Sak 3: Styring og kontroll av tilgang til helseopplysninger i elektroniske pasientjournaler i fire helseforetak

Stortinget har i mange år framhevet betydningen av informasjons- og kommunikasjonsteknologi (IKT) for å nå helse- og omsorgspolitiske mål om bedre kvalitet, pasientsikkerhet, effektivitet og ressursbruk. Rask utveksling av helseopplysninger er viktig for å sikre god pasientbehandling og effektiv ressursutnyttelse i spesialisthelsetjenesten. Helseopplysninger er personidentifiserbar taushetsbelagt informasjon som er underlagt et strengt lovregulert behandlingsregime. Helseforetakene har flere elektroniske fagsystemer der helseopplysninger er registrert og lagret. Denne undersøkelsen omhandler styring og kontroll av tilgang til helseopplysninger i elektroniske pasientjournaler (EPJ) som har et stort omfang av sensitive opplysninger.

Målet med undersøkelsen har vært å vurdere om helseforetakenes styring og kontroll av tilgang til helseopplysninger i EPJ-systemet er i samsvar med gjeldende regelverk. Undersøkelsen omfatter Oslo universitetssykehus HF, Helse Bergen HF, St. Olavs Hospital HF og Universitetssykehuset Nord-Norge HF, og behandlingsområdene somatikk, psykisk helsevern og rus.

Undersøkelsen har tatt utgangspunkt i følgende lover og forskrifter:
- Lov om behandling av personopplysninger av 14. april 2000
- Forskrift om behandling av personopplysninger av 15. desember 2000
- Lov om helseregistre og behandling av helseopplysninger av 18. mai 2001
- Lov om behandlingsmåten i forvaltningssaker av 10. februar 1967
- Lov om spesialisthelsetjenesten av 2. juli 1999
- Lov om helsepersonell av 2. juli 1999
- Forskrift om pasientjournal av 21. desember 2000

Utkast til rapport ble forelagt Helse- og omsorgsdepartementet ved brev av 25. juni 2014. Departementet har i brev av 20. august 2014 gitt kommentarer til rapportutkastet. Kommentarene er i hovedsak innarbeidet i rapporten og i dette dokumentet.

1 Hovedfunn

- Helseforetakene har ikke i tilstrekkelig grad implementert gjeldende regelverk om informasjonssikkerhet og behandling av helseopplysninger.
- Ansatte i helseforetakene har tilgang til helseopplysninger utover tjenstlig behov.
- Helseforetakene har ingen systematisk kontroll og oppfølging av ansattes tilganger til EPJ.
- Helseforetakene har mangelfull internkontroll av tilgangsstyringen i EPJ.

2 Riksrevisjonens merknader

2.1 Helseforetakene har ikke i tilstrekkelig grad implementert gjeldende regelverk om informasjonssikkerhet og behandling av helseopplysninger

De fire helseforetakene har utarbeidet skriftlige prosedyrer basert på regelverket om blant annet personlig systempålogging, tilgangsstyring og loggkontroll i EPJ-systemet. Likevel er det flere eksempler på manglende etterlevelse av og lite kunnskap om interne rutiner og gjeldende regelverk:

- I to av fire helseforetak har ansatte lånt hverandres bruker-ID og passord for pålogging til EPJ-systemet.

- Det er gjennomgående for lite kunnskap om de tre ulike tilgangsrettighetene (normal-, aktualisert- og nødrettstilgang) til EPJ-systemet som helseforetakene benytter, og manglende kunnskap om når de skal brukes.

- Ingen av helseforetakene har gjennomført sikkerhetsrevisjoner slik regelverket pålegger, og det er ulik oppfatning blant helseforetakene om hva pålegget innebærer.

- Ingen av helseforetakene fører journalansvarlig i journalen slik regelverket pålegger, og det er gjennomgående manglende kunnskap om hvilket ansvar journalansvarlig har. I Universitetssykehuset Nord-Norge HF føres eksempelvis ikke journalansvarlig i journalen, selv om journalansvarlig ifølge prosedyrer for logganalyser er tillagt konkret ansvar for å bestille kontroller ved mistanke om ureglementert innsyn i pasientjournal.

Riksrevisjonen mener at helseforetakene verken har implementert gjeldende regelverk i tilstrekkelig grad, eller i tilstrekkelig grad lagt til rette for at de ansatte blir i stand til å overholde sine lovpålagte plikter for behandling av sensitive taushetsbelagte helseopplysninger. Det er dessuten uheldig at pålegg i regelverk blir tolket og praktisert ulikt av helseforetakene.

2.2 Ansatte i helseforetakene har tilgang til helseopplysninger utover tjenstlig behov

Helseforetakenes egne prinsipper for tilgangsstyring fastslår at det må foretas en konkret vurdering av hvilke opplysninger den enkelte skal få tilgang til basert på det som er nødvendig, slik gjeldende regelverk forutsetter. Likevel viser undersøkelsen at det i liten grad foretas slike konkrete vurderinger av den enkeltes tjenstlige behov for helseopplysninger når ansatte tildeles roller av klinikk- og avdelingsledere. Etter Riksrevisjonens syn vil ikke EPJ-systemets forutsetning om en viss grad av standardisert tildeling være til hinder for å foreta konkrete behovsvurderinger.

Samtidig viser undersøkelsen at tre av fire undersøkte helseforetak gir normal tilgang eller aktualisert tilgang til de ansatte, på tvers av systemområdene somatikk og psykisk helsevern/rus. I St. Olavs Hospital HF gis det eksempelvis svært brede normale tilganger og rett til å benytte aktualisert tilgang til mange ansatte og roller, på tvers av somatikk og psykisk helsevern/rus. En vid tildelingspraksis med fravær av systematiske vurderinger av den enkelte ansattes individuelle tjenstlige behov, innebærer etter Riksrevisjonens syn at mange ansatte gis tilgang til helseopplysninger uten at det foreligger nødvendig behov for tilgang til pasientjournal. Det er heller ingen av helseforetakene som har rutiner for systematisk å avslutte tilganger når ansatte bytter arbeidssted internt, og ved flere helseforetak er det ansatte som har tilganger de selv ikke er klar over. Etter Riksrevisjonens vurdering viser disse funnene et stort behov for at helseforetakene rydder opp i tildelingspraksisen slik at den blir i samsvar med gjeldende regelverk.

I helseforetakene som bruker DIPS-systemet, viser undersøkelsen at ansatte kan se samtlige kontakter (innleggelser og polikliniske konsultasjoner) en pasient har hatt med helseforetaket innen både somatikk og psykisk helsevern/rus. De ansatte kan også se samtlige henvisninger for den enkelte pasient, der mye sensitiv informasjon som diagnoser og koder av Diagnose Relaterte Grupper (DRG-koder) kan være tilgjengelig. I Universitetssykehuset Nord-Norge HF blir mange dokumenter med sensitiv informasjon rutinemessig scannet og lagret i pasientjournal som bilder. Disse bildene er tilgjengelig for ansatte på tvers av systemområdene somatikk og psykisk

helsevern/rus. Etter Riksrevisjonens vurdering viser dette at ansatte har tilgang til mye sensitiv taushetsbelagt informasjon uavhengig av hvilke tilgangsrettigheter de har blitt tildelt og uten å åpne selve pasientjournalen.

EPJ-systemene legger til rette for å tidsbegrense tilgangen til pasientjournaler. Likevel viser undersøkelsen at det innen psykisk helsevern/rus i Oslo Universitetssykehus HF og Universitetssykehuset Nord-Norge HF ikke er tidsbegrensning for de ansattes normale tilgang til pasientjournal i etterkant av utskrivning eller avsluttet konsultasjon. Dette innebærer at journalene til disse pasientene forblir tilgjengelige for de ansatte uten at det er nødvendig å oppgi noen behovsbegrunnelse for oppslag. Utgangspunktet ved aktualisert tilgang er at det er den enkelte ansattes individuelle tilgang som gjøres normal for en bestemt tidsperiode. Ved bruk av aktualisering i Universitetssykehuset Nord-Norge HF, ble pasientjournalen tilgjengelig også for øvrige ansatte gjennom normal tilgang på tvers av områdene somatikk og psykisk helsevern/rus i 24 timer. Dette innebærer at mange ansatte i disse timene har tilgang til journalen uten å være involvert i pasientbehandlingen. Riksrevisjonens mener disse funnene viser at mange ansatte gis tilgang til helseopplysninger uavhengig av om den enkelte ansatte er involvert i pasientbehandlingen.

Etter Riksrevisjonens vurdering viser undersøkelsen at helseforetakenes praksis for tilgangsstyring ikke er i samsvar med gjeldene regelverks krav om at ansattes tilgang til helseopplysninger skal være nødvendig for arbeidet vedkommende utfører (tjenstlig behov).

2.3 Helseforetakene har ingen systematisk kontroll og oppfølging av ansattes tilganger til EPJ

Ifølge prosedyrene har alle de fire helseforetakene delegert ansvaret for etterlevelse av vedtatte rutiner for tilgangsstyring og oppgavene med å tildele og administrere tilgangene til EPJ-systemet, til klinikk- eller avdelingsledere med budsjett- og personalansvar. Likevel viser undersøkelsen at det ikke er etablert rutiner for å administrere og vedlikeholde ansattes tilganger på avdelingsnivå. Avdelingene oppgir at dette er oppgaver som skal ivaretas av overordnet nivå. Samtidig viser undersøkelsen at overordnet nivå verken gjennomfører systematisk kontroll av tilganger eller følger opp at delegerte oppgaver blir utført. Riksrevisjonen mener dette viser at klinikk- og avdelingsnivå verken har tilstrekkelige ressurser eller verktøy til å ivareta det delegerte ansvaret for å sikre korrekt etterlevelse.

Etter Riksrevisjonens vurdering har helseforetakene mangelfullt grunnlag for å etterprøve om ansattes faktiske behov for bruk av aktualisert tilgang eller nødrettstilgang var tilstede. Dette fordi behovsbegrunnelsene som må oppgis er forhåndsdefinerte og lite tilrettelagt for de ansattes faktiske arbeidssituasjon og behov, og fordi EPJ-systemet gjør det mulig å overstyre kravet om reell behovsbegrunnelse ved å godta et hvilket som helst ord eller tegn.

Alle helseforetakene har utarbeidet prosedyrer som slår fast at loggkontroller av ansattes oppslag i pasientjournaler skal gjennomføres rutinemessig, både på eget initiativ, og basert på forespørsler fra pasienter. Likevel viser undersøkelsen at ingen av helseforetakene gjennomfører systematiske loggkontroller på eget initiativ for å avdekke ureglementerte oppslag, som for eksempel snoking. De få loggkontrollene som utføres er primært på forespørsel fra pasienter. Riksrevisjonen mener det nærmest vil være tilfeldig om helseforetakene oppdager snoking i pasientjournaler.

Departementet mener at det er en forutsetning ved vide tilgangsrettigheter at de følges opp med god logging og et velfungerende kontrollregime som sikrer at ansatte ikke

misbruker mulighetene. Riksrevisjonen mener derfor det er bekymringsfullt at undersøkelsen viser at helseforetakene verken har systematisk kontroll med oppslagene ansatte gjør i pasientjournalene, eller systematisk oppfølging av hvorvidt de ansattes tilganger er riktige ut fra faktisk behov.

Stortinget vedtok 20. juni 2014, ved endelig behandling av Innst. 295 L (2013–2014), jf. Prop. 72 L (2013–2014), at det skal kunne gis tilgang til helseopplysninger for ansatte på tvers av virksomheter. Dagens regelverk, som denne undersøkelsen tar utgangspunkt i, gir derimot kun tilgang til pasientjournaler for ansatte innad i egen virksomhet. Etter Riksrevisjonens vurdering vil lovendringen fordre at helseforetakene har et langt bedre kontrollregime enn det resultatet av denne undersøkelsen viser.

2.4 Helseforetakene har mangelfull internkontroll av tilgangsstyringen i EPJ

Helseforetakene er pålagt å ha internkontroll der databehandlingsansvarlige (administrerende direktør) skal etablere, vedlikeholde, dokumentere og gjøre tilgjengelig nødvendige systematiske tiltak. Likevel viser undersøkelsen at ingen av helseforetakene har etablert systematisk og integrert internkontroll for tilgangsstyring i EPJ-systemet.

Helseforetakene har fastsatt ambisiøse sikkerhetsmål for behandling av helseopplysninger. De er av overordnet karakter og i liten grad operasjonalisert. Samtlige helseforetak har en tilnærmet nullaksept på risiko for etterlevelse av sikkerhetsmålene, og legger til grunn at sikkerhetsbrudd ikke aksepteres. Samtidig viser undersøkelsen at helseforetakene verken har en systematisk oppfølging av risikovurderinger, eller gjennomfører sikkerhetsrevisjoner i samsvar med regelverket. Til tross for at helseforetakene har etablert en rutine for rapportering til ledelsen (ledelsens gjennomgang), er risikoene ledelsen får seg forelagt av svært overordnet karakter, og resultater fra gjennomførte risikovurderinger og avvikshåndtering blir i liten grad gjennomgått. Etter Riksrevisjonens vurdering innebærer dette at det ikke er samsvar mellom helseforetakenes fastsatte sikkerhetsmål, faktisk kontrollregime for tilgangsstyring og håndtering av risiko.

Utilstrekkelig kontroll på tilgangene i EPJ-systemet og fravær av systematisk og integrert internkontroll for tilgangsstyring, gjør etter Riksrevisjonens syn at administrerende direktør i helseforetakene ikke vil være i stand til å overholde sin lovpålagte plikt som databehandlingsansvarlig.

3 Riksrevisjonens anbefalinger

Riksrevisjonen anbefaler at:

- Helse- og omsorgsdepartementet pålegger de regionale helseforetakene å forsikre seg om at alle helseforetakene etterlever gjeldende regelverk for informasjonssikkerhet og behandling av helseopplysninger.

- Helse- og omsorgsdepartementet sørger for at pålegg i regelverket om føring av journalansvarlig person og gjennomføring av sikkerhetsrevisjoner blir tolket og praktisert ensartet.

- Helse- og omsorgsdepartementet og de regionale helseforetakene følger opp at helseforetakene har en hensiktsmessig tildelingspraksis som balanserer EPJ-systemets standardisering etter rolle og regelverkets pålegg om at tilgang skal være basert på individuelt tjenstlig behov.

- Helse- og omsorgsdepartementet og de regionale helseforetakene sørger for at det blir utviklet verktøy og iverksatt tiltak som er egnet for å oppdage urettmessig tilegnelse av helseopplysninger.

- De regionale helseforetakene følger opp at helseforetakene etablerer systematisk kontroll og oppfølging av ansattes tilganger, og at det etableres en tilstrekkelig internkontroll av tilgangsstyringen.

- Helseforetakene iverksetter tiltak som sikrer økt kunnskap om gjeldende regelverk og interne rutiner om behandling av helseopplysninger.

4 Departementets oppfølging

Statsråden opplyser at Riksrevisjonens merknader og anbefalinger fremstår som relevante og viktige for det videre arbeidet på området, og at anbefalingene vil bli fulgt opp gjennom krav om oppfølging og rapportering til de regionale helseforetakene i foretaksmøtet i januar 2015.

Statsråden viser til at det pågår et systematisk arbeid i de regionale helseforetakene for å rette opp forhold som Riksrevisjonen har påpekt i rapporten. Dette gjelder blant annet anbefalingene som omhandler helseforetakenes tolking og etterlevelse av regelverket. Statsråden viser dessuten til at det vil være naturlig at aktører som Nasjonal IKT HF, Helsedirektoratet og Norsk Helsenett SF bidrar inn i et samarbeid med de regionale helseforetakene, for å sikre at regelverket praktiseres så likt som mulig.

Statsråden viser videre til at departementet vil vurdere om det er behov for rundskriv eller annen informasjon om forståelsen av regelverket om informasjonssikkerhet og behandling av helseopplysninger. Ifølge statsråden kan dette være aktuelt i forbindelse med implementeringen av den nye pasientjournalloven og helseregisterloven.

Når det gjelder anbefalingen om at departementet og de regionale helseforetakene følger opp at helseforetakene har en hensiktsmessig tildelingspraksis, viser statsråden til at de regionale helseforetakene vil følge opp at tildelingen balanserer EPJ-systemets standardisering og vurdering av det enkelte helsepersonellets behov. Statsråden påpeker at pasienter med sammensatte lidelser, endringer i pasientforløpene, økt spesialisering og samhandling er forhold som innebærer at flere virksomheter er involvert i pasientbehandlingen enn tidligere, og at mange ansatte må ha tilgang til opplysninger, også på tvers av grensen mellom psykiatri og somatikk.

Statsråden opplyser at de regionale helseforetakene må arbeide videre med forbedring av systematisk kontroll og oppfølging av ansattes tilganger, og etablering av tilstrekkelig internkontroll av tilgangsstyringen. Ifølge statsråden vil Nasjonal IKT HF kunne ha en sentral rolle i dette arbeidet.

5 Riksrevisjonens sluttmerknad

Riksrevisjonen har merket seg at merknadene og anbefalingene framstår som relevante og viktige for departementets oppfølging av arbeidet på området. Riksrevisjonen vil likevel påpeke at Helse- og omsorgsdepartementet må sørge for at pålegg i regelverket, som i liten grad gir rom for ulik tolkning, blir praktisert ensartet.

leasing ikke var tillatt, jf. helseforetakslovens § 33, var dette i en periode der helseforetakene hadde store økonomiske utfordringer og det var bekymring for at helseforetakene skulle benytte leieavtaler som finansieringskilde for investeringsønsker, og på den måten å øke kostnadsnivået utover gitte rammer.

Statsråden opplyser at det er vurdert om det finnes områder der vedtektsbestemmelsen er til hinder for gode og hensiktsmessige løsninger. Med bakgrunn i dette har statsråden i statsbudsjettet for 2015 foreslått å gi de regionale helseforetakene åpning for å inngå leieavtaler for inntil 100 mill. kroner per avtale. Vedtektsendringer vil foretas i foretaksmøter i januar 2015.

4 Riksrevisjonens sluttmerknad

Riksrevisjonen har ingen ytterligere merknader.

Vedlegg 3.3: Rapport fra utvidet kontroll om styring og kontroll av tilgang til helseopplysninger i elektroniske pasientjournaler i fire helseforetak

1 Innledning

1.1 Bakgrunn

Stortinget har i mange år framhevet betydningen av informasjons- og kommunikasjonsteknologi (IKT) for å nå helse- og omsorgspolitiske mål om bedre kvalitet, pasientsikkerhet, effektivitet og ressursbruk.

Rask utveksling av helseopplysninger er viktig for å sikre god pasientbehandling og effektiv ressursutnyttelse i spesialisthelsetjenesten. Helseopplysninger er personidentifiserbar taushetsbelagt informasjon som er underlagt et strengt lovregulert behandlingsregime. Helseforetakene har flere elektroniske fagsystemer der helseopplysninger er registrert og lagret. Omfanget av sensitive opplysninger antas å være størst i systemet for elektroniske pasientjournaler (EPJ).

Ifølge Datatilsynets rapport *Sviktende tilgangsstyring i elektroniske pasientjournaler? Lovforslag om å tillate direkte tilgang til pasientjournaler på tvers av virksomhetsgrensene* fra april 2009 har helseforetakenes interne tilgangsstyring vært gjenstand for utstrakt kontroll og massiv kritikk fra både Datatilsynet og Helsetilsynet. Datatilsynets kontroller i helseforetakene i perioden 2005–2008 har vist at både helsepersonell og andre ansatte gjennomgående hadde altfor vid tilgang til å tilegne seg pasientopplysninger i den elektroniske journalen. Samtidig var virksomhetens kontroll med hvilke opplysninger den enkelte ansatte faktisk tilegnet seg, altfor svak.

Flere av de regionale helseforetakenes internrevisjoner har også gjennomført revisjoner om helseforetakenes internkontroll ved behandling av helseopplysninger. Internrevisjonen i Helse Nord RHF konkluderer i rapport nr. 7/2010 med at behandlingen av helseopplysninger på flere områder ikke var i samsvar med gjeldende regelverk, og at helseforetakenes opplegg for internkontroll hadde svakheter som burde forbedres. Internrevisjonen i Helse Midt-Norge RHF konkluderer i rapport datert 29. august 2013 at helseforetakene har god styring og kontroll på tilgangsstyringen i EPJ-systemet, men at det er svikt i andre rutiner knyttet til systemet.

1.2 Formål og problemstillinger

Formålet med undersøkelsen er å vurdere om helseforetakenes styring og kontroll av tilgang til helseopplysninger i systemet for elektroniske pasientjournaler er i samsvar med gjeldende regelverk.

Formålet vil bli belyst gjennom følgende problemstillinger:

1 I hvilken grad har helseforetakene tilstrekkelige prosedyrer og rutiner for tilgangsstyring i systemet for elektroniske pasientjournaler?
2 I hvilken grad har helseforetakene tilstrekkelig kontroll på den faktiske tilgangen i systemet for elektroniske pasientjournaler?

1.3 Revisjonskriterier

Krav til behandling av helseopplysninger

Opplysninger om helseforhold er definert som sensitive personopplysninger i personopplysningsloven.[123] Slike opplysninger kan bare behandles dersom behandlingen er nødvendig for forebyggende sykdomsbehandling, medisinsk diagnose, pasientbehandling eller for forvaltning av helsetjenester, og opplysningene behandles av helsepersonell med taushetsplikt.[124] Med behandling av helseopplysninger menes enhver formålsbestemt bruk av helseopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.[125]

Helseregisterloven[126] slår fast at enhver som behandler helseopplysninger, har taushetsplikt etter forvaltningsloven[127] og helsepersonelloven. Det innebærer at alle ansatte i helseforetakene, både helsepersonell og øvrige profesjoner, er underlagt taushetsplikt ved behandling av helseopplysninger. Videre pålegger helsepersonelloven[128] de ansatte å hindre at andre får tilgang eller kjennskap til opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold som de får vite om i egenskap av sin ansattrolle.

Spesialisthelsetjenesteloven[129] og helsepersonelloven[130] pålegger helseforetakene å tilrettelegge sine tjenester og organisere virksomheten slik at ansatte blir i stand til å overholde sine lovpålagte plikter.

Krav til tilgangsstyring

Ifølge helseregisterloven[131] og helsepersonelloven[132] er det forbud mot urettmessig tilegnelse av helseopplysninger. For ansatte som behandler helseopplysninger, er det uten at det er begrunnet i helsehjelp eller særskilt hjemlet i lov eller forskrift, forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold.

I henhold til helseregisterloven[133] kan tilgang til helseopplysninger bare gis den databehandlingsansvarlige, databehandlere og den som arbeider under disses instruksjonsmyndighet. *Databehandlingsansvarlig* er legaldefinert[134] som den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes, hvis ikke behandlingsansvaret er særskilt angitt i loven eller i forskrift i medhold av loven. Ansvaret skal ivaretas av den daglige ledelsen av virksomheten. Med virksomhet menes i denne sammenheng helseforetak. *Databehandler* er legaldefinert[135] som den som behandler helseopplysninger på vegne av den behandlingsansvarlige. Dette må være en ekstern person/virksomhet utenfor den databehandlingsansvarliges virksomhet (helseforetak). Tilgang skal bare gis i den grad det er nødvendig for arbeid vedkommende utfører og i samsvar med gjeldende bestemmelser om taushetsplikt.

En rekke pålegg om kontrolltiltak for å hindre uautorisert bruk av elektroniske systemer er gitt i personopplysningsforskriften[136]. Autorisert bruk av systemet skal

123) LOV 2000-04-14-31: Lov om behandling av personopplysninger § 2 nr. 8 bokstav c.
124) LOV 2000-04-14-31: Lov om behandling av personopplysninger § 9 bokstav g.
125) LOV 2001-05-18-24: Lov om helseregistre og behandling av helseopplysninger § 2 nr. 5.
126) LOV 2001-05-18-24: Lov om helseregistre og behandling av helseopplysninger § 15.
127) LOV 1967-02-10: Lov om behandlingsmåten i forvaltningssaker §§ 13 til 13 e.
128) LOV 1999-07-02-64: Lov om helsepersonell §§ 21 og 26.
129) LOV 1999-07-02-61: Lov om spesialisthelsetjenesten § 2-2.
130) LOV 1999-07-02-64: Lov om helsepersonell § 16.
131) LOV 2001-05-18-24: Lov om helseregistre og behandling av helseopplysninger § 13a.
132) LOV 1999-07-02-64: Lov om helsepersonell § 21a.
133) LOV 2001-05-18-24: Lov om helseregistre og behandling av helseopplysninger § 13, første ledd.
134) LOV 2001-05-18-24: Lov om helseregistre og behandling av helseopplysninger § 2 nr. 8.
135) LOV 2001-05-18-24: Lov om helseregistre og behandling av helseopplysninger § 2 nr. 9.
136) FOR 2000-12-15-1265: Forskrift om behandling av personopplysninger §§ 2-8, 2-11 og 2-14.

registreres. Det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig. Sikkerhetstiltak skal hindre uautorisert bruk av systemet og gjøre det mulig å oppdage forsøk på slik bruk. I helseregisterloven[137] slås det fast at pasienten har rett til utskrift av tilgangsloggen fra sin journal. Med logg menes en oversikt over aktivitet i systemet, blant annet over oppslagene brukerne av EPJ-systemet har gjort. For helseforetakene innebærer det at de er forpliktet til å logge tilgangen til systemet for elektroniske pasientjournaler. Hvordan loggene skal brukes, hva som skal logges, og hvordan loggene skal følges, er ikke regulert i personopplysningsforskriften, og avhenger derfor av helseforetakets vurderinger ved fastsettelsen av sikkerhetsmål og -strategier og ved gjennomføringen av risikovurderinger.

Krav til journal

Helsepersonelloven slår fast at den som yter helsehjelp, skal registrere i pasientens journal,[138] og at helsepersonell som yter helsehjelp, skal gis tilgang til alle helseopplysninger som er nødvendig for å gi forsvarlig helsehjelp, med mindre pasienten motsetter seg dette.[139]

Journal er definert som en samling eller sammenstilling av nedtegnede/registrerte opplysninger om en pasient i forbindelse med helsehjelp.[140] Det skal opprettes en journal for hver pasient, og som hovedregel skal det anvendes en samlet journal for den enkelte pasient selv om helsehjelp ytes av flere innen virksomheten.[141] Det skal også utpekes en person som har det overordnede ansvaret for den enkelte journal (*journalansvarlig*), og det skal framgå av journalen hvem dette er.[142]

Spesialisthelsetjenesteloven[143] pålegger helseforetakene å sørge for at journal- og informasjonssystemene er forsvarlige.

Krav til informasjonssikkerhet

Et datasystem som er laget for å oppbevare og organisere elektroniske pasientjournaler, er ifølge helseregisterloven[144] å anse som et behandlingsrettet helseregister. Formålet med helseregisterloven[145] er å sikre at helseopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på helseopplysningene.

Helseforetakene er pålagt å sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger gjennom planlagte og systematiske tiltak. For å oppnå tilfredsstillende informasjonssikkerhet skal den databehandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene, og dokumentasjonen skal være tilgjengelig.[146] For å oppfylle lovens krav er helseforetakene pålagt å ha internkontroll der databehandlingsansvarlige skal etablere, vedlikeholde, dokumentere og gjøre tilgjengelig nødvendige systematiske tiltak.[147]

En rekke pålegg om informasjonssikkerhet er gitt i personopplysningsforskriften[148]. Det skal fastsettes sikkerhetsmål for virksomheten og en sikkerhetsstrategi for å nå

137) LOV 2001-05-18-24: Lov om helseregistre og behandling av helseopplysninger § 13, siste ledd.
138) LOV 1999-07-02-64: Lov om helsepersonell § 39, jf. § 40.
139) LOV 1999-07-02-64: Lov om helsepersonell § 45.
140) FOR 2000-12-21-1385: Forskrift om pasientjournal § 3a), jf. helsepersonelloven § 40 første ledd.
141) FOR 2000-12-21-1385: Forskrift om pasientjournal § 5.
142) FOR 2000-12-21-1385: Forskrift om pasientjournal § 6.
143) LOV 1999-07-02-61: Lov om spesialisthelsetjenesten § 3-2.
144) LOV 2001-05-18-24: Lov om helseregistre og behandling av helseopplysninger § 2 nr. 7.
145) LOV 2001-05-18-24: Lov om helseregistre og behandling av helseopplysninger § 1.
146) LOV 2001-05-18 nr. 24: Lov om helseregistre og behandling av helseopplysninger § 16.
147) LOV 2001-05-18 nr. 24: Lov om helseregistre og behandling av helseopplysninger § 17.
148) FOR 2000-12-15-1265: Forskrift om behandling av personopplysninger §§ 2-3, 2-4, 2-5 og 2-7.

målene. Videre er det pålagt å gjennomføre og dokumentere sikkerhetsrevisjon av informasjonssystemet jevnlig, fastlegge kriterier for akseptabel risiko og utføre risikovurdering for å kartlegge sannsynlighet og konsekvens for sikkerhetsbrudd. Det skal også etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet.

1.4 Metode og gjennomføring

Problemstillingene i undersøkelsen er belyst ved dokumentanalyse, analyse av helseforetakenes svar på spørsmål i brev og testing av EPJ-systemet i fire utvalgte helseforetak. De utvalgte helseforetakene er Oslo universitetssykehus HF, Helse Bergen HF, St. Olavs Hospital HF og Universitetssykehuset Nord-Norge HF, som er de største helseforetakene i hver foretaksgruppe målt etter antall innbyggere i opptaksområdene.

Dokumentanalysen omfattet helseforetakenes prosedyrer for behandling av helseopplysninger og tilgangsstyring, fastsatte sikkerhetsmål, sikkerhetsstrategier og akseptabelt risikonivå for informasjonssikkerhet. Videre omfattet dokumentanalysen helseforetakenes planlagte og gjennomførte risikovurderinger, sikkerhetsrevisjoner og ledelsens gjennomgang av internkontroll for behandling av helseopplysninger for årene 2011–2013. Det er også innhentet og analysert noe tilleggsdokumentasjon fra de utvalgte avdelingene.

For å belyse helseforetakenes opplæring av ansatte i interne prosedyrer og gjeldende regelverk, herunder rutiner for tilgangsstyring og oppfølging av tilganger i EPJ-systemet for årene 2011–2013, er helseforetakene bedt om å svare skriftlig på spørsmål i brev. Svarene er sammenstilt og analysert.

Helseforetakenes praksis er belyst ved test av hovedjournal EPJ i fire avdelinger i hvert av de fire helseforetakene. Hovedjournal ble valgt siden den antas å være den applikasjonen med størst konsentrasjon av pasientenes helseopplysninger. For at undersøkelsen skulle dekke samtlige tre behandlingsområder, ble avdelingene valgt fra henholdsvis somatikk, psykisk helsevern og rus. Siden St. Olavs Hospital HF ikke hadde ansvar for rus før 1. januar 2014, viser tabellen at det der ble valgt to avdelinger innen psykisk helsevern. Hvilke avdelinger i de fire helseforetakene som ble valgt ut for testing, framgår av tabell 1.

Tabell 1 Oversikt over utvalgte avdelinger innen behandlingsområdene per helseforetak

Helseforetak/behandlingsområde	Somatikk	Psykisk helsevern	Rus
Oslo universitetssykehus HF	Hjertemedisinsk avdeling Avdeling for plastikk- og rekonstruktiv kirurgi	Josefinesgate DPS	Avdeling for avhengighetsbehandling voksne
Helse Bergen HF	Nevrologisk avdeling Hudavdelingen	Kronstad DPS	Avdeling for rusmedisin, poliklinikk voksne
St. Olavs Hospital HF	Lungeavdelingen Avdeling for karkirurgi	Nidaros DPS Trondheimsklinikken	
Universitetssykehuset Nord-Norge HF	Kvinneklinikken Anestesi- og operasjonsavdelingen	Psykiatrisk senter for Tromsø og omegn	Ruspoliklinikken

Testene var en kombinasjon av intervju, deltakende observasjon og stikkprøver i utvalgte pasientjournaler. Utvalget av journaler er gjort ut fra lister over utskrevne pasienter, anonymisert med bruk av nr. (pasient-ID), ved hver av de fire utvalgte avdelingene i perioden 1. oktober–31. desember 2013.

Testene, som ble gjennomført i april–mai 2014, omfattet rutiner for systempålogging og bestilling av tilganger, kontroll av journallogger og ansattes bruk av tildelte tilganger til journaler innen egen avdeling og behandlingsområde og på tvers av behandlingsområder. Testene er gjennomført av bemyndigede ansatte i hvert helseforetak/avdeling etter konkret bestilling fra revisjonen, mens revisjonen observerte og fylte ut testresultatet i kontrollskjemaer. Utfylte kontrollskjemaer for hver avdeling ble verifisert og signert av en representant for helseforetaket og undersøkelsens prosjektleder, som beholdt hvert sitt signerte eksemplar. I forbindelse med testene er også oversikter over ansattes tilgangsrettigheter innhentet.

Helseforetakene grupperer tilgangene til EPJ-systemet for de ansatte etter mange forskjellige roller. Revisjonen har konsentrert seg om tilgangsrettighetene til legerollen, sykepleierrollen og sekretærrollen, og har analysert helseforetakenes tilgangsstyring ut fra tre aspekter. Det første er hvilke tilgangsrettigheter de ulike ansattrollene har til pasientjournalene. Det andre er hvilken informasjon de ansatte har tilgang til. Det tredje og siste er hvor lenge de ansatte har tilgang til informasjonen.

Siden undersøkelsens tema grenser nært opp til tilsynsmyndighetens mandat og oppgaver, har revisjonen hatt dialog med Datatilsynet.

2 Resultatet av undersøkelsen

2.1 Er tilgang til helseopplysninger i EPJ-systemet basert på reelt behov?

2.1.1 Helseforetakenes systemer for elektroniske pasientjournaler

Det er hovedsakelig to leverandører av system for elektroniske pasientjournaler (EPJ-system) til helseforetakene. Disse er DIPS ASA, som leverer systemet DIPS, og Siemens, som leverer systemet Doculive.

Universitetssykehuset Nord-Norge HF og Helse Bergen HF bruker DIPS, men ulike versjoner av systemet. St. Olavs Hospital HF bruker Doculive. Oslo universitetssykehus HF er alene om å bruke begge systemene, men har eldre versjoner enn de andre helseforetakene. Tre av fire utvalgte avdelinger i Oslo universitetssykehus HF bruker Doculive, mens en avdeling (rus-området), som tidligere var lokalisert på Aker, bruker en gammel versjon av DIPS. Systemene Doculive og DIPS er ikke kompatible. Det innebærer at samme pasient eventuelt må ha en pasientjournal i hvert system samtidig. Oslo universitetssykehus HF oppgir at det planlegger å innføre felles integrert DIPS-system for hele helseforetaket i oktober 2014.

For øvrig viser undersøkelsen at DIPS ved Universitetssykehuset Nord-Norge HF ikke har en fødemodul. Kvinneklinikken der bruker derfor i stedet et annet system, Partus, som er tilpasset kravene til fødselsregisteret. Partus er ikke kompatibelt med DIPS, noe som innebærer at samme pasient eventuelt må ha en journal i hvert system samtidig. Departementet påpeker at alle helseforetak bruker et eget system for fødejournal, og at dette ikke er spesielt for Universitetssykehuset Nord-Norge HF. Partus brukes av helseforetakene i Helse Nord og Helse Sør-Øst, mens helseforetakene i Helse Midt-Norge og Helse Vest bruker Natus.

2.1.2 Prosedyrer og rutiner for behandling av helseopplysninger

Alle de fire helseforetakene har utarbeidet skriftlige prosedyrer for behandling av helseopplysninger. Prosedyrene er i hovedsak av overordnet karakter og langt på vei en gjengivelse av lov og forskrift som regulerer hvordan sensitiv taushetsbelagt personidentifiserbar informasjon, som helseopplysninger, skal behandles.

Helseforetakene oppgir at utarbeidet skriftlig materiell er elektronisk tilgjengelig for de ansatte, og at det er etablert obligatorisk opplæring, blant annet gjennom e-læringskurs. Samtidig viser undersøkelsen at helseforetakene ikke utpeker eller fører opp journalansvarlig, slik som forutsatt i forskrift om pasientjournal § 6, og at de mangler kunnskap om hva ansvaret for rollen som journalansvarlig innebærer. Ved Universitetssykehuset Nord-Norge HF ble det i forbindelse med testene oppgitt at praksisen med å ikke føre opp journalansvarlig, er basert på en sentral beslutning.

2.1.3 Prosedyrer og rutiner for pålogging i EPJ-systemet

Alle de fire helseforetakene har skriftlige prosedyrer for personlig og individuell systempålogging og autentisering. Med unntak av St. Olavs Hospital HF vil systemene generere krav om at de ansatte i helseforetakene skal bytte passord.

Ved testene i Oslo universitetssykehus HF ble det i tre av de fire avdelingene oppgitt at ansatte har lånt hverandres bruker-ID og passord. I Helse Bergen HF oppgir én avdeling at lån av bruker-ID og passord har skjedd flere ganger inntil en intern omorganisering ble gjennomført i 2013. St. Olavs Hospital HF er det eneste helseforetaket der de ansatte må bruke individuelt ID-kort og kortleser i tillegg til passordpålogging. Undersøkelsen viser at passord i hovedsak ikke byttes. For eksempel har én ansatt aldri byttet passord i løpet av de 9 årene vedkommende har jobbet i St. Olavs Hospital HF. I Universitetssykehuset Nord-Norge HF oppgir alle de fire utvalgte avdelingene at passord byttes hver 3. måned og at ingen ansatte låner hverandres bruker-ID og passord.

2.1.4 Prosedyrer og rutiner for tilgangsstyring

Ifølge prosedyrene har alle de fire helseforetakene delegert ansvaret for korrekt etterlevelse av vedtatte rutiner for tilgangsstyring og oppgavene med å tildele tilgangene til EPJ-systemet til klinikk- eller avdelingsledere med budsjett- og personalansvar. Delegeringen innebærer vide fullmakter for lederne til å beslutte hvem som skal ha hvilke tilgangsrettigheter til systemet.

Helseforetakene har fastsatt prinsipper for tilgangsrettigheter i EPJ-systemet. Prinsippene slår fast at det må foretas en konkret vurdering av hvilke opplysninger den enkelte skal få tilgang til, basert på det som er nødvendig for å kunne yte forsvarlig helsehjelp. I EPJ-systemet opererer helseforetakene med de tre tilgangsrettighetene som er beskrevet i faktaboks 1.

Faktaboks 1 Tilgangsrettigheter til EPJ-systemet brukt av helseforetakene

Normal tilgang: Gir ansatte automatisk tilgang til hele eller deler av pasientjournalen til pasienter som er i et aktivt behandlingsforløp ut fra hva ansatte i kraft av sin rolle, organisatorisk tilhørighet og arbeidsoppgaver har behov for.

Aktualisert tilgang: Gir ansatte samme tilgang som normal tilgang til pasientjournalen til pasienter som ikke er innlagt enda, som er innlagt på annen avdeling/enhet eller som er utskrevet. Forutsetter at det oppgis en begrunnelse for tilgangsbehovet som blir registrert i systemet.

Nødrettstilgang: Gir ansatt tilgang til pasientjournal på samme måte som ved aktualisering, men utvidet til alle pasienter på tvers av områdene somatikk, psykisk helsevern og rus. Forutsetter at det oppgis en begrunnelse for tilgangsbehovet som blir registrert i systemet.

Undersøkelsen viser at det gjennomgående er lite kunnskap i helseforetakene om de ulike tilgangsrettighetene og manglende innsikt i når de skal brukes. Videre viser undersøkelsen at begrunnelsene som må oppgis ved behov for aktualisert tilgang og nødrettstilgang, er forhåndsdefinerte. De ansatte oppgir at de forhåndsdefinerte begrunnelsene i for liten grad er tilrettelagt for faktisk arbeidssituasjon og behov. EPJ-systemet i alle helseforetakene gjør det dessuten mulig å overstyre kravet om en reell behovsbegrunnelse ved at et hvilket som helst tegn eller ord godtas som begrunnelse. Dette gjør det vanskelig å etterprøve hvorvidt de oppgitte behovsbegrunnelsene ved aktualisert tilgang og nødrettstilgang har vært reelle.

Organisering av tilgangsrettigheter i EPJ-systemene baseres på de ansattes roller (profesjon og arbeidsoppgaver) og arbeidssted (tilhørighet til behandlingsområde/klinikk/avdeling). Dette innebærer at de ansatte skal få tilgang til pasientjournalen ut fra hva de i kraft av sin rolle og sine arbeidsoppgaver vil ha behov for.

Selv om helseforetakene har tre behandlingsområder, viser undersøkelsen at EPJ-systemene kun opererer med to områder: ett for somatikk og ett for psykisk helsevern/rus. I den videre framstillingen blir derfor disse omtalt som systemområder. Hver enkelt pasientjournal skiller mellom disse to systemområdene, og består av en rekke ulike dokumentkategorier som for eksempel epikrise, legenotat, sykepleienotat og oversikt over pasientens kontakter med helseforetaket (innleggelser og polikliniske konsultasjoner).

Tilgangsrettigheter til de ulike rollene i helseforetakene

Normal tilgang
For Oslo universitetssykehus HF viser dokumentanalysen at tildeling av tilgang til EPJ-systemet skal skje ut fra standardiserte roller med noe tilpasning til hvilken avdeling/enhet den ansatte arbeider ved. Leger og en del sekretærer gis normal tilgang på avdelingsnivå på tvers av underliggende seksjoner/enheter. Lege med selvstendig behandleransvar gis normal tilgang på tvers av systemområdene somatikk og psykisk helsevern, mens sykepleier skal ha normal tilgang begrenset til postnivå. Stikkprøvene i utvalgte pasientjournaler viser tilfeller av at ansatte har ubrukte normale tilganger som ikke er avsluttet, noe som gir ansatte i Oslo universitetssykehus HF tilganger til helseopplysninger de ikke lenger har behov for.

For Helse Bergen HF viser dokumentanalysen at tilgangsstyringen er basert på regionale føringer om at ansatte skal ha tilgang etter hvilken rolle vedkommende har overfor pasienten, og at tilgang skal gis til den eller de enhetene som omfattes av ved-

kommendes ansvars- og arbeidsområde. Det skal være felles journal på tvers av både avdelinger og systemområdene somatikk og psykisk helsevern/rus. Leger og en del sekretærer gis normal tilgang på avdelingsnivå på tvers av underliggende seksjoner/enheter, mens sykepleiere i utgangspunktet gis normal tilgang begrenset til egen enhet. Stikkprøvene i utvalgte pasientjournaler viser at ansatte ved behov tildeles flere tilgangsroller til EPJ-systemet, og at ubrukte normale tilganger i hovedsak blir avsluttet.

St. Olavs Hospital HF oppgir i brev at det generelle utgangspunktet for tilgangsstyring er at det ikke skal gis normal tilgang til EPJ-systemet på tvers av systemområdene somatikk og psykisk helsevern/rus. Likevel viser dokumentanalysen at lege i somatikken skal gis standardisert normal tilgang til psykisk helsevern/rus, mens lege i psykisk helsevern/rus automatisk skal gis tilgang til somatikken. Tilsvarende gjøres for sykepleiere og sekretærer, men da etter vurdering av tjenstlig behov. Tilsendt oversikt viser for øvrig at det er mange andre roller som har normal tilgang på tvers av systemområdene. Oversikten i dokumentene viser blant annet flere tilfeller av at fysioterapeuter, hjelpepleiere, ernæringsfysiologer og farmasøyter i somatikken har normal tilgang til pasientjournaler i psykisk helsevern/rus. Også sosionomer, vernepleiere og ergoterapeuter i psykisk helsevern/rus har tilgang til pasientjournaler i somatikken. Videre viser stikkprøver flere tilfeller av ubrukte tilganger som ikke er avsluttet, noe som innebærer at ansatte i St. Olavs Hospital HF har tilganger til helseopplysninger de ikke lenger har behov for.

Undersøkelsen viser at Universitetssykehuset Nord-Norge HF er det eneste helseforetaket som baserer tilgangsstyringen på at det skal skilles tydelig mellom somatikk og psykisk helsevern/rus, og at det ikke skal gis normal tilgang på tvers av systemområdene for noen roller. Testene viser at det benyttes standardroller for de ulike yrkesgruppene basert på tilhørighet og funksjon der normal tilgang gis for registrerte pasienter ved avdelingen. Dokumentanalysen viser at lege har normal tilgang til pasientjournaler for avdelinger innen samme systemområde og på tvers av avdelinger, mens sykepleiers tilgang er begrenset til egen avdeling, enhet eller sengepost. Leger som går vakt, får i tillegg en utvidet vaktrolle som gir tilgang på tvers av avdelinger. Stikkprøver viser at jordmødre har bred normal tilgang på tvers av geografiske lokasjoner (sykehus) siden alle lokasjoner organisasjonsmessig tilhører samme avdeling.

Aktualisert tilgang
For Oslo universitetssykehus HF viser testene at leger i de tre utvalgte avdelingene, som bruker Doculive-systemet, har lik tilgang til pasientjournaler på tvers av systemområdene somatikk og psykisk helsevern ved bruk av aktualisering. Stikkprøver i de utvalgte avdelingene viser at når sykepleiere aktualiserer, får de både tilgang til informasjon om pasientens kontakt (innleggelser og polikliniske konsultasjoner) ved egen avdeling og annen avdeling innen samme systemområde. Sykepleiere får ikke tilgang på tvers av systemområdene. Ved én av disse tre avdelingene var det ikke kjent for verken sykepleier selv, seksjonsleder eller avdelingsleder at vedkommende kunne bruke aktualisert tilgang.

For Helse Bergen HF viser testene at leger i alle de fire utvalgte avdelingene har tilgang til pasientjournaler på tvers av systemområdene somatikk og psykisk helsevern/rus ved bruk av aktualisering. Stikkprøver viser at sykepleiere kan aktualisere pasientjournaler for egen avdeling og annen avdeling innen samme systemområde, men ikke på tvers av somatikk og psykisk helsevern/rus.

Undersøkelsen viser at St. Olavs Hospital HF skiller seg ut fra de øvrige tre helseforetakene ved å gi svært mange ansatte innen mange roller rett til å bruke aktualisert tilgang. Tilsendt oversikt viser at både lege, sykepleier (på avdelingsnivå, operasjon og poliklinikk) og sekretær har rett til å bruke aktualisert tilgang. Stikkprøver i de utvalgte avdelingene viser at sykepleiere kan aktualisere pasientjournaler for egen avdeling, annen avdeling innen samme område og på tvers av systemområdene somatikk og psykisk helsevern/rus. Ved én avdeling innen psykisk helsevern/rus var det overhodet ikke kjent for sykepleier at vedkommende hadde tilgang til somatikk.

For Universitetssykehuset Nord-Norge HF viser dokumentanalysen at lege har aktualisert tilgang til pasientjournaler for avdelinger innen samme systemområde og på tvers av avdelinger, mens sykepleiers aktualiserte tilgang er begrenset til egen avdeling, enhet eller sengepost. Testene viser at ingen av de undersøkte rollene har aktualisert tilgang på tvers av systemområdene.

Nødrettstilgang
Undersøkelsen viser at nødrettstilgang ikke er i bruk ved Oslo universitetssykehus HF og St. Olavs Hospital HF. Både ved Helse Bergen HF og Universitetssykehuset i Nord-Norge HF er nødrettstilgang i bruk, men det er vanligvis kun leger som gis denne rettigheten. Tilsendt oversikt viser derimot at det i Universitetssykehuset i Nord-Norge HF er langt flere roller enn leger som har rett til å bruke nødrettstilgang, som eksempelvis sykepleier, sekretær, hjelpepleier, barnepleier og pleiemedhjelper. I Universitetssykehuset i Nord-Norge HF er det kun nødrettstilgang som gir tilgang på tvers av systemområdene somatikk og psykisk helsevern/rus.

Informasjonen de ansatte i helseforetakene har tilgang til
Testene viser at ansatte ved de utvalgte avdelingene i helseforetakene som bruker DIPS-systemet, uten å bruke tilgangsrettigheter for å åpne selve pasientjournalen, kan se samtlige kontakter (innleggelser og polikliniske konsultasjoner) en pasient har hatt med helseforetaket innen både somatikk og psykisk helsevern/rus. Videre kan de ansatte, uavhengig av rolle, se samtlige henvisninger for den enkelte pasient, der mye sensitiv informasjon som diagnoser og DRG-koder kan være tilgjengelig. Ved stikkprøver i Helse Bergen HF kom det fram at svært mye sensitiv informasjon var tilgjengelig i henvisningene. Stikkprøver i Universitetssykehuset Nord-Norge HF viser at mange dokumenter med sensitiv informasjon rutinemessig blir scannet og lagret i pasientjournal som bilder. Disse bildene er tilgjengelig for alle ansatte i hele helseforetaket på tvers av systemområdene somatikk og psykisk helsevern/rus.

Ved St. Olavs Hospital HF og de delene av Oslo universitetssykehus HF som bruker Doculive, er tilsvarende informasjon ikke tilgjengelig for de ansatte i EPJ-systemet, men i de pasientadministrative systemene.

Videre viser testene at Helse Bergen HF differensierer hvilken informasjon i pasientjournalen lege har tilgang til, ut fra hvilket systemområde vedkommende tilhører. Dette innebærer at lege innen psykisk helsevern/rus har en videre tilgang til informasjon fra somatikk enn det lege i somatikk har til informasjon fra psykisk helsevern/rus. Ved Universitetssykehuset Nord-Norge HF gir bruk av aktualisering kun tilgang til informasjon om pasienter i det systemområdet vedkommende tilhører. Ved både Helse Bergen HF og Universitetssykehuset Nord-Norge HF viser stikkprøver at rollene de ansatte har, gir forskjellige muligheter til å velge forhåndsdefinerte behovsbegrunnelser ved bruk av aktualisering, og at de forskjellige behovsbegrunnelsene gir ulik tilgang til informasjon i pasientjournalen.

For Oslo universitetssykehus HF viser testene at bruk av aktualisering faktisk innebærer en vid tilgang til hele DIPS-systemet på tvers av den ansattes tilhørighet og systemområder, nærmest som en nødrettstilgang. For øvrig kom det fram at personnummeret til alle i Norge som er registrert i folkeregisteret, kan søkes opp i DIPS-systemet av de ansatte ved Oslo universitetssykehus HF.

Ansattes tilgang til informasjon i forkant og etterkant av innleggelse eller konsultasjon

Universitetssykehuset Nord-Norge HF, St. Olavs Hospital HF og Oslo universitetssykehus HF oppgir at de ansatte, ved bruk av normal tilgang, ikke skal ha tilgang til pasientens journal i forkant av innleggelse eller konsultasjon. Tilgang i forkant fordrer bruk av aktualisert tilgang. Helse Bergen HF derimot oppgir at de ansatte får tilgang til pasientens journal ved bruk av normal tilgang sju dager i forkant av innleggelse eller konsultasjon.

Testene viser at det St. Olavs Hospital HF oppgir stemmer, mens pasientjournalen i Universitetssykehuset Nord-Norge HF blir tilgjengelig for de ansatte ved normal tilgang når henvising er vurdert og behandling besluttet, eller når operasjonsmelding er opprettet. For Oslo universitetssykehus HF viste testene en nyansering for systemområdet psykisk helsevern/rus om at pasientens journal er tilgjengelig ved normal tilgang fra pasienten er satt på venteliste. I Helse Bergen HF oppgir de ansatte i systemområdet psykisk helsevern/rus at de må aktualisere for å få tilgang til pasientens journal i forkant, i strid med det helseforetaket oppgir om normal tilgang sju dager i forkant.

Hvor lenge de ansatte har tilgang til pasientens journal i etterkant av utskrivning eller avsluttet konsultasjon ved bruk av normal tilgang, varier mellom 14 dager i Oslo universitetssykehus HF, 30 dager i Universitetssykehuset Nord-Norge HF og St. Olavs Hospital HF og 60 dager i Helse Bergen HF.

Ved testene i Oslo universitetssykehus HF oppga ansatte i én avdeling innen systemområdet psykisk helsevern/rus at det ikke var noen tidsbegrensning i etterkant, og at journalen forble tilgjengelig med normal tilgang siden vedkommende ikke hadde rett til å bruke aktualisert tilgang. Dette ble bekreftet ved stikkprøve.

Stikkprøve i Universitetssykehuset Nord-Norge HF viser at en pasientjournal tilhørende systemområdet psykisk helsevern/rus var tilgjengelig for lege i somatikken med normal tilgang. Dette til tross for at pasientens siste kontakt med helseforetaket innen somatikken var november 2013. Dette innebærer at journalen har vært åpen lenger enn de oppgitte 30 dagene etter utskrivning eller avsluttet konsultasjon.

Utgangspunktet ved aktualisert tilgang er at det er den enkelte ansattes tilgang som gjøres normal for en bestemt tidsperiode når tilgangsbehovet er oppgitt og registrert. Undersøkelsen viser at denne tidsperioden varierer fra 1 time i Oslo universitetssykehus HF til 24 timer i Universitetssykehuset Nord-Norge HF. Videre viser testene at bruk av aktualisering i Universitetssykehuset Nord-Norge HF faktisk gjør at selve pasientjournalen blir åpen gjennom normal tilgang for ansatte på tvers av systemområdene i 24 timer.

2.2 Er det tilstrekkelig kontroll og oppfølging av tilgang til EPJ-systemet?

2.2.1 Kontroll av journallogger

EPJ-systemene genererer logger over hvilke ansatte som har foretatt oppslag i pasientjournaler, når oppslaget blir foretatt, hvilken tilgangsrettighet som er benyttet, hva

slags dokument det har vært gjort oppslag i, hvem som har skrevet hva, og behovsbegrunnelser ved aktualisering og nødrettstilgang.

Med unntak av Oslo universitetssykehus HF har helseforetakene utarbeidet skriftlige prosedyrer for gjennomføring av logganalyser. Prosedyrene viser at helseforetakene skal gjennomføre rutinemessige loggkontroller, både egeninitierte, og basert på forespørsler fra pasienter. Ved Universitetssykehuset i Nord-Norge HF og St. Olavs Hospital HF er det spesifisert at det skal gjennomføres rutinemessige loggkontroller kvartalsvis. Helseforetakene oppgir at formålet med loggkontroll blant annet er å kontrollere om det snokes i pasientjournalene, og om det har vært oppslag og aktivitet det ikke har vært grunnlag for å gjøre.

Prosedyren viser at det ved St. Olavs Hospital HF er avdelings-/divisjonsklinikksjef som har ansvaret for å etablere rutiner for kontroll av logger. St. Olavs Hospital oppgir at det kun er disse som har en reell mulighet til å vurdere loggene opp mot tjenstlige behov. Den som får delegert oppgaven med å kontrollere, skal innhente logger og vurdere loggene opp mot ansattes tjenstlige behov.

Helse Bergen HF har skriftlig prosedyre for ulike loggkontrolltiltak der journalansvarlig person er tildelt konkret oppgave. Ved kontrolltiltaket rutinemessig kontroll skal journalansvarlig bestille utskrift av logg fra IT-sikkerhetsleder ved behandlingsslutt eller ved mistanke om uregelmessigheter.

Prosedyren for Universitetssykehuset i Nord-Norge HF viser at ved rutinekontroll skal Sikkerhetssjef IKT kjøre systematisk kontroll på seks pasienter. Ved konkret mistanke om innsyn kan avdelingssjef eller journalansvarlig person be om stikkprøvekontroll av innsynslogg. Klinikkleder eller avdelingsdirektør utpeker da en lege ved klinikken som bestemmer hvilke pasienter stikkprøve skal foretas på. Den som skal utføre kontrollen, har ikke automatisk tilgang til loggene, og må derfor få tildelt tilgang for en gitt tidsperiode for å kunne analysere loggene. Ifølge prosedyren kan det også gjennomføres kontroll av logger for nødrettstilgang.

Oslo universitetssykehus HF har ikke en skriftlig prosedyre for loggkontroll, men oppgir at det gjennomføres stikkprøver der det velges ut logger for noen pasienter. Disse gjennomgås for å se om det har vært gjort oppslag i journalene som ikke kan forklares. Det er normalt profilerte personers logger som gjennomgås. Dersom pasientene selv mener eller stiller spørsmål ved om det har vært uberettigede oppslag, blir loggene gjennomgått.

Undersøkelsen viser at antallet pasientjournaler, antallet dokumenter i journalene og antallet oppslag i pasientjournaler i helseforetakene er av et betydelig omfang. For eksempel oppgir Oslo universitetssykehus HF at det er mer enn 100 millioner oppslag i pasientjournaler per år. Samtidig viser undersøkelsen at helseforetakene i liten grad gjennomfører rutinekontroller og stikkprøvekontroller av pasientjournallogger. Ved Universitetssykehuset i Nord-Norge HF har det i perioden 2011–2013 blitt gjennomført 45 loggkontroller. St. Olavs Hospital HF har ikke en komplett oversikt, men anslår at det gjennomføres omtrent ti loggkontroller per år. Oslo universitetssykehus HF oppgir at det gjennomføres halvårlige gjennomganger av høyprofilerte personers logger, samt logger der pasienter mener det er grunnlag for mistanke. Helse Bergen HF oppgir at det utfører fast månedlig gjennomgang av logg for bruk av nødrettstilgang, og at andre kontroller utføres sporadisk.

Ved stikkprøver i helseforetakene kom det fram at ingen av de utvalgte avdelingene på eget initiativ gjennomførte loggkontroller, og de fleste avdelingene kjente heller ikke

til hvordan de kunne få tilgang til pasientjournalloggene. Undersøkelsen viser at loggene må bestilles særskilt fra sentralt ansatte, og at dette ikke gjøres. Med unntak av én avdeling innen systemområdet psykisk helsevern/rus i ett av helseforetakene, er det ingen andre avdelinger i helseforetakene som på eget initiativ kontrollerer om de ansatte etterlever fastsatte rutiner og regelverk.

Alle helseforetakene oppgir at dagens løsninger for loggkontroll ikke er egnet til å avdekke snoking. Omfanget av pasientjournaler og antallet oppslag er så stort at manuelle loggkontroller er lite effektivt for å avdekke ureglementerte oppslag, og at sannsynligheten for å avdekke snoking er liten. St. Olavs Hospital HF oppgir blant annet at de tilfellene der det er avdekket snoking, har vært basert på konkrete mistanker og tips fra pasienter. Alle de fire helseforetakene viser til et pågående prosjekt som etter planen skal levere en sluttrapport i mars 2015. Prosjektet kalles "Mønstergjenkjenningsprosjektet" og går ut på å etablere en statistisk metode for kontroll av logger basert på gjenkjenning av avvik.

Departementet kommenterer i sitt svar at tilgangsstyring alene ikke kan sikre at helsepersonell bare får tilgang til nødvendig informasjon, og at det er nødvendig med et samspill av virkemidler. Departementet poengterer at det er en forutsetning ved vide tilgangsrettigheter at det følges opp med god logging og et velfungerende kontrollregime som sikrer at helsepersonellet ikke misbruker mulighetene.

2.2.2 Administrering av tilganger

I alle de fire helseforetakene er oppgavene med å tildele og administrere tilganger til EPJ-systemet delegert til klinikk- eller avdelingsledere med budsjett- og personalansvar. Likevel viser testene at de utvalgte avdelingene i helseforetakene ikke har rutiner for å administrere og vedlikeholde ansattes tilganger ved bytte av arbeidssted internt. Siden tilgang til EPJ-systemet blir stoppet ved opphør av lønn, har imidlertid helseforetakene bedre system for å avslutte tilganger når ansattes arbeidsforhold opphører.

Undersøkelsen viser at helseforetakene verken har systematisk kontroll med at ansatte har de riktige tilgangene i avdelingene eller sentralt i helseforetaket. Det utarbeides ikke rapporter over aktive tilganger, og det er ingen systematisk kontroll med at tildelte tilganger avsluttes når ansatte bytter jobb internt i helseforetakene. Videre viser testene at alle helseforetakene har ansatte med tilganger de ikke lenger har tjenstlig behov for. Stikkprøver viser at ubrukte tilganger ikke er avsluttet, at ansatte har rett til aktualisert tilgang både innen egen avdeling og på tvers av systemområder, uten at de selv var kjent med dette. Alle helseforetakene erkjenner at de ikke har tilfredsstillende rutiner for å vaske og administrere de ansattes tilganger til EPJ-systemet.

2.3 Hvordan er det overordnede ansvaret for tilgangsstyring ivaretatt?

Det er administrerende direktør som har ansvaret for informasjonssikkerheten og de ulike informasjonssystemene i helseforetakene, gjennom rollen som databehandlingsansvarlig. De fire helseforetakene har organisert sikkerhetsarbeidet noe ulikt, men alle har definert ansvars- og myndighetsforhold for bruk av systemene og egne roller som skal ivareta informasjonssikkerhetsarbeidet i den daglige driften. Alle helseforetakene har også opprettet eget personvernombud som har et særlig ansvar for å følge opp behandlingen av helse- og personopplysninger. Det er likevel administrerende direktør som har det overordnede ansvaret for informasjonssikkerheten, og herunder tilgangsstyringen i EPJ.

2.3.1 Styrende dokumenter

Helseforetakene har utarbeidet styrende dokumenter i samsvar med regelverket, men dokumentene er generelle og i varierende grad operasjonalisert. Sikkerhetsmålene er av overordnet karakter, og for tilgangsstyringen begrenser de seg til å omtale at det kun er autorisert personell med tjenstlig behov som skal ha tilgang til systemene og/ eller helse- og personopplysningene.

Tre av fire helseforetak har i hvert sitt dokument på overordnet nivå fastlagt kriterier for akseptabelt risikonivå. Helse Bergen HF har ikke fastlagt akseptkriterier i et slikt dokument. I svarbrev erkjenner Helse Bergen HF manglende oppfølging av akseptabel risiko. Helseforetaket redegjør for at akseptkriterier hovedsakelig settes i den enkelte risikovurdering, og at ansvaret med oppfølgingen faller tilbake på ledere i linjen.

Samtlige helseforetak har en tilnærmet nullaksept på risiko for etterlevelse av fastsatte sikkerhetsmål, og legger til grunn at sikkerhetsbrudd ikke aksepteres. St. Olavs Hospital HF har det strengest formulerte kriteriet der det spesifiseres at det er nulltoleranse for at informasjon om pasienter gjøres tilgjengelig for feil person. Både Oslo universitetssykehus HF og Universitetssykehuset Nord-Norge HF erkjenner at det er sannsynlig at sikkerhetsbrudd kan forekomme, og har nyansert akseptkriteriene med utgangspunkt i at sikkerhetstiltak skal redusere risikoen knyttet til informasjonssikkerhet.

Sikkerhetsstrategiene skal beskrive helseforetakenes valg og prioriteringer i sikkerhetsarbeidet. Alle helseforetakene har beskrevet strategier for å oppnå sikkerhetsmålene og nivå for akseptabel risiko, men detaljnivået i strategiene varierer. Både Helse Bergen HF og Universitetssykehuset Nord-Norge HF har utarbeidet sikkerhetsstrategiene regionalt. Sikkerhetsstrategien som gjelder for Helse Bergen HF, er svært overordnet og generell, og mangler lokal tilpasning. De tre øvrige helseforetakene har beskrevet mer konkrete tiltak for å oppnå sikkerhetsmål og akseptabelt risikonivå, men strategiene er i liten grad operasjonalisert. Formuleringer som at noe skal være "tilstrekkelig", eller at man skal sikre "nødvendig" informasjonssikkerhet, er gjennomgående for alle helseforetakenes sikkerhetsstrategier.

2.3.2 Internkontroll

I helseforetakenes egne skriftlige prosedyrer framkommer det at det skal etableres internkontroll relatert til informasjonssikkerhet slik det forutsettes i regelverket. Det varierer hvor utfyllende beskrivelsen av den planlagte internkontrollen er, men helseforetakene oppgir at risikovurderinger, avviksbehandling, revisjoner og rapportering til ledelsen er sentralt i oppfølgingen av styringen med informasjonssikkerhet.
I tillegg er viktige internkontrollmomenter omtalt i helseforetakenes sikkerhetsstrategi eller i beskrivelsen av ansvarsroller i organiseringen av sikkerhetsarbeidet. Undersøkelsen viser imidlertid at det er tydelige mangler i den faktiske gjennomføringen av tiltakene som skal sikre tilstrekkelig internkontroll.

Risikovurderinger

Samtlige helseforetak mangler en systematisk oppfølging av risikovurderinger. Det er samtidig stor variasjon mellom helseforetakene i antall gjennomførte risikovurderinger for perioden 2011–2013.

Til tross for at alle helseforetakene har rutiner og maler som tilsier at det skal settes frister og ansvarlig person for sikkerhetstiltakene, gjøres dette i liten grad i de oversendte risikovurderingene. Oslo universitetssykehus HF og Universitetssykehuset Nord-Norge HF oppgir at det benyttes frist og ansvarlig person for iverksettelse av

tiltak, men en gjennomgang av de oversendte risikovurderingene viser at dette etterleves i liten grad. Helse Bergen HF erkjenner at det har svakheter knyttet til oppfølgingen av risikovurderingene. Risikovurderingene fra St. Olavs Hospital HF viser at frist og ansvarlig person ikke settes konsekvent.

På forespørsel om å få oversendt gjennomførte risikovurderinger har Universitetssykehuset Nord-Norge HF og Oslo universitetssykehus HF for perioden 2011–2013 oversendt én risikovurdering hver som omfatter EPJ, mens Helse Bergen HF har oversendt 13. Både Universitetssykehuset Nord-Norge HF og Oslo universitetssykehus HF har imidlertid sendt over flere risikovurderinger fra 2010. I Helse Bergen HF er alle, med unntak av en av de oversendte risikovurderingene, gjennomført av den regionale ikt-enheten. De andre helseforetakenes risikovurderinger er gjennomført på foretaksnivå. Det er ingen av de utvalgte avdelingene som selv har gjennomført risikovurderinger i perioden 2011–2013.

Av de oversendte risikovurderingene er det få som omfatter tilgangsstyringen i EPJ. De oversendte risikovurderingene fra Helse Bergen HF inneholder i hovedsak konsolidering av DIPS-systemet, og alle risikovurderingene er av teknisk art. Med unntak av én overordnet risikovurdering gjennomført av Oslo universitetssykehus HF i 2010, er ingen av de oversendte risikovurderingene fra helseforetakene gjort med utgangspunkt i organisatoriske endringer.

Sikkerhetsrevisjoner

Ingen av helseforetakene har gjennomført sikkerhetsrevisjoner i samsvar med regelverket eller egne interne prosedyrer. Selv om Universitetssykehuset Nord-Norge HF og St. Olavs Hospital HF har oversendt dokumentasjon på interne revisjoner som omhandler informasjonssikkerheten, følger ikke revisjonene helseforetakenes interne rutiner og regelverkets krav om at sikkerhetsrevisjonene skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandør. Oslo universitetssykehus HF og Helse Bergen HF oppgir at de ikke har gjennomført sikkerhetsrevisjoner for den etterspurte perioden. Det er heller ingen av de utvalgte avdelingene i helseforetakene som har gjennomført sikkerhetsrevisjoner på eget initiativ i perioden.

Mens St. Olavs Hospital HF og Helse Bergen HF har utarbeidet egne prosedyrer for gjennomføring av sikkerhetsrevisjoner, inngår sikkerhetsrevisjoner som en del av rutinene for interne revisjoner i de to øvrige helseforetakene. Helseforetakenes prosedyrer for interne revisjoner og sikkerhetsrevisjoner viser at det er ulike oppfatninger om hva kravet til sikkerhetsrevisjoner innebærer.

Helseforetakene har ulik tolkning av regelverkets krav om at sikkerhetsrevisjoner skal gjennomføres jevnlig. To av helseforetakene tolker kravet som at det skal gjennomføres årlige sikkerhetsrevisjoner. Ett helseforetak mener at hvert andre eller tredje år vil være tilfredsstillende. Ett helseforetak mener at behovet for sikkerhetsrevisjoner vil variere ut fra de ulike informasjonssystemenes vesentlighet og risiko.

Ledelsens gjennomgang

Alle helseforetakene har rutiner for ledelsens gjennomgang, som skal bidra til god styring og internkontroll for blant annet å sikre etterlevelse av egne rutiner og regelverk. Undersøkelsen viser at hvor ofte ledelsens gjennomgang gjennomføres, varierer fra tertialvis til årlig, og at temaet informasjonssikkerhet blir behandlet i varierende grad.

Ved Oslo universitetssykehus HF er informasjonssikkerhet ikke en del av ledelsens gjennomgang, utover at risikoer knyttet til integreringen av ulike ikt-systemer i forbindelse med sammenslåingen omtales. Helseforetaket redegjør for at ledelsen løpende blir orientert om risikovurderinger knyttet til informasjonssikkerhet. Oslo universitetssykehus HF er derimot det eneste helseforetaket som ikke nevner rapportering til ledelsen som en del av oppfølgingen med å etterleve foretakets fastsatte sikkerhetsmål.

I de tre andre helseforetakene gjennomgås informasjonssikkerhet som et eget punkt, men risikoene som rapporteres til ledelsen er av svært overordnet karakter. Gjennomgangene inneholder i varierende grad resultater fra risikovurderinger og sikkerhetsrevisjoner, og det er ikke en tydelig vurdering av hvorvidt helseforetakenes sikkerhetsstrategi gir tilfredsstillende informasjonssikkerhet.

St. Olavs Hospital HF og Universitetssykehuset Nord-Norge HF har etablert ledelsens gjennomgang på klinikknivå. Informasjonssikkerhet er derimot ikke behandlet, med unntak av at én kontroll utført av Datatilsynet omtales i ett av dokumentene.

Avviksbehandling

Ifølge helseforetakenes prosedyrer er avvik enhver behandling av helseopplysninger som ikke er i henhold til interne prosedyrer og gjeldende regelverk. Avviksbehandling skal være et viktig element i helseforetakenes kvalitetsarbeid. For å identifisere og iverksette nødvendige forebyggende tiltak skal avvik registreres. Undersøkelsen viser imidlertid at helseforetakene over en treårsperiode har registrert få avvik, og at det ifølge helseforetakene er knyttet usikkerhet til tallene. Antall registrerte avvik i EPJ-systemet som helseforetakene oppgir, framgår av tabell 2.

Tabell 2 Antall oppgitte avvik relatert til EPJ i perioden 2011–2013

Helseforetak	Antall oppgitte avvik i perioden
Oslo universitetssykehus HF	Ca. 6–15
Helse Bergen HF	159
St. Olavs Hospital HF	5
Universitetssykehuset Nord-Norge HF	22 registrert i det elektroniske avvikssystemet

Kilde: Helseforetakene

Tabellen viser at det over en treårsperiode er registrert få avvik, og at antallet varierer, fra 5 i St. Olavs Hospital HF til 159 i Helse Bergen HF. For avvikene som er registrert i det elektroniske avvikssystemet i Universitetssykehuset Nord-Norge HF har to personer blitt oppsagt og ni personer fått skriftlig advarsel. Ingen av de andre helseforetakene har oversikt over hvilke konsekvenser de registrerte avvikene har fått. Avvikshåndteringen blir i helseforetakene behandlet av ledere med personalansvar, eventuelt i samråd med sentralt ansatte på ikt-området og HR-/personalavdeling. Helse Bergen HF redegjør for at de ikke ønsker en oversikt sentralt over reaksjoner iverksatt av ledere, og at dokumentasjonen lagres i personalmappen til den ansatte.

De utvalgte avdelingenes egen oversikt over registrerte avvik viser at det er svært få avvik med tilknytning til EPJ-systemet. For de fire avdelingene i hvert helseforetak er det 1–2 avvik totalt som er relatert til EPJ og brudd på konfidensialitet.

I ledelsens gjennomgang rapporterer både Helse Bergen HF, St. Olavs Hospital HF og Universitetssykehuset Nord-Norge HF om underrapportering av avvik. Ledelsens

gjennomgang i Universitetssykehuset Nord-Norge HF for årene 2011–2013 viser imidlertid et bevisst fokus og en forbedring i meldekultur og avvikshåndtering.

Opplæring
Helseforetakene gjør gjeldende rutiner og prosedyrer for opplæring tilgjengelig for ansatte gjennom elektroniske dokumentsystemer. Alle ansatte skal i tillegg gjennomføre obligatorisk e-læringskurs om informasjonssikkerhet, der blant annet avviks-system og konsekvenser ved brudd på rutiner og regelverk blir behandlet.

Ved Helse Bergen HF er det en rutine at e-læringskurset skal repeteres hvert andre år. Universitetssykehuset Nord-Norge HF oppgir at ansatte må bestå en test i e-læringskurset innen 30 dager etter ansettelse, og at den ansattes tilgang til informasjonssystemene stenges automatisk dersom kurset ikke er bestått innen fristen. Videre oppgir Universitetssykehuset Nord-Norge HF at det gjennomføres klasseromsundervisning i informasjonssikkerhet. Oslo universitetssykehus HF har utarbeidet brosjyremateriell og veiledere med utgangspunkt i interne prosedyrer, som er tilrettelagt for ledere og ansatte.

Ifølge prosedyrene har alle helseforetakene delegert ansvaret for korrekt etterlevelse av vedtatte rutiner for tilgangsstyring til klinikk- eller avdelingsledere med budsjett- og personalansvar. Delegasjonen innebærer ansvar for opplæring av egne ansatte. Undersøkelsen viser gjennomgående at det verken på klinikk-/avdelingsnivå eller på overordnet nivå blir gitt systematisk opplæring til ansatte som skal tildele og administrere tilganger.

Departementet kommenterer i sitt svar at selv om flere av helseforetakene i dag har bedre styring og kontroll av tilgangen til helseopplysninger enn tidligere, så er dette et område det fremdeles er nødvendig å prioritere høyt. Departementet poengterer at dette arbeidet krever fortsatt ledelseforankring, at det prioriteres tilstrekkelige ressurser, at systemene blir enda sikrere og at kunnskapen på området økes.

3 Vurderinger

3.1 Gjeldende regelverk er ikke tilstrekkelig implementert
Alle de fire helseforetakene har utarbeidet skriftlige prosedyrer basert på regelverket. Disse inneholder rutiner for pålogging, behandling av sensitiv taushetsbelagt informasjon, tilgangsstyring og loggkontroll i EPJ-systemet. I tillegg er det utarbeidet overordnede styrende dokumenter om informasjonssikkerhet. Undersøkelsen viser imidlertid flere eksempler på manglende etterlevelse av og lite kunnskap om interne rutiner og gjeldende regelverk.

Selv om helseforetakene har fastsatt rutiner for personlig og individuell systempålogging, viser undersøkelsen flere tilfeller av at ansatte har lånt hverandres bruker-ID og passord for pålogging til systemet. Videre er det i helseforetakene for lite kunnskap om de ulike tilgangsrettighetene (normal-, aktualisert- og nødrettstilgang) og manglende innsikt i når de skal brukes.

Helseforetakene er pålagt å utpeke journalansvarlig, som skal ha det overordnede ansvaret for den enkelte pasientjournal, og det skal framgå av journalen hvem dette er. Ingen av helseforetakene fører journalansvarlig i journalene slik regelverket pålegger. Gjennomgående mangler det dessuten kunnskap om hva ansvaret for rollen som journalansvarlig innebærer. I Universitetssykehuset Nord-Norge HF føres eksempelvis ikke journalansvarlig i journalen, selv om journalansvarlig ifølge prosedyrer for

logganalyser er tillagt konkret ansvar for å bestille kontroller ved mistanke om ureglementert innsyn i pasientjournal.

Helseforetakene skal i henhold til regelverket gjennomføre og dokumentere sikkerhetsrevisjoner jevnlig. Likevel har ingen av helseforetakene gjennomført sikkerhetsrevisjoner i samsvar med regelverket, og undersøkelsen viser at det er ulik oppfatning blant helseforetakene om hva pålegget innebærer.

Etter revisjonens vurdering har ikke helseforetakene i tilstrekkelig grad lagt vekt på å implementere fastsatte rutiner og gjeldende regelverk, slik at de ansatte blir i stand til å overholde sine lovpålagte plikter for behandling av sensitive taushetsbelagte helseopplysninger.

3.2 Ansatte har tilgang til helseopplysninger utover det reelt behov tilsier

Gjeldende regelverk er tatt inn i helseforetakenes prinsipper for tilgangsstyring. Prinsippene slår fast at det må foretas en konkret vurdering av hvilke opplysninger den enkelte skal få tilgang til, basert på det som er nødvendig for å utføre arbeidet. Helseforetakenes tilgangsstyring er analysert ut fra tre aspekter: tilgangsrettigheter til ansattrollene, informasjonen ansatte har tilgang til, og tiden de ansatte har tilgang til informasjonen.

Når det gjelder hvilke tilgangsrettigheter ansattrollene har til pasientjournaler, viser undersøkelsen gjennomgående at tildeling av tilgangsrettigheter i hovedsak er standardisert, og i liten grad basert på konkrete vurderinger av den enkeltes behov. Tre av fire helseforetak gir normal eller aktualisert tilgang på tvers av systemområdene somatikk og psykisk helsevern/rus. Eksempelvis gis det i St. Olavs Hospital HF svært brede normale tilganger til mange ansatte og roller på tvers av systemområdene, og tilsvarende når det gjelder rett til å benytte aktualisert tilgang. Dessuten har ingen av helseforetakene rutiner for systematisk å avslutte tilganger når ansatte bytter arbeidssted internt, og i flere helseforetak har ansatte tilganger de selv ikke er klar over.

Undersøkelsen viser at de ansatte i helseforetakene gjennomgående har tilgang til mye sensitiv taushetsbelagt informasjon uavhengig av rolle og uten å åpne selve pasientjournalen. Ved de utvalgte avdelingene i helseforetakene som bruker DIPS-systemet, kan ansatte se samtlige kontakter (innleggelser og polikliniske konsultasjoner) en pasient har hatt med helseforetaket innen både somatikk og psykisk helsevern/rus. Videre kan de ansatte se samtlige henvisninger for den enkelte pasient, der mye sensitiv informasjon som diagnoser og DRG-koder kan være tilgjengelig. Stikkprøver i Universitetssykehuset Nord-Norge HF viser at mange dokumenter med sensitiv informasjon rutinemessig blir scannet og lagret i pasientjournal som bilder. Disse bildene er tilgjengelig for alle ansatte i hele helseforetaket på tvers av systemområdene somatikk og psykisk helsevern/rus.

Tiden de ansatte har tilgang til informasjonen, er i flere tilfeller lengre enn behovet. Innen systemområdet psykisk helsevern/rus i Oslo universitetssykehus HF og Universitetssykehuset Nord-Norge HF er det ikke tidsbegrensning for de ansattes normale tilgang til pasientjournal i etterkant av utskrivning eller avsluttet konsultasjon. Utgangspunktet ved aktualisert tilgang er at det er den enkelte ansattes tilgang som gjøres normal for en bestemt tidsperiode. Undersøkelsen viser imidlertid at bruk av aktualisering i Universitetssykehuset Nord-Norge HF gjør pasientjournalen tilgjengelig også for øvrige ansatte i helseforetaket gjennom normal tilgang på tvers av systemområdene i 24 timer. Etter revisjonens vurdering innebærer dette at mange ansatte får tilgang til sensitive helseopplysninger uten at de har behov for det.

Etter revisjonens vurdering viser de ovennevnte eksemplene at de ansatte har tilgang til helseopplysninger utover det reelt behov tilsier. Konsekvensen av dette er at det i helseforetakene er mange ansatte som har tilgang til hele eller deler av de elektroniske pasientjournalene uavhengig av om de er involvert i pasientbehandling eller ikke.

3.3 Ingen systematisk kontroll og oppfølging av tilganger til EPJ

Helseforetakenes praksis med å gi de ansatte vide standardiserte tilganger til sensitiv taushetsbelagt informasjon i EPJ-systemet fordrer systematisk kontroll og oppfølging for å sikre at de ansattes bruk av tilganger ikke går utover det de etter regelverket skal ha tjenstlig behov for. Imidlertid viser undersøkelsen flere eksempler på at helseforetakene ikke har systematisk kontroll og oppfølging av ansattes bruk av tilganger.

Ifølge prosedyrene har alle de fire helseforetakene delegert ansvaret for korrekt etterlevelse av vedtatte rutiner for tilgangsstyring og oppgavene med å tildele og administrere tilgangene til EPJ-systemet til klinikk- eller avdelingsledere med budsjett- og personalansvar. Delegasjonen innebærer vide fullmakter for lederne til å utføre tilgangsstyring og beslutte hvem som skal ha hvilke tilgangsrettigheter til systemet. Gjennomgående viser undersøkelsen at de utvalgte avdelingene ikke har etablert rutiner for å administrere og vedlikeholde ansattes tilganger. Avdelingene oppgir at dette er oppgaver som skal ivaretas av overordnet nivå. Imidlertid viser undersøkelsen at overordnet nivå verken systematisk gjennomfører kontroller av tilganger eller følger opp at delegerte oppgaver faktisk blir gjennomført.

Videre viser undersøkelsen at begrunnelsene som må oppgis ved bruk av aktualisert tilgang og nødrettstilgang, er forhåndsdefinerte og i for liten grad tilrettelagt de ansattes faktiske arbeidssituasjon og behov. Dessuten kan kravet om faktisk behovsbegrunnelse lett overstyres ved at et hvilket som helst tegn eller ord godtas som begrunnelse. Etter revisjonens vurdering innebærer dette at helseforetakene har mangelfullt grunnlag for å etterprøve hvorvidt det faktiske behovet var til stede.

Helseforetakene har utarbeidet prosedyrer som slår fast at loggkontroller av ansattes oppslag i pasientjournaler skal gjennomføres rutinemessige, både egeninitierte og basert på forespørsler fra pasienter. Samtidig viser undersøkelsen at ingen av helseforetakene gjennomfører systematiske loggkontroller på eget initiativ for å avdekke ureglementerte oppslag, som for eksempel snoking. De få loggkontrollene som utføres, er primært på forespørsel fra pasienter.

I henhold til regelverket skal helseforetakene behandle bruk av EPJ-systemet som både er i strid med fastlagte rutiner og sikkerhetsbrudd, som avvik, og resultatet av avviksbehandlingen skal dokumenteres. Til tross for fastsatte prosedyrer viser undersøkelsen at samtlige helseforetak har registrert svært få avvik, og at det i forbindelse med rapporteringen til ledelsen i flere helseforetak framkommer at avvik blir underrapportert. Videre mangler helseforetakene systematisk oversikt over avvikene og hvilke konsekvenser de har fått for de ansatte. Helseforetakenes faktiske avviksbehandling synes ikke å være egnet som et viktig element i kvalitetsarbeidet, slik de fastsatte prosedyrene legger opp til.

Sett i forhold til stor bruk av vide tilganger til mange ansatte, antall pasientjournaler og antall oppslag er dagens kontrollpraksis i helseforetakene etter revisjonens vurdering ikke egnet til å gi en tilstrekkelig grad av sikkerhet for at de ansattes bruk av tilganger er i samsvar med gjeldende regelverk.

3.4 Mangelfull internkontroll av helseforetakenes tilgangsstyring

Helseforetakene er pålagt å ha internkontroll der databehandlingsansvarlige skal etablere, vedlikeholde, dokumentere og gjøre tilgjengelig nødvendige systematiske tiltak. Internkontroll er en prosess som blant annet skal sikre korrekt etterlevelse av interne rutiner og regelverk. Undersøkelsen viser imidlertid at ingen av helseforetakene har etablert systematisk og integrert internkontroll for tilgangsstyring i EPJ-systemet.

Helseforetakene har fastsatt ambisiøse sikkerhetsmål for behandling av helseopplysninger. Sikkerhetsmålene er av overordnet karakter og i liten grad operasjonalisert. Samtlige helseforetak har en tilnærmet nullaksept på risiko for etterlevelse av fastsatte sikkerhetsmål, og legger til grunn at sikkerhetsbrudd ikke aksepteres.

Til tross for ambisiøse sikkerhetsmål viser undersøkelsen at helseforetakene verken har en systematisk oppfølging av risikovurderinger eller gjennomfører sikkerhetsrevisjoner i samsvar med regelverket. Selv om helseforetakene har etablert rutiner for ledelsens gjennomgang, viser undersøkelsen at risikoene som rapporteres til ledelsen i helseforetakene er av svært overordnet karakter, og at resultater fra gjennomførte risikovurderinger og avvikshåndtering i liten grad blir gjennomgått.

Fravær av systematisk og integrert internkontroll gjør at det etter revisjonens vurdering er vanskelig å se at administrerende direktør som databehandlingsansvarlig i helseforetakene, kan overholde sin lovpålagte plikt om å sikre tilfredsstillende informasjonssikkerhet relatert til tilgangsstyring i EPJ-systemet.