksettes. Virksomheten må vise til en risikovurdering om virksomheten må gjennomføre, på hvorfor det er svart nei.

4.5. Avviksbehandling

Gjennomføring av risikovurdering og etablering av tiltak vil aldri kunne forebygge alle uønskede hendelser. Når en hendelse oppstår eller et brudd avdekkes, skal virksomheten på en systematisk måte registrere, håndtere og følge opp hendelsen.

Uønskede hendelser eller brudd på personvern eller informasjonssikkerhet skal behandles som avvik. Virksomhetens ledelse skal behandle avvik for å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse.

Manglende eller uhensiktsmessige rutiner bør også håndteres som avvik.

Det er viktig at det jobbes aktivt for å få oversikt over alle avvik i virksomheten og at det er gode rutiner for hvordan avvik håndteres. Alle i virksomheten, inkludert administrativt personell, skal være kjent med hvordan og til hvem avvikene meldes. Alle avvik skal dokumenteres. Om virksomheten allerede har et avvikssystem vil det være hensiktsmessig å benytte dette også på personvernområdet.

Risikoen for personen (den registrerte) avviket gjelder, skal vurderes. Dersom avviket er et brudd på personopplysningsikkerheten og har medført middels eller høy risiko for personen, skal avviket rapporteres til Datatilsynet innen 72 timer etter å ha fått kjennskap til det. Ved høy risiko for personen skal avviket også meldes til personen. Les mer om avviksbehandling i Normens veileder om internkontroll for informasjonssikkerhet og personvern.

Her kan du melde avvik til Datatilsynet.

Tre eksempler på avvik fra Normland Helsesenter:

1. Maren mottar en klage fra en pasient. Pasienten har fått et prøvesvar i posten fra Helsenteret. På side to hadde det ved en feiltakelse kommet et annet prøvesvar som gjaldt en annen pasient. Prøven gjaldt svar på en HIV-test. Maren tar det opp med Lena. Hun ber Maren dokumentere hendelsen som et avvik i internkontrollsystemet. Sammen vurderte de avviket til å være høy risiko for pasienten. Lena melder videre avviket til Datatilsynet, via Altinn. Hun gjør det samme dag, for å være helt sikker på at det gjøres innen 72 timer. Siden avviket er høy risiko, meldes avviket også til de registrerte.
2. Dagen etterpå dukker det opp en annen henvendelse fra vergen til en av pasientene på Helsesentret. Vergen som er advokat fikk tilsendt dokumenter om en annen pasient enn den advokaten var verge for. Det viser seg nemlig at Helsesenteret har to pasienter med verger fra samme advokatfirma. Advokaten meldte at hun hadde makulert dokumentene og viste til sin lovpålagte taushetsplikt.
3. Maren fikk beskjed av Lars om å dokumentere hendelsen som et avvik i internkontrollsystemet, og endret i ettertid på rutinen sin for oversendelse av dokumenter. De vurderte hendelsen til å være lav risiko pga. advokatens taushetsplikt og meldte dette ikke videre til Datatilsynet.
4. Uken etterpå kom Maren på jobb og oppdaget at en ansatt hadde glemt å lukke vinduet til legekontoret dagen før. Det var ingen tegn til at uvedkommende hadde tatt seg inn i lokalet. Maren dokumenterte også denne hendelsen som et avvik i internkontrollsystemet. De vurderte hendelsen til å være lav risiko og meldte ikke videre til Datatilsynet.
5. Normland Helsesenter blir rammet av et kryptovirus som krypterer filserveren deriblant innkomne prøvesvar. Disse prøvesvarene er ikke sendt ut til pasientene. Normland hadde heldigvis backup og får tilbake alle filene. DE går gjennom filene og sjekker at det ikke er et integritetsbrudd. Pga. at de raskt fikk tilbake filene er det heller ikke et lengre

tilgjengelighetsbrudd. Både for integritet og tilgjengelighet vurderes risikoen til lav. Maren dokumenterer avviket i internkontrollsystemet, men melder ikke til Datatilsynet. De må også huske å vurdere om avviket skal meldes til Statens helsetilsyn

5. Organisering

Små helsevirksomheter er organisert på ulike måter. Enkelte driver helt selvstendig. Noen går sammen med andre virksomheter og samarbeider om pasientjournalsystemer og andre fagsystemer. Noen virksomheter setter ut mesteparten av drift og vedlikehold til leverandører (databehandler), og noen har servere lokalt. Andre inngår løsninger for tilgang på tvers ved behov.

Uavhengig om det er aksjeselskap eller enkeltpersonforetak er det viktigste å avklare dataansvar, roller, oppgaver og ansvar.

Når én virksomhet bestemmer formålet og hjelpemidlene for behandlingen av helse- og personopplysninger, er virksomheten dataansvarlig.

Det er den dataansvarlige som har det daglige ansvaret for personvernet og informasjonssikkerheten. Oppgavene med å behandle helse- og personopplysningene kan delegeres til egne ansatte i virksomheten, eller leverandører. Leverandøren blir da en databehandler som gjennomfører behandlingene av helse- og personopplysningene på vegne av dataansvarlig.

5.1. Tekniske IT løsninger

Små virksomheter har flere ulike tekniske løsninger.

- Virksomheten har installert journalsystemet på eget utstyr (server eller PC) som ikke er tilknyttet Internett
- Virksomheten har installert journalsystemet på eget utstyr (server eller PC) og har tilkobling til helsenett for tilgang til Internett og ekstern e-post.
- Virksomheten benytter databehandler (leverandør) som drifter journalsystemet hos seg og helsepersonellet har tilgang til journalsystemet via helsenett eller Internett

Journalsystem og oppbevaring av helse og personopplysninger kan gjøres via nettverk, web basert eller i en skytjeneste. Tilbud om slike løsninger kommer fra flere leverandører. Mange små helsevirksomheter velger at ASP[1] leverandører leverer både journalsystem, tilgang til helsenett og drifter den tekniske løsningen. Sikkerheten blir i mange tilfeller bedre ivaretatt på denne måten, igjennom leverandørens kunnskap og kompetanse. All tjenesteutsetting skal reguleres i en databehandleravtale.

Dersom virksomheten bruker eksterne leverandører av IKT-funksjoner eller andre tjenester skal avtalen med leverandøren omfatte bl.a.:

- dokumentert risikovurdering som viser at virksomhetens nivå for akseptabel risiko samt Normens sikkerhetsnivå er etablert. Ved tjenesteutsetting av IKT-tjenester til andre land bør forhold ved vertslandet vurderes fordi forholdene kan påvirke risikovurderingen.

[1] ASP = Application Service Provider = en leverandør som tilbyr datatjenester til kunder over et nettverk = «en plugg i veggen» for kontoret

- hvilke oppgaver av sikkerhetsmessig betydning som er omfattet, og ansvarsforholdene for disse
- beskrivelse av leverandørens løsning og grensesnitt mot virksomheten i form av konfigurasjonskart (tegning over teknisk løsning

Virksomheten skal sørge for å inngå databehandleravtale når leverandører behandler helse- og personopplysninger på vegne av virksomheten. Les mer om bruk av databehandler (faktaark 10).

Avtalen skal sikre at virksomheten også gis rett til å revidere leverandørens aktiviteter som er knyttet til avtalen. Revisjonene kan gjennomføres av en avtalt tredjepart.

Ved avslutning av kontrakten skal det foreligge en signert erklæring fra leverandøren om at alle data tilhørende virksomheten er tilbakelevert eller slettet til avtalt tid.

5.1.1 Skytjenester

Skyen er en betegnelse for alt fra dataprosessering og -lagring til programvare på servere som står i eksterne serverparker, som vanligvis bruker Internett som bærer av datatrafikken. Skytjenester gir virksomheten mulighet til å leie programmer og infrastruktur som en tjeneste, i stedet for at det er virksomheten selv som eier den.

Eksempler på områder hvor bruk av skytjenester til helse- og personopplysninger er tatt i bruk er:
- Journalsystemer for primærhelsetjenesten (f.eks. legekontor, tannklinikk, psykolog mv.)
- Velferdsteknologi
- Video- og mobilteknologi for å behandle helse- og personopplysninger
- Pasientportaler for elektronisk pasientkommunikasjon
- Kurveløsninger, fagsystemer, e-postsystem mv.

Bruk av skytjenester kan bidra til godt personvern og informasjonssikkerhet ved at helse- og personopplysningene blir håndtert av en profesjonell leverandør med kompetanse innen fysisk og digital sikkerhet. Imidlertid introduserer skytjenester nye risikoer, som mindre grad av kontroll på helse- og personopplysningene og hvordan de behandles. Det er derfor sentralt med blant annet risikovurderinger i forkant av anskaffelsen og databehandleravtaler som setter virksomheten i stand til god leverandøroppfølging etter avtaleinngåelsen.

Les mer om dette i veilederen i bruk av skytjenester til behandling av helse- og personopplysninger.

Normland Helsesenter har eksterne avtaler om vaktmestertjenester og IKT-drift. EPJ kjøpes som en tjeneste og er skybasert. Dette omfatter fakturering og betalingsoppfølging. Regnskap og lønn håndteres av eksternt regnskapskontor. Den eneste serveren som er installert lokalt på helsesenteret er en filserver som brukes til lagring av Word-dokumenter osv. Helsesenteret er tilknyttet helsenettet, og får internett og e-post levert via dette.

Morten har gjort en enkel risikovurdering av at EPJ-løsningen kjøres som en skybasert tjeneste. Leverandøren har gitt gode svar på spørsmålene Morten har stilt bl.a. om hvor data lagres, om leverandøren har tilgang til helseopplysninger, og at bruk av EPJ-løsningen ikke vil medføre at helsesenteret ikke er i stand til å etterleve personvernforordningen og Normen.

Databehandleravtalen som benyttes er basert på leverandørens egen mal, men Lena har forsikret seg om at oppgaver som har betydning for sikkerhet er godt beskrevet, at ansvarsforholdene er tydelige, at det er vedlagt en enkel beskrivelse av løsningen, og at helsesenteret får tilgang til revisjonsrapporter gjennomført av et anerkjent, uavhengig revisjonsfirma.

5.2. Felles pasientjournal (og andre behandlingsrettede helseregistre)

I de tilfellene det er to eller flere dataansvarlige, som f.eks. når flere fastleger, fysioterapeuter, psykologer mv. går sammen om å bestemme hva helse- og personopplysninger skal brukes til og hvilke system en velger å bruke vil de være felles dataansvarlige. Dette gjelder for alle typer systemer, enten det er felles pasientjournal, fagsystemer, kurveløsninger eller administrative systemer som e-postsystem. Når flere virksomheter går sammen om bruk av felles systemer skal de ansatte bare ha tilgang til helse- og personopplysninger ved tjenstlig behov.

Felles pasientjournal innebærer at hver pasient har én journal innen samarbeidet. Helsepersonellet tilknyttet fellesskapet fører opplysninger kun i denne journalen.

Ved samarbeid om felles pasientjournal, skal dette reguleres i en skriftlig avtale som inneholder:

- Hva samarbeidet omfatter
- Hvordan pasientens rettigheter skal ivaretas
- Hvordan helseopplysninger behandles og sikres – også ved endring/opphør
- Plikten de dataansvarlige har til å gi informasjon som sikrer den registrerte en rettferdig og åpen behandling av personopplysninger, herunder hvordan personopplysninger behandles og kontaktdetaljer.
- Dataansvar

Hvis det leies ut kontorplass til andre, og tilgang til felles pasientjournaler en del av leieforholdet, skal enhver ny part inngå i den skriftlige avtalen om samarbeid om felles pasientjournal.

Les mer om dette i veileder med avtaleeksempler ved samarbeid om felles journal.

Siden Lena og Lars har felles journal, har de en avtale om felles journal. Her fremgår det at de har delt dataansvar hvor begge har et like stort ansvar for pasientjournalsystemet, og at rutinene de har etablert følges.

Lars har flere jobber ved siden av sin praksis og har ikke særlig god tid til å sørge for sitt ansvar daglig. Derfor har de skriftlig avtalt at Lena sørger for at dataansvaret ivaretas. I sin årlige sikkerhetsprat gjennomgår de ansvarsforholdet.

6. Risiko

Risikovurdering er et verktøy for å identifisere uønskede hendelser, om risiko ved behandlingen av helse- og personopplysninger.

Det skal alltid gjennomføres risikovurdering:

- før behandling av helse- og personopplysninger starter
- ved alvorlige sikkerhetshendelser
- endringer i IT systemer, støttesystemer/pasientjournalsystemet eller i organisasjonen
- ved bytte av leverandør (for eksempel ved overgang til bruk av skytjenester)

Normland helsesenter gjennomførte en risikovurdering ved omleggingen til sky-basert EPJ-tjeneste. I tillegg tas en jevnlig gjennomgang av om det har skjedd endringer i risikobildet i forbindelse med "sikkerhetspraten".

Virksomheten skal ha en bevisst holdning til hvilke risikoer som finnes ved behandling av helse og personopplysninger. Gjennomfør heller flere små vurderinger enn en stor risikovurdering.

En risikovurdering for å forebygge svikt og uønskede hendelser skal gi svar på:

- hva som kan gå galt (uønsket hendelse). Identifisere områder der svikt kan få alvorlige eller uønskede følger for pasienter/brukere eller virksomheten.
- hvor stor sannsynlighet det er for at det går galt. Identifisere områder der svikt kan inntre ofte
- hva som er konsekvensene hvis det går galt.
- hvilke tiltak som er iverksatt og om nye tiltak må iverksettes.
- hvem som skal gjennomføre tiltakene, når og hvordan.

Start med å utarbeide konkrete forslag til trusler og uønskede hendelser knyttet til scenarioer.

6.1. Eksempler på scenarioer

Eksempler på scenarioer som kan vurderes:

- Opplysninger i journalsystemet endres uten at dette er sporbart (logges)
- Epikrise skannes inn i journalsystemet på feil pasient
- Serveren med journalsystemet blir stjålet
- IT-systemer hackes
- Utskrifter med helseopplysninger kommer på avveie
- Snoking i journaler
- Helseopplysninger sendes i ordinær e-post eller som ordinær SMS
- Journalsystemet er nede i mer enn 4 timer per uke

- Driftsavbrudd med varighet over én arbeidsdag

Scenariene bør drøftes, prioriteres og hvert scenario vurderes for:

- mulige konsekvenser
- eksisterende tiltak og behov for nye eller endrede tiltak

Utarbeid en oppsummering og et sammendrag. Det er viktig at alle i virksomheten blir involvert i en slik prosess og det kan med fordel opprettes en arbeidsgruppe.
Øverste leder må sikre at virksomheten planlegger hvordan risiko innenfor de aktuelle områdene kan minimaliseres.

Utarbeid en tiltaksliste som viser tiltak, hvem som er ansvarlig og når tiltakene skal være gjennomført.

Se Normen sin veileder om risikostyring i informasjonssikkerhet og personvern som forklarer mer om risikovurdering.

7. Nærmere om innholdet i sjekklisten

Holdninger og kultur er grunnlaget for hvordan den enkelte forholder seg til bruk av helse- og personopplysninger. En daglig bevisst holdning om informasjonssikkerhet og personvern beskytter mot brudd på konfidensialitet, integritet og tilgjengelighet. Det vil øke pasientens tillit til tjenesten og gi virksomheten et kvalitetsstempel og godt renommé.

Dette kapittelet gir utfyllende informasjon til de viktigste punktene i vedlegget sjekkliste for sikkerhet.

7.1. Tilgangsstyring, tildeling av rettigheter (autorisasjon) og autentisering

Tilgangsstyring handler om hvordan virksomheten gjennomfører:

- autorisering, som er tildeling av rettigheter til å kunne lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger
- autentisering, som sikrer identifisering av autorisert bruker
- tilgjengeliggjøring av helse- og personopplysninger om bestemte pasienter/brukere for autorisert personell
- tilgjengeliggjøring av helse- og personopplysninger til annet personell enn virksomhetens eget personell
- regulering av privat bruk av virksomhetens informasjonssystemer
- kontroll av tildelte rettigheter og kontroll av logger

Les mer i veileder for tilgang til helse- og personopplysninger.

Tilgang skal tildeles medarbeiderne etter hvilke arbeidsoppgaver de har. Tilgangen som gis skal være basert på et konkret tjenstlig behov (arbeidsoppgaver). Ved tildeling av autorisasjon skal lovbestemt taushetsplikt vurderes og ivaretas.

Tilgangsstyringen må ta utgangspunkt i hvordan den enkelte virksomheten konkret er organisert 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. Momenter som vil kunne påvirke den konkrete tilgangsstyringen er bl.a.:

- størrelsen på praksisen: en liten praksis med få ansatte vil ha en enkel tilgangsstyring mens en stor praksis med mange ansatte i virksomheten, felles pasientjournal og mulig hjelpepersonell som sekretær vil ha behov for mer nyansert tilgangsstyring.
- når databehandler har tilgang til helse- og personopplysninger (skal reguleres i databehandleravtale)

- leverandør av journalsystem, der leverandøren har fjernaksess[2] (les mer i veileder for fjernaksess mellom virksomhet og leverandør)
- nødrettstilgang

Autentiseringen .
Autentisering vil si å bekrefte en påstått identitet. Journalopplysninger kan bare gjøres tilgjengelig for personell som gjennom autentisering kan bekrefte sin identitet på en sikker måte.

I praksis gjøres dette ved hjelp av et passord eller PKI (personlige sertifikater som BuyPass eller Comfides eller Bank-ID)**,** som sikrer identifisering av autorisert bruker. Autentisering skal være forholdsmessig ut fra virksomhetens størrelse og virkefelt

Det skal etableres rutine for tildeling og administrasjon av tilgangsrettigheter:

- **Autorisasjon** for å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger skal gis til dem som har tjenstlig behov. Lovbestemt taushetsplikt skal vurderes og overholdes. Også tekniske tiltak skal etableres for å ivareta krav til konfidensialitet ved aktivt å hindre uvedkommende i å få tilgang og for å sikre dokumentasjon av denne tildelte autorisasjonen.
- Autorisasjonen skal angi hvilke virksomheter autorisasjonen omfatter (om samme autorisasjon gir tilgang til helse- og personopplysninger i flere virksomheter)
- Autorisasjonen skal være tidsbegrenset.
- Teknisk personell (f.eks. en leverandør eller IT-service) med særskilt behov for tilgang kan autoriseres for større mengder helse- og personopplysninger. Det skal etableres tiltak slik at mulig misbruk skal kunne avdekkes.
- Autorisasjon for andre tjenester gis etter tjenstlig behov.

Autorisasjonen skal vurderes på nytt når det oppstår endringer i ansvarsområder eller ansettelsesforhold

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. Virksomheten bør lage en oversikt som viser tilgangene per rolle.

Gjennomgang og kontroll av tilgangsstyring, herunder tildelte autorisasjoner, skal foretas av den enkelte leder

- minimum årlig (gjerne i forbindelse med sikkerhetsrevisjon)
- ved sikkerhetsbrudd for det informasjonsområdet som blir berørt av bruddet
- ved organisasjonsendringer, overflytting av personell til annen enhet/avdeling eller endring av arbeidsområde

Virksomhetens ledelse skal påse at det jevnlig gjennomføres kontroll av hvem som har hatt elektronisk tilgang.

[2] Med "fjernaksess" menes i dette dokumentet ekstern tilgang fra leverandør til virksomhet via kommunikasjonslinje. Eksempler på anvendelsesområder er: feilretting, feilsøking, oppdateringer, fjernadministrasjon, test- og utvikling, overføring av datafiler, driftsovervåking (databaser, servere, lagringsløsninger), behandling av feilmeldinger og datafiler hos leverandør og sending av feildiagnoser, m.v. av fagsystemer og IKT-infrastruktur.

Normland helsesenter har etter en vurdering av arbeidsprosessene på kontoret satt opp tilgangsstyringen sin slik at helsepersonellet har tilgang til hverandres pasienter. De merkantilt ansatte har tilgang til pasientadministrasjon for alle pasienter. Hvis f.eks familiemedlemmer til de ansatte på kontoret er pasienter, hender det at helsepersonellet på eget initiativ sperrer journalnotater for innsyn fra de andre på kontoret.

7.2. Informasjon til pasient (etter reglene i personvernforordningen)

Virksomheten har plikt til å gi informasjon om behandling av helse- og personopplysninger på en kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk.

Informasjonen skal gis skriftlig eller på en annen måte, herunder elektronisk dersom det er hensiktsmessig. Eks: oppslag på kontoret, personvernerlæring på nett, i brev til pasienten eller i en brosjyre.

Dataansvarlig skal på en forståelig måte informere den registrerte om:

- navn og kontaktinformasjon til dataansvarlig
- eventuelle mottakere av personopplysningene (dersom virksomheten deler opplysninger med andre virksomheter, offentlige virksomheter mv)
- hvor lenge opplysningene skal lagres, eller hva som avgjør når de skal slettes
- formål og rettslig grunnlag for behandlingen av helse- og personopplysningene
- retten til innsyn, retting og sletting
- informasjon om eventuelt gjenbruk av opplysningene til annet formål
- retten til å klage til Datatilsynet

Dersom opplysninger innhentes fra andre enn den registrerte (pasient/bruker) skal det i tillegg gis informasjon om hvilke kategorier personopplysninger som innhentes, og hvor de kommer fra, eventuelt om dette er offentlig tilgjengelige data eller ikke. F.eks. fra kommunehelsetjenesten, NAV, andre fastleger, avtalespesialister, fysioterapeuter, sykehus mv.

Normland helsesenter har valgt å bruke nettside og oppslag på venterommet for å informere pasientene.

7.3. Innsyn

Virksomheten skal sikre at pasienten (den registrerte) kan få innsyn i opplysninger registrert om seg selv. Dette innsynet gjelder også loggen over hvem, og eventuelt fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger, på hvilket tidspunkt.

Pasienten har som utgangspunkt rett til innsyn i alle opplysninger i journal. Dette gjelder også lydlogger, røntgenbilder, videoopptak etc. Dersom slikt materiale – etter at nødvendige og relevante opplysninger fra materialet er nedtegnet i journalen – oppbevares av hensyn til for eksempel kvalitetssikring i virksomheten, har pasienten innsynsrett.

Pasienter kan nektes innsyn i opplysninger i journalen eller deler av journalen dersom det er påtrengende nødvendig for å hindre fare for liv eller alvorlig helseskade for pasienten selv, eller innsyn er klart utilrådelig av hensyn til personer som står vedkommende nær. Det skal mye til for at innsyn skal nektes, og det må være en reell fare for konsekvenser av et visst omfang.

Dataansvarlig skal gi innsyn innen 30 dager, uten kostnad fra pasienten.

Leverandør av journalsystem bør kunne bistå ved forespørsler om innsyn. Databehandler skal bistå ved forespørsler om innsyn.

7.4. Retting, sletting og sperring

Hovedregelen i personopplysningsloven er at den registrerte har rett til å få uriktige eller ufullstendige opplysninger rettet uten ugrunnet opphold. Helselovgivningen har regler om sletting og endring av opplysninger. Det er avgjørende for forsvarlig helsehjelp at viktig informasjon ikke slettes eller endres.

Pasienten kan bare kreve at opplysningene i journal slettes dersom opplysningene er feilaktige eller misvisende og føles belastende for den de gjelder, eller de åpenbart ikke er nødvendige for å gi helsehjelp.

Rettingen i journal skal skje ved at oppføringen føres på nytt, eller ved at en datert rettelse tilføyes i journalen. Retting skal ikke skje ved at opplysninger slettes.

7.5. Oppbevaring

Helse- og personopplysninger skal oppbevares til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem. Virksomheter som yter helse- og omsorgstjenester har de journalføringsplikt. Det kan være viktig for helsepersonell å gå tilbake til journalnotater og se hva som er gjort tidligere for å kunne gi videre behandling. Det samme gjelder loggen om hvem som har hatt tilgang til eller fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer.

Når det ikke lenger er behov for helse- og personopplysningene og de ikke skal bevares etter arkivlov eller annen lovgivning, skal de slettes.

7.6. Fysisk sikring av områder og utstyr

Det er viktig at virksomheten sikrer det fysiske området. Sikringen har som formål å hindre at pasienter, pårørende eller andre uautoriserte får tilgang til helse- og personopplysninger.

I praksis kan dette bety at behandlingsrom er avskjermet fra venterom og treningssal, at dørene til behandlingsrom kan låses, at arkivrommet er låst, at bærbare PC er passordbeskyttet, og har et skjermfilter slik at pasienten ikke kan se på skjermen, og at PC låses med en gang de forlates.

Virksomheten skal sikre at utskrifter ikke kommer på avveie. Dette kan løses ved at skriveren er passordbeskyttet og står i et område hvor pasienter eller pårørende eller andre ikke har

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

Virksomheten bør også utarbeide rutiner/ prosedyrer for daglig sikring av kontordører/-vinduer (låsing, alarmsystemer), resepsjonsområde, PC, printere, telefakser, kopimaskiner, bærbare datamaskiner mm.

Les i

- Veileder i personvern og informasjonssikkerhet – medisinsk utstyr
- Veileder i informasjonssikkerhet og personvern ved bruk av teknologi i kommuner (velferdsteknologi)

Det er gjort en vurdering av hvordan fysisk sikring av PC og printere er gjort på helsesenteret. Tidligere sto bl.a. printeren ute på gangen. Den er nå flyttet inn på resepsjonskontoret. Dette er bemannet til enhver tid unntatt i spisepausen, da det låses. Siste ansatte som forlater kontoret skal alltid sjekke vinduer og dører.

7.7. Sikkerhet i nettverket og datautstyret

Mange av disse oppgavene kan settes ut til eksterne leverandører, f.eks. driftsleverandør og/eller EPJ-leverandør. Men ansvaret for at det gjøres, ligger alltid på dataansvarlig/ virksomheten.

Oversikt over utstyr og programvare

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

Dokumentasjonen skal inneholde en oversikt / tekstlig beskrivelse med:

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

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 sørge for at helse- og personopplysninger sikkerhetskopieres etter en fastsatt rutine. I tillegg skal oppsett av pasientjournalsystemet, røntgensystemet, servere mv. sikkerhetskopieres jevnlig slik at hele informasjonssystemet kan gjenopprettes.

- Sikkerhetskopier skal oppbevares avlåst og brannsikret, og adskilt fra driftsutstyret.
- Det skal jevnlig foretas test av at sikkerhetskopiene er korrekte og kan tilbakeføres.
- Minimum en sikkerhetskopi skal beskyttes mot ondsinnet programvare

Siden EPJ-systemet benyttes som en tjeneste behøver ikke helsesenteret tenke på backup av EPJ. Filserveren for kontorstøtte sikkerhetskopieres via en nettbasert løsning i helsenettet, så det eneste Morten må følge opp er at status på er OK på sikkerhetskopiering.

Beskyttelse mot ondsinnet programvare (f.eks. datavirus)

Virksomheten skal sørge for at datamaskinene (PC. MAC, mobiltelefon, nettbrett mv.) som benyttes i virksomheten har installert en løsning for å hindre ondsinnet programvare.

Programvaren skal være satt opp slik at den automatisk henter ned og installerer oppdateringer. Dette forutsetter en sikker Internettilknytning. 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.

Utfasing av utstyr

Ved utfasing av utstyr (for eksempel kopimaskin, telefaks, multifunksjonsskriver, PC, server mv.) skal virksomheten påse at helse- og personopplysninger blir overført til nytt utstyr eller slettes 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.

Det anbefales at virksomheten benytter en leverandør som påtar seg sikker sletting av utrangert utstyr.

Der leverandør må inn og behandle personopplysninger må virksomheten inngå databehandleravtale. Sletting er også en behandling av personopplysninger.

7.8. Hjemmekontor

Med hjemmekontor menes tekniske løsninger som er virksomhetens eiendom og som skal benyttes til arbeidsoppgaver utenfor arbeidsplassens fysiske lokaler. Eksempler på mobilt utstyr er PC, nettbrett og mobiltelefoner.

Virksomheten skal sikre at tilgangen til hjemmekontor og mobilt utstyr skjer ved bruk av en sikker autentiseringsløsning. F.eks. ved bruk av passord, to-faktorautentisering, eller

lignende for å hindre at uautoriserte får tilgang, på samme måte som for stasjonært utstyr på klinikken.

Med mobilt utstyr og lagring på selve utstyret kommer problemstillinger knyttet til at enhetene kan bli stjålet, gjenglemt eller hacket. Utstyret må derfor sikres. Virksomheten skal gjennomføre risikovurdering av de løsningene som benyttes. Og det skal etableres fastsatte rutiner for bruk av mobilt utstyr og hjemmekontor.

Helse- og personopplysninger skal bare lagres lokalt på utstyret når dette er nødvendig ut fra tjenstlig behov, og skal alltid lagres kryptert.

Det er blitt mer vanlig at helsepersonell tar bilder av journalnotater, pasienten eller andre bilder som gjengir helse- og personopplysninger med sin private mobiltelefon. Helselovgivningen åpner for å gjøre dette i hastesituasjoner. Ved bruk utover hastesituasjoner skal bruken av private mobiler risikovurderes og sikres, og virksomheten må sørge for at alle relevante lovkrav ivaretas.

Bildene skal dokumentere i pasientjournalen dersom de vurderes som å være nødvendige og relevante for helsehjelpen. Bildene skal slettes fra utstyret etter at de er journalført eller det ikke lenger er et behov for å lagre bildene. Her er det viktig å tenke på at mobiltelefoner ofte har automatisk lagring i diverse skytjenester. Bildene skal også slettes fra disse. Bruken av skytjenester til dette må også risikovurderes

ASP-leverandørene og journalleverandørene har ofte en hjemmekontorløsning de kan tilby.

Les mer om:

- Sikring av bærbart utstyr (faktaark 18)
- Hjemmekontor og annet fjernarbeid (faktaark 29)
- Sikring av mobilt utstyr utenfor virksomheten (faktaark 30)

7.9. Opplæring og kompetanseheving

Leder har ansvar for å gi de ansatte opplæring i informasjonssikkerhet og personvern. Det må tydeliggjøres at hver enkelt ansatt har et selvstendig ansvar og må bidra til å sikre pasientinformasjonen.

Medarbeidere i virksomheten skal ha tilstrekkelig kunnskap og kompetanse til å utføre jobben sin på en faglig forsvarlig og god måte, herunder mht. informasjonssikkerhet og personvern. Kjennskap til regelverket vil i ulik grad inngå som et ledd i de ulike profesjonenes utdannelse. Hvilke krav til kompetanseheving de enkelte har behov for vil derfor variere. Den enkelte medarbeider har også en selvstendig plikt til å holde seg oppdatert innen sitt fagområde.

Plakat for daglig informasjonssikkerhet kan være til hjelp for å huske små ting i hverdagen. Lag gjerne en egen, eller bruk fra andre. Flere av interesseorganisasjonene har laget slikt materiell.

Se mer om retningslinjer for daglig informasjonssikkerhet i veileder om internkontroll for informasjonssikkerhet og personvern.

7.10. Digital kommunikasjon med pasienter

SMS og e-post

Det skal ikke brukes ordinær SMS eller e-post til overføring av helseopplysninger.

SMS og epost 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 bryter med kravet til informasjonssikkerhet og personvern.

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.

Normland helsesenter benytter SMS til timepåminnelse og digital dialog via Helsenorge.no. Pasienten oppfordres til å benytte disse tjenestene.

E-konsultasjon

E-konsultasjon gir fastlegen en enkel og trygg kommunikasjonskanal med pasienten når det trengs helsehjelp som ikke er akutt eller når det ikke krever fysisk oppmøte. Les mer om e-konsultasjon hos Helsenorge.

Virksomheten skal vurdere informasjonssikkerheten og personvernet ved bruk av e-konsultasjon. Spørsmål som må vurderes er bl.a. hvor opplysningene blir lagret, kryptering av datatrafikk, autentisering av helsepersonell, hvordan er brukerens personvern ivaretatt, kan pasienten få tilgang til sine data. osv.

Det må lages gode rutiner for å journalføre nødvendige og relevante opplysninger fra konsultasjonen.

På Normland Helsesenter opplever Lars at det i noen tilfeller ville vært praktisk å ta i bruk løsninger for videokonsultasjon. Lars bruker mye tid på å delta i tverrfaglige møter at uten pasient er til stede, eller når han må reise til ulike institusjoner hvor pasienten befinner seg. Han følger også opp disse pasientene via kommunikasjon med pleie og omsorgstjenesten i kommunen. Normland går derfor i gang med å skaffe seg en løsning for videokonsultasjon.

Faktaark 54 inneholder en liste over minimumskrav til personvern og informasjonssikkerhet i videokonsultasjoner. Denne listen inneholder punkter om hvordan virksomheter kan ha tilstrekkelig autentiseringsløsning av pasienten, kryptering, informasjon til pasient, hvordan ivareta den registrertes rettigheter osv. I tillegg inneholder faktaarket en liste over ulike risikoscenarioer som virksomheten kan benytte som inspirasjon, samt forslag til ulike rutiner for bruk av video ved ytelse av helse- og omsorgstjenester. Les mer om videokonsultasjon (faktaark 54).

Sosiale media

Bruk av sosiale medier kan ha nytteverdi. Sosiale medier kan f.eks. bidra til at helsepersonellet lærer av erfaringer og tilbakemeldinger fra pasienter og brukere. De sosiale mediene kan i tillegg styrke arbeidet med å dele kunnskap og bygge felles kultur.

Samtidig som sosiale medier gir økte muligheter for kommunikasjon, er det viktig å være bevisst at mulighetene også gir utfordringer. Disse knytter seg i første rekke til personvernet og virksomhetenes ansvar som dataansvarlig.

Taushetsplikten for de som jobber med pasienter, gjelder fullt ut også i sosiale medier og skal alltid overholdes. Dette innebærer blant annet:

- At det ikke publiseres helse- og personopplysninger uten samtykke fra de opplysningene gjelder.
- Det skal innhentes et særskilt samtykke dersom helse- og personopplysninger og bilde/video av en pasient skal kunne publiseres på Internett. Selv om det foreligger et samtykke skal helsepersonellet alltid foreta en selvstendig vurdering av om publisering kan være tilskade for pasienten
- At pasienter, pårørende og ansatte ikke kan identifiseres uten at de samtykker til det

Det er viktig at virksomheten har tenkt i gjennom hvordan sosiale medier skal brukes. Det kan være lurt å lage felles kjøreregler dersom man er flere på kontoret. Hva er greit og hva er ikke greit "Slik gjør vi det hos oss".

7.11. Kvalitetssikring og læring

Med mindre pasienten motsetter seg det, kan taushetsbelagte opplysninger gjøres tilgjengelige for helsepersonell som tidligere har ytt helsehjelp til pasienten i et konkret behandlingsforløp. Opplysningene må være nødvendige og relevante for helsepersonellets egen læring eller for kvalitetssikring av helsehjelpen.

7.12. Forskning

Dersom virksomheten skal drive forskning, enten alene eller i samarbeid med andre, er det viktig å sette seg inn i regelverket om hvordan helse- og personopplysninger skal behandles. Det er noe forskjellig fra regelverket rundt bruken av opplysningene ved ytelse av helsehjelp og annen tjenesteyting.

Det er viktig å ha etablert et lovlig grunnlag for å drive forskning, dette kan være samtykke eller lovhjemmel.

Les mer i veileder i personvern og informasjonssikkerhet i forskningsprosjekter.

Besøksadresse
Direktoratet for e-helse
Verkstedveien 1
0277 Oslo

Kontakt
sikkerhetsnormen@ehelse.no