HELSE FINNMARK
FINNMÁRKKU DEARVVAŠVUOHTA
Administrasjonen

HELSE NORD

Styremøte i Helse Finnmark HF **Dato. 18. mai 2011**

Møtedato: 26. mai 2011

Saksbehandler: Kvalitetsleder Leif Arne Asphaug-Hansen

Sak nr:	**28/2011**
Navn på sak:	**Plan for oppfølging av Internrevisjonsrapport**

Tilrådning:

1. Styret i Helse Finnmark tar plan for oppfølging og imøtekommelse av anbefalinger i Internrevisjonsrapport nr. 04/2010: "Internkontroll ved behandling av helseopplysninger i Helse Finnmark HF" til orientering.
2. Styret ber om at statusrapport for oppfølging av planen fremlegges styret høsten 2011.

Vedlegg:

1. Saksfremlegg.
2. Internrevisjonsrapport Helse Nord
3. Forslag til plan for oppfølging av de 14 anbefalingene i

Hans Petter Fundingsrud
Adm. dir.

HELSE FINNMARK
FINNMÁRKKU DEARVVAŠVUOHTA

HELSE NORD

Saksbehandler: Kvalitetsleder Leif Arne Asphaug-Hansen
Dato: 18. mai 2011

Styresak 28/2011 Plan for oppfølging av Internrevisjonsrapport

Innledning

Styret i Helse Finnmark HF behandlet aktuelle Internrevisjonsrapport i sitt desembermøte i 2010. Følgende ble da enstemmig vedtatt (Protokoll sak 84-2010):

1: *Styret i Helse Finnmark HF tar Internrevisjonsrapport nr. 04/2010: "Internkontroll ved behandling av helseopplysninger i Helse Finnmark HF" til orientering og ber om at den legges til grunn i det videre arbeidet..*

2: *Styret ber direktøren sørge for at arbeid med informasjonssikkerhet blir tilstrekkelig prioritert i hele organisasjonen samt sikre at nødvendige ressurser er avsatt til dette arbeidet. Styret ber videre direktøren sørge for at det arbeides videre med de anbefalinger som ikke allerede er imøtekommet, og at det utarbeides en konkret fremdriftsplan for dette arbeidet.*

3: *Styret forutsetter at nytt felles "Styringssystem for informasjonssikkerhet" med tilhørende prosedyrer blir implementert i foretaket når disse er besluttet.*

4: *Styret ber om statusrapport i fht til anbefalingene fremlegges styret høsten 2011.*

Tilsvarende revisjoner ble i 2010 gjennomført i samtlige foretak i Helse Nord. Styret i Helse Nord behandlet i sitt styremøte 23.2.2010 i styresak 20-2010 Internrevisjonsrapport 07/2010: Internkontroll ved behandling av helseopplysninger i Helse Nord oppsummering, vedtok Styret i Helse Nord RHF under pkt 2 følgende:

> *"Styret ber adm. direktør sørge for at styret før sommeren 2011 får presentert en fremdriftsplan som viser gjennomførte og planlagte tiltak for forbedring av internkontrollen, i samsvar med internrevisjonens anbefalinger. Tidsperspektivet i fremdriftsplanen bør ikke overstige ett år."*

Sak til styret i Helse Nord RHF skal forelegges til møtet i juni i år. Som følge av ovennevnte er Helse Finnmark HF bedt om å oversende fremdriftsplan som viser gjennomførte og planlagte tiltak for forbedring av internkontrollen i samsvar med internrevisjonens anbefalinger, snarest og senest 31.5.11.

Saksframlegg
Arbeidet med plan for å imøtekomme de gitte anbefalinger startet etter at *Internrevisjonsrapport nr. 04/2010: "Internkontroll ved behandling av helseopplysninger i Helse Finnmark HF"* ble mottatt i foretaket. Det var samlet 14 anbefalinger internrevisjonen knyttet til informasjonssikkerhet som skal imøtekommes for å ivareta lovkrav. Foretaksledelsen har nå behandlet aktuelle Plan for oppfølging av de aktuelle anbefalinger, og oppdrag er fordelt innad i foretaket i tråd med besluttet plan.

Anbefalingene var innen følgende områder:

Anbefaling 1:
Videreutvikle oversikten over behandlinger av helseopplysninger, og etablere rutiner som sikret
at oversikten kontinuerlig er oppdatert og fullstendig, inkludert informasjon om databehandlere.
Anbefaling 2:
Sørge for at meldeplikten til Datatilsynet etterleves for alle meldepliktige behandlinger av helse og personopplysninger.
Anbefaling 3:
Benytte avviksmeldinger mer aktivt i internt forbedringsarbeid.
Anbefaling 4:
Videreføre og videreutvikle gjennomføring og bruk av risikovurderinger, gjerne i samarbeid med
Helse Nord IKT.
Anbefaling 5:
Definere hvordan foretakets samlede journalsystem er organisert, og etablere rutiner som sikrer
at informasjon i den enkelte pasientjournal samsvarer med dette
Anbefaling 6:
Fullføre oppryddingsarbeidet for å skape samsvar mellom tilganger til IT-systemer og tjenestelige behov, sørge for at tilganger løpende inaktiveres når tjenestelige behov opphører, samt gjennomføre regelmessige kontroller av at samsvar mellom tilganger og behov opprettholdes
Anbefaling 7:
Gjennomgå og oppdatere tilgangsmatrise og rollemaler i DIPS
Anbefaling 8:
Legge til rette for felles praksis i bruk av DIPS og andre elektroniske journalsystemer, herunder
innføre felles rutiner for registrering av journalansvarlig person i DIPS
Anbefaling 9:
Sørge for at utveksling av røntgeninformasjon på tvers av HF-ene samsvarer med gjeldende lovverk (eventuelt i samarbeid med andre aktører i Helse Nord), og fjerne tilgangene for ansatte
ved andre helseforetak til å hente røntgeninformasjon fra Helse Finnmark.
Anbefaling 10:
Foreta en konkret risikovurdering i forbindelse med etablert fjerntilgang til røntgensystemer, samt gjennomføre risikoreduserende tiltak dersom uakseptabel risiko avdekkes
Anbefaling 11:
Vurdere etablering av system for dokumentasjon/kontroll av uttak og retur av papirjournal fra

Anbefaling 12:
Gjennomføre sikkerhetsrevisjon og ledelsens gjennomgang minimum årlig.
Anbefaling 13:
Iverksette tiltak for jevnlig å forsikre seg om at sikkerhetsstrategien hos databehandlere og leverandører gir tilfredsstillende informasjonssikkerhet
Anbefaling 14:
Videreutvikle helseforetakets internkontrollrutiner med sikte på forbedring av øvrige svakheter
Internrevisjonen har påpekt i denne rapporten.

Behovet for å styrke foretakets egen IKT-kompetanse medførte søknad og tildeling av prosjektmidler. Tilsettingsprosess er iverksatt slik at vi regner med å ha IKT-ansvarlig på plass i løpet av kort tid. Denne stillingen skal tillegges oppgaver og relatert til ivaretakelse av informasjonssikkerhetskrav.

Oppgaver sammen med tidsfrister knyttet til de ulike anbefalinger framkommer i vedlagte plan. Omfanget av oppgaven er gitt gjennom Internrevisjonens rapport og styrets vedtak. Samtlige anbefalinger må følges opp for å ivareta lovkrav.

Følgende anbefalinger bør være greie å kvittere ut:

- **1, 2, 3, 6, 7, 9, 11** (hvorav 2 og 11 ansees imøtekommet)

Følgende anbefalinger ansees som mer ressurskrevende å få gjennomført, uten å være spesielt kompliserte for vår del:

- **5** som både omfatter å få reetablert et fungerende journalutvalg samt vil avhenge av arbeid i HN-IKT gjeldende IKT/serverstruktur.

Mer ressurs- og kompetansemessige krevende anbefalinger ansees:

- **4** hvor arbeid med formaliserte risikovurderinger bør prioriteres ytterligere, noe som innebærer at det avsettes nødvendig tid og ressurs
- **8** hvor vi har flere hendelser som har bekreftet behov for gode rutinebeskrivelser på flere områder enn registrering av pasientansvarlig lege. Ex. Ventelisteproblematikk, rutiner for rapporter og internkontroll ved bruk av DIPS.
- **10** hvor vi med sannsynlighet må innhente ekstern kompetanse
- **12** som innebærer betydelig ressursbruk samt kompetanse. Området vil bli styrket ved tilsetting av IKT-ansvarlig.
- **14** som vil innebære ytterligere opplæring og at nødvendig tid blir avsatt for gjennomføring.

Da styret i Helse Finnmark HF behandlet Internrevisjonsrapport nr. 04/2010: ”Internkontroll ved behandling av helseopplysninger i Helse Finnmark HF” ble det orientert om et felles arbeid i regionen med utarbeidelse av et nytt felles styringssystem for informasjonssikkerhet. Det er utarbeidet forslag som er oversendt Helse Nord RHF. Styrets forutsetning om at overordnet styringssystem sammen med tilhørende prosedyrer skal implementeres vil bli fulgt opp straks dette er godkjent. Styringssystemet sammen med tilhørende prosedyrer vil blant annet ved tydeliggjøring av oppgaver sammen med ansvarsplassering bidra til at vi også i Helse Finnmark i ettertid skal være bedre à jour med informasjonssikkerhetsarbeidet.

Arbeidet vil bli fulgt via statusrapportering som i henhold til styrevedtak forelegges styret i Helse Finnmark høsten 2011.

Oppfølgingsplan: Anbefalinger etter Internrevisjon – informasjonssikkerhet

Anbefaling	Kommentar	*Ansvar*	*Delegert til:*	*Tidsfrist:*
Anbefaling 1: Videreutvikle oversikten over dataprogrammer og behandlinger av helseopplysninger, og etablere rutiner som sikret at oversikten kontinuerlig er oppdatert og fullstendig, inkludert informasjon om databehandlere	a) Oversikt over dataprogrammer er allerede etablert men må vedlikeholdes. Ansvar for dette anbefales lagt til driftssjef med mulighet for å delegere oppgaven til IKT-bestiller - på sikt IKT-ansvarlig når slik funksjon er etablert. b) Oversikt over lokale helseregistre må utarbeides. Dette innebærer kartlegging i fagmiljøene i våre klinikker. Kartlegging må foregå i klinikkene. Resultat av kartlegging oversendes informasjons-sikkerhetsansvarlig som etablerer oversikt i Docmap. c) Lage oversikt over medisinsk-teknisk utstyr som inneholder lagringsmedie for lagring av pasientopplysninger, og etablere rutiner som sikret at oversikten kontinuerlig er oppdatert og fullstendig, inkludert informasjon om databehandlere.	a) Driftssjef b) Klinikksjefer c) Driftssjef	a) IKT-bestiller / IKT-ansvarlig b) klinikksjef delegerer c) **Hammerfest:** Avd. leder MTA H.fest **Kirkenes:** Avd. leder MTA K.nes	a) 1.juni 2011 b) 1. sept. 2011 c) 1. august 2011
Anbefaling 2: Sørge for at meldeplikten til Datatilsynet etterleves for alle meldepliktige behandlinger av helse- og personopplysninger.	a) Applikasjoner som behandler pasientopplysninger b) Innmelding av kameraovervåking samt nøkkelkortsystemer.	a) Informasjons-sikkerhetsansvarlig b) Driftssjef	 b) Teknisk sjef	a) **Utført** b) **Utført**
Anbefaling 3: Benytte avviksmeldinger mer aktivt i internt forbedringsarbeid.	a) Har nå tilgjengelige superbrukere i klinikkene. b)	a) Klinikksjefer/ Stabsledere	a) avd. ledere	a) Kontinuerlig

Anbefaling	Kommentar	*Ansvar*	*Delegert til:*	*Tidsfrist:*
	Gjennomført kurs for superbrukere og for ledere	b) kvalitetsleder		b) Er à jour pt, men "Turn-over" skaper behov for nye kurs
	c) Avviksmeldinger inngår i saksliste for KVAM-grupper/KVAM-råd/ FAMU og Kvalitetsutvalg	c) Klinikksjefer/ Stabsledere	c) Ledere av slike utvalg	c) Påbegynt, men Kontinuerlig prosess
Anbefaling 4: Videreføre og videreutvikle gjennomføring og bruk av risikovurderinger, gjerne i samarbeid med Helse Nord IKT.	a) Styrke IKT-ressurs med IKT-ansvarlig. Vurdere å skille roller for henholdsvis kvalitetsleder/info sikkerhetsansvarlig Stilling er utlyst.	a) adm. dir		a) 1. sept 2011
	b) Arbeide for å få utvidet samarbeidet via IS-nettverk med tanke på foretaksovergripende samarbeid og ved utførelse av analyser	b) informasjons-sikkerhetsansvarlig		b) kontinuerlig
	c) Styrke intern samhandling innen IKT. Tilrettelegge for bedret samhandling følgende: IKT-bestiller, ny IKT-ansvarlig, Info sikkerhetsansvarlig og EPJ-konsulenter	c) adm. dir		c) 1. august 2011
Anbefaling 5: Definere hvordan foretakets samlede journalsystem er organisert, og etablere rutiner som sikrer at informasjon i den enkelte pasientjournal samsvarer med dette.	a) Sak gjeldende organisering av pasientjournalsystem avklares i Journalutvalget	a) adm. dir	a) leder journalutvalg	a) 1. juli 2011
	b) Gjennomgå/beslutte mandat og sammensetning for journalutvalg	b) adm. dir		b) 1. juni 2011
	c) etablere de nødvendige	c)	c)	c)

Anbefaling	Kommentar	*Ansvar*	*Delegert til:*	*Tidsfrist:*
	rutiner/arbeidsbeskrivelser	leder journalutvalg	EPJ-kons	Kontinuerlig
Ad anbefaling 5: Framdriftsplan for etablering en felles DIPS database i Finnmark er ikke detaljert eller besluttet ennå. Representant fra HN-IKT opplyser at det på fellesmøte i Helse Nord IKT, etter at anbudsresultatet var offentliggjort, ble det tegnet en framdriftsplan der man bl.a ennå ikke har tatt stilling til om det skal være 1,2,3 eller 4 ulike lokaliseringer av DIPS. Det er også beregnet en planleggingsfase på 4-6 mndr, og deretter en forprosjektfase på ca. 1 år.				
Anbefaling 6: Fullføre oppryddingsarbeidet for å skape samsvar mellom tilganger til IT-systemer og tjenestelige behov, sørge for at tilganger løpende inaktiveres når tjenestelige behov opphører, samt gjennomføre regelmessige kontroller av at samsvar mellom tilganger og behov opprettholdes	a) Implementering av BAS vil effektivisere men og forflytte oppgaver til ansatte på klinikk eller avdelingsnivå. Avdelinger vil enklere få oversikt. b) etablere felles rutiner som sikrer inn- og utmeldinger av personell c) Gjennomføre internkontroll d) Sikre at arbeidsoppgaver ikke blir liggende når ansatte deaktiveres.	a) adm. dir b) HR-sjef/Personalsjef c) HR-sjef d) Klinikksjef	a) HR-sjef/ personalsjef b) delegeres senere c) delegeres d) avdelingsledere	a) ikke avklart. Implementering tidlig høsten 2011 b) 1. august 2011 c) jevnlig via rapporter d) kontinuerlig
Anbefaling 7: Gjennomgå og oppdatere tilgangsmatrise og rollemaler i DIPS	Etablering av oppdaterte tilgangsmatriser var behandlet som egen sak i Journalutvalget i 2009. Klinikksjefer er tidligere bedt om å utarbeide klinikkvise tilgangsmatriser som skal vise standardtilganger til de ulike yrkesgrupper. Tilgangsmatriser skal legges i Docmap og etterleves.	Klinikksjefer Med støtte fra EPJ-konsulent	Avdelingsledere Med støtte fra EPJ-konsulent	1. juli 2011
Anbefaling 8: Legge til rette for felles praksis i bruk av DIPS og andre elektroniske journalsystemer, herunder innføre felles rutiner for registrering av journalansvarlig person i DIPS	a) Etablere/Implementere nødvendige felles arbeidsrutiner/prosedyrer i bruk av DIPS b) Etablere og etterleve rutine for	a) Leder journalutvalg b) klinikksjefer	a) EPJ-konsulenter b) avdelingsledere	a) iverksettes innen 1. sep – 2011 b) 1. juni 2011

Anbefaling	Kommentar	*Ansvar*	*Delegert til:*	*Tidsfrist:*
	imøtekommelse journalforskriftens § 6.- registrerer pasientansvarlig lege			
Anbefaling 9: Sørge for at utveksling av røntgeninformasjon på tvers av HF-ene samsvarer med gjeldende lovverk (eventuelt i samarbeid med andre aktører i Helse Nord), og fjerne tilgangene for ansatte ved andre helseforetak til å hente røntgeninformasjon fra Helse Finnmark	Løsning ved bruk av Arcidis vil vedlikeholde mulighet for utveksling av informasjon i samsvar med regelverk.	klinikksjef Hammerfest	Avd leder radiologisk avdeling	1. juni 2011
Anbefaling 10: Foreta en konkret risikovurdering i forbindelse med etablert fjerntilgang til røntgensystemer, samt gjennomføre risikoreduserende tiltak dersom uakseptabel risiko avdekkes.	Gjennomføre risikovurdering. IKT-bestiller og informasjons-sikkerhetsansvarlig kan sammen med ressurser evt fra HN-IKT bistå	klinikksjef Hammerfest	Avd leder radiologisk avdeling	1. sept 2011
Anbefaling 11: Vurdere etablering av system for dokumentasjon/kontroll av uttak og retur av papirjournal fra arkiv ved BUP	I forbindelse med at dette området ble fokusert under revisjonen ble det etablert ordning som må oppfattes som tilfredsstillende ved at papirjournaler nå kvitteres inn/ut når slike utleveres/tilbakeleveres til/fra arkiv. Ordningen er bekreftet iverksatt.			**Utført**
Anbefaling 12: Gjennomføre sikkerhetsrevisjon og ledelsens gjennomgang minimum årlig	Sikkerhetsrevisjon gjennomføres i 3 utvalgte enheter	informasjons-sikkerhetsansvarlig / IKT-ansvarlig med hjelp fra IKT-bestiller		a) revisjon gjennomføres innen oktober b) ledelsens gjennomgang i etterkant av dette straks rapport foreligger – innen utgang av 2011
Anbefaling 13: Iverksette tiltak for jevnlig å forsikre seg om at	Et koordinerende ansvar og oppfølging av dette punktet foreslås tillagt IKT-	Driftssjef	IKT-bestiller	Kontinuerlig Statusrapport

Anbefaling	Kommentar	*Ansvar*	*Delegert til:*	*Tidsfrist:*
sikkerhetsstrategien hos databehandlere og leverandører gir tilfredsstillende informasjonssikkerhet	bestiller som i sin funksjon er foretakets kontaktperson opp mot eksterne dataleverandører inkludert Helse Nord IKT			medtas i ledelsens gjennomgang jfr. Pkt 12
Anbefaling 14: Videreutvikle helseforetakets internkontrollrutiner med sikte på forbedring av øvrige svakheter Internrevisjonen har påpekt i denne rapporten	a) Samarbeide med internrevisjon i øvrige foretak mht å definere revisjonsområder- Årlige møter. b) Vurdere behov for ytterligere opplæring innen internrevisjon – repetere kurs c) sikre at internkontrollforskrifter er kjent for ledere. Ledelsesansvar skal ivaretas. d) Årlig utarbeide plan for interne revisjoner – plan over 3 år	a) adm dir b) opplæringsansvarlig c) klinikkledere/ stabssjefer d) Foretakscontroller/ Kval. leder	a) controller sammen med kval leder	a) OK for 2011 b) vurdere behov innen 1. juni 2011 c) innen 1. juni d) **Utført 2011**

HELSE NORD

Internkontroll ved behandling av helseopplysninger i Helse Finnmark HF

Internrevisjonsrapport nr.: 04/2010

Dato: 21.10.2010

INNHOLDSFORTEGNELSE

1 SAMMENDRAG

Rapporten er utarbeidet etter internrevisjon ved Helse Finnmark HF i perioden 25.02.–17.09.2010.

Formålet med revisjonen:
Formålet med revisjonen var å kartlegge om Helse Finnmark HF har etablert og vedlikeholdt et opplegg for internkontroll som sikrer at helseopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på helseopplysninger.

Konklusjon:
Basert på de undersøkelser som er foretatt ved Helse Finnmark HF konkluderer Internrevisjonen med at behandlingen av helseopplysninger innenfor enkelte områder ikke er i samsvar med gjeldende regelverk.

Helse Finnmark HF sitt opplegg for internkontroll inneholder svakheter som bør forbedres for å sikre at helseopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på helseopplysninger.

Observasjoner og vurderinger:
De vesentligste svakhetene i Helse Finnmarks opplegg for internkontroll er etter Internrevisjonens observasjoner og vurderinger:

- Meldeplikten til Datatilsynet er ikke ivaretatt for alle meldepliktige registre.
- Avviksmeldinger kan med fordel benyttes mer aktivt i internt forbedringsarbeid.
- Helse Finnmark HF har ikke gjennomført sikkerhetsrevisjoner.
- Det er ikke gjennomført risikovurderinger knyttet til den enkelte kliniske applikasjon.
- Det er ikke lagt til rette for felles praksis i bruk av DIPS. Dette medfører en risiko for at datagrunnlag i DIPS ikke er pålitelig og sammenlignbart.
- Pasienten har ikke en samlet journal i Helse Finnmark HF.
- Ved Klinikk Hammerfest framgår det ikke av journalen hvem som er journalansvarlig person.
- Tilganger til IT-systemer trekkes ikke tilbake når tjenestelige behov opphører.
- Det er behov for å gjennomgå og oppdatere tilgangsmatrise og rollemaler i DIPS.
- Det eksisterer gjensidige tilganger, som ikke er i samsvar med gjeldende lovverk, til å hente røntgeninformasjon på tvers av HF-grensene.
- En ordning med ekstern tilgang til røntgensystemene fra Sverige er etablert uten at det er foretatt en konkret risikovurdering i denne forbindelse. Ordningen innebærer risikofaktorer ut over det som gjelder for ordinære hjemmetilganger.
- Det er ikke etablert noe system for dokumentasjon eller kontroll av uttak og retur av papirjournal fra arkiv ved BUP Hammerfest.

Anbefalinger:
Internrevisjonen anbefaler Helse Finnmark HF å iverksette en rekke forbedringstiltak knyttet til blant annet: ivaretakelse av meldeplikt, risikovurderinger, tilgang til røntgeninformasjon, dokumentasjon av journalansvarlig person, tilganger og bruk av DIPS og tilbaketrekking av tilganger til IT-systemer.

2 INNLEDNING

Rapporten er utarbeidet etter internrevisjon ved Helse Finnmark HF i perioden 25.02.–17.09.2010, Revisjonen er gjennomført av Internrevisjonen i Helse Nord RHF, og inngikk som en del av vedtatt revisjonsplan for 2009/2010. Alle helseforetakene i Helse Nord, samt Helse Nord IKT (HNIKT) som databehandler for helseforetakene, har hatt/skal ha revisjon innenfor samme tema. Helseforetakene har mottatt kopi av rapporten for HNIKT.

Internrevisjonen har omfattet følgende aktiviteter:

- Melding om internrevisjon sendt ut 25.02.2010.
- Oppstartsmøte 07.09.2010.
- Intervju av 14 ledere og ansatte ved Helse Finnmark, samt EPJ-konsulent i Helse Nord IKT, i perioden 20.04.-09.09.2010. Se vedlegg 1, Deltakeroversikt.
- Dokumentgjennomgang. Oversikt over dokumenter som er innhentet i forbindelse med revisjonen er gitt i vedlegg 2, Dokumentoversikt.
- Verifikasjoner/tester. Se nærmere beskrivelse i kapittel 4, Metoder.
- Oppsummeringsmøte 09.09.2010.

2.1 Definisjoner

Følgende definisjoner fra regelverket (se pkt. 3.2) er sentrale i denne revisjonen:

helseopplysninger: 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,

behandling av helseopplysninger: enhver formålsbestemt bruk av helseopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter,

behandlingsrettet helseregister: journal- og informasjonssystem eller annet helseregister som har til formål å gi grunnlag for handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende mål i forhold til den enkelte pasient og som utføres av helsepersonell, samt administrasjon av slike handlinger,

pasientjournal/journal: samling eller sammenstilling av nedtegnede/registrerte opplysninger om en pasient i forbindelse med helsehjelp, jf. helsepersonelloven § 40 første ledd,

behandlingsansvarlig/databehandlingsansvarlig: den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes, hvis ikke (data)behandlingsansvaret er særskilt angitt i loven eller i forskrift i medhold av loven,

databehandler: den som behandler helseopplysninger på vegne av den behandlingsansvarlige.

3 FORMÅL OG OMFANG

3.1 Formål med revisjonen

Formålet med revisjonen var å kartlegge om Helse Finnmark HF har etablert og vedlikeholdt et opplegg for internkontroll som sikrer at helseopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på helseopplysninger.

3.2 Regelverk

Virksomheten er vurdert opp mot følgende regelverk (revisjonskriterier):

- Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)
- Lov om behandling av personopplysninger (personopplysningsloven)
- Forskrift om behandling av personopplysninger (personopplysningsforskriften)
- Lov om helsepersonell (helsepersonelloven)
- Forskrift om pasientjournal (journalforskriften)
- Lov om spesialisthelsetjenesten (spesialisthelsetjenesteloven)
- Lov om pasientrettigheter (pasientrettighetsloven)
- Norm for informasjonssikkerhet i helsesektoren (Normen)
- Interne bestemmelser

Både helseregisterlovens § 17 og personopplysningslovens § 14 stiller krav om at den behandlingsansvarlige skal etablere og holde ved like planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av disse lovene. Personopplysningsforskriftens kapittel 2 (Informasjonssikkerhet) og kapittel 3 (Internkontroll) gir nærmere føringer for hvilke tiltak dette skal omfatte.

Norm for informasjonssikkerhet i helsesektoren (Normen) er et omforent sett av krav til informasjonssikkerhet, basert på lovverket. Normen omfatter alle krav som må tilfredstilles for å oppfylle lov- og forskriftskrav til informasjonssikkerhet i helsesektoren. Normen kan også stille strengere krav enn det som følger av lovverket. Alle aktører i helsesektoren som er tilknyttet Norsk Helsenett[1] er avtalerettslig forpliktet til å følge Normen.

Kravene om internkontroll skal bidra til å sikre at lovverkets samlede krav blir oppfylt. Velfungerende internkontroll på dette området reduserer risikoen for negativ omtale/tap av anseelse, økonomisk tap, tap av helse og tap av liv.

[1] Elektronisk samhandlingsarena (nettverk) for helse- og omsorgssektoren.

3.3 Omfang og avgrensninger

Prosjektet har omfattet helse- og personopplysninger som behandles helt eller delvis med elektroniske hjelpemidler i forbindelse med pasientbehandling, herunder også pasientadministrasjon og utlevering av legemidler. Det ble gjort undersøkelser av både innhold/omfang og etterlevelse av internkontrollsystemet ved Helse Finnmark HF.

Gjennom undersøkelsene har revisjonen først og fremst hatt fokus på:

- Risikovurderinger
- Journalansvar
- Tilgangsstyring
- Ivaretakelse av informasjonssikkerhet hos databehandlere og leverandører
- Utvalgte kliniske applikasjoner: DIPS[2], røntgensystemer og Bupdata.

Internrevisjonen har i dette prosjektet ikke sett på behandling av helse- og personopplysninger til andre formål enn pasientbehandling, for eksempel i forbindelse med personalregistre og forskning.

4 METODER

Til sammen 14 ledere og ansatte ved Helse Finnmark er intervjuet. I tillegg er en av EPJ-konsulentene i HNIKT intervjuet i forhold til arbeidsoppgaver knyttet til Helse Finnmark. Se vedlegg 1, Deltakeroversikt.

Tilsendt/framlagt dokumentasjon er gjennomgått. Se vedlegg 2, Dokumentoversikt.

Følgende verifikasjoner/tester er utført:

Test 1: Registrerte meldinger i Datatilsynets meldingsdatabase.
Det ble undersøkt hvilke meldinger om behandling av helse- og personopplysninger ved Helse Finnmark HF som er registrert i meldingsdatabasen hos Datatilsynet.

Test 2: Journalføring av journalansvarlig person i DIPS.
Det ble undersøkt om den enkelte journal inneholdt opplysninger om hvem som var utpekt som journalansvarlig person i feltet "Pasientopplysninger/Roller overfor pasienten" (F5-bildet) og i epikrisen. 10 journaler i DIPS ved Klinikk Hammerfest ble valgt ut fra forhåndsdefinerte kriterier.

Test 3: Journalføring av journalansvarlig person i Bupdata.
Det ble undersøkt i eksempler på journaler ved BUP Hammerfest om det framgikk hvem som var utpekt som journalansvarlig person i bildet "Pasientopplysninger" og i epikrisen.

Test 4: Tilganger i DIPS.
Registrerte tilganger i DIPS ble sammenlignet med oversikt over personer i aktivt ansettelsesforhold, inkludert faste vikarer, ved Akuttmottaket (inkludert ambulanse), Klinikk Hammerfest.

[2] DIPS er den kliniske applikasjonen som benyttes som pasientadministrativt system (PAS) og elektronisk pasientjournal (EPJ) innenfor all somatisk og voksenpsykiatrisk behandling i Helse Nord.

Test 5: Tilganger i Impax.
Registrerte tilganger i Impax ble sammenlignet med oversikt over personer i aktivt ansettelsesforhold, inkludert faste vikarer, ved Radiologisk avdeling, Klinikk Hammerfest.

Test 6: Tilganger i Bupdata.
Registrerte tilganger i Bupdata ble sammenlignet med oversikt over personer i aktivt ansettelsesforhold, inkludert faste vikarer, ved BUP Hammerfest, Klinikk Psykisk helsevern og rus.

Oppslagene i DIPS, Impax og Bupdata ble utført av personell underlagt den behandlingsansvarliges instruksjonsmyndighet.

Grunnlagsdokumentasjon for utførte tester er oversendt Helse Finnmark separat.

5 OBSERVASJONER OG VURDERINGER

Myndighetene stiller en rekke konkrete krav til hvilke tiltak internkontrollsystemet for behandling av helse- og personopplysninger skal omfatte, se pkt. 3.2. I dette kapittelet redegjøres det først (pkt. 5.1) for Internrevisjonens observasjoner og vurderinger knyttet til sentrale krav i det generelle internkontrollsystemet ved behandling av helseopplysninger. I de etterfølgende punktene omtales spesifikt de elementene i internkontrollsystemet som Internrevisjonen har hatt særlig fokus på ved denne revisjonen, se pkt. 3.3.

Vedlegg 3 inneholder en oversikt over de utvalgte krav og elementer, samt Internrevisjonens vurdering av om disse er oppfylt.

5.1 Generelt om internkontroll ved behandling av helseopplysninger

5.1.1 Sikkerhetsmål, sikkerhetsstrategi og ansvarsfordeling

Personopplysningsforskriftens kapittel 2 stiller krav om at det skal fastsettes sikkerhetsmål for virksomheten og en sikkerhetsstrategi for å nå disse målene. Videre kreves det at ansvaret for informasjonssikkerhet skal være definert på alle nivå, dokumentert og kjent i organisasjonen.

De overordnede mål for informasjonssikkerhetsarbeidet ved Helse Finnmark framgår av PR0015 Informasjonssikkerhet – overordnet sikkerhetspolicy for Helse Finnmark (23.10.2008). Her er også ansvarsfordeling knyttet til informasjonssikkerhet beskrevet. I tillegg er sikkerhetsledelsen illustrert ved hjelp av et organisasjonskart i RL1910 Sikkerhetsledelse i Helse Finnmark – applikasjonsoversikt (23.04.2010). Internrevisjonen konstaterer at beskrivelsen av ansvarsfordeling i overordnet sikkerhetspolicy ikke helt samsvarer med dagens organisering og sikkerhetsledelsens sammensetning.

Felles "Styringssystem for Informasjonssikkerhet" i Helse Nord, med blant annet sikkerhetspolicy, sikkerhetsmål og sikkerhetsstrategi, er under utarbeidelse. En generell beskrivelse av fordeling av ansvar og oppgaver inngår også her. Når styringssystemet er godkjent er dette ment å erstatte deler av de foretaksspesifikke styringssystemer som finnes i dag. Det enkelte helseforetak må likevel definere og dokumentere egen sikkerhetsledelse og eventuelle tilpasninger i ansvars- og oppgavefordeling i forhold til egen organisasjon.

5.1.2 Meldeplikt / oversikt over behandlinger av helseopplysninger

I henhold til Personopplysningslovens kapittel VI, og Personopplysningsforskriftens § 7-26 har Helse Finnmark HF meldeplikt til Datatilsynet om behandling av helseopplysninger. En samlet og oppdatert oversikt over alle behandlinger av helseopplysninger i foretaket, formålet/hjemmelen for behandlingen og eventuell bruk av databehandlere, er viktig som grunnlag for ivaretakelse av meldeplikten. En slik oversikt vil også være et nyttig bidrag til internkontrollen generelt.

Helse Finnmark har utarbeidet en oversikt over applikasjoner hvor helse- og personopplysninger behandles. Oversikten inneholder opplysninger om delegert ansvar for drift, forvaltning og sikkerhet for den enkelte applikasjon. Hvilke opplysninger som behandles, hjemmel for denne behandlingen, samt opplysninger om eventuelle databehandlere inngår imidlertid ikke i oversikten.

En gjennomgang av Datatilsynets meldingsdatabase (test 1) viser at det er fire registrerte meldinger fra Helse Finnmark i databasen. Tre av disse gjelder forskning, og en gjelder kvalitetssikring av personal-opplysninger. Melding om pasientjournal i Helse Finnmark mangler. Internrevisjonen har ikke undersøkt om foretaket foretar andre meldepliktige behandlinger, eksempelvis kameraovervåkning. Gjennom intervju kom det fram at nøkkelpersonell ikke var kjent med foretakets meldeplikt, og at det ikke er etablert rutiner som sikrer at denne plikten blir ivaretatt.

5.1.3 Avviksbehandling

Personopplysningsforskriftens § 2-6 stiller krav om intern avviksbehandling, samt at avvik som har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal varsles til Datatilsynet.

I forkant av denne revisjonen har Internrevisjonen vært i kontakt med Datatilsynet for å undersøke hvordan helsevesenet generelt praktiserer denne rapporteringsplikten. Datatilsynet opplyste i e-post 10.02.2010: Erfaringene fra dette er at vi får noen meldinger uoppfordret fra virksomheter og noen meldinger etter oppfordring fra oss eller helsetilsynet i saker som kommer frem i det offentlige lys. Antallet meldinger er ikke høyt, så enten er det underrapportering, lite kjennskap til § 2-6 i virksomhetene eller ingen rutine i virksomhetene på dette området. Noen virksomheter er veldig flinke, men andre hører vi aldri noe fra. Det kan tenkes at de ikke har avvik, men vanligvis finnes ikke den virksomheten som ikke har avvik.

I samråd med Stein Erik Vetland i Tilsyn- og sikkerhetsavdelingen hos Datatilsynet, nevnes følgende eksempler på hendelser i helsetjenesten som ønskes rapportert til Datatilsynet:

- Publisering av sensitive personopplysninger på internett.
- Papirer med sensitive personopplysninger funnet i søppeldunk (også internt på sykehuset).
- Sensitive opplysninger funnet i tøy på vaskeriet.
- Mistet ark på kjøpesenter med sensitive personopplysninger.
- Sensitive personopplysninger levert til feil mottaker (elektronisk eller på papir).

I Helse Nord er det besluttet at Docmap skal benyttes som verktøy for registrering og behandling av avvik. Det vises i denne sammenheng til Oppdragsdokumentet 2009, pkt. 3.2: Helse Finnmark HF skal ta i bruk og videreutvikle Docmap som system for forebygging og oppfølging av avvik (felles prosjekt i kvalitetsnettverket). I Helse Finnmark er avviksmodulen i Docmap fortsatt under implementering. Flere opplyste i intervju at de nå venter på opplæring i bruk av Docmap for å ta dette i bruk i egen enhet.

Internrevisjonen har mottatt oversikt over registrerte avviksmeldinger i Docmap fra høsten 2008 til medio mars 2010 innenfor området informasjonssikkerhet/personvern. Dette utgjorde 11 meldinger. Vi har også fått opplyst at det var meldt enkelte hendelser relatert til behandling av helseopplysninger før Docmap ble tatt i bruk. Internrevisjonen har ikke gjennomgått meldingenes innhold, men ser at de fleste av disse nå har status lukket, noe som indikerer at de har blitt fulgt opp. Gjennom intervju kom det fram at enkelte avdelinger sjelden registrerer avvik. Avviksmodulen i Docmap er fortsatt under implementering, og flere har opplyst at de nå venter på opplæring.

Ingen av avvikene i Helse Finnmark er rapportert til Datatilsynet. Internrevisjonen har ikke vurdert om slik rapportering burde vært gjort for noen av de registrerte avvikene. Rapporteringsplikten til Datatilsynet ved uautorisert utlevering av helseopplysninger er omtalt i foretakets prosedyre for avviksbehandling, og er kjent for nøkkelpersonell.

Internrevisjonen konstaterer at avviksmeldinger med fordel kan benyttes mer aktivt i internt forbedringsarbeid. Ved en høyere meldefrekvens vil det trolig også avdekkes flere hendelser der spørsmålet om rapportering til Datatilsynet aktualiseres.

5.1.4 Sikkerhetsrevisjoner

Personopplysningsforskriftens § 2-5 pålegger den behandlingsansvarlige å utføre jevnlige sikkerhetsrevisjoner. I Normen slås det fast at slike revisjoner som minimum skal gjennomføres årlig, og det stilles en rekke krav til hvilke vurderinger revisjonene skal omfatte.

Det har ved Helse Finnmark ikke vært gjennomført sikkerhetsrevisjoner. Direktøren har i vår besluttet å ta i bruk internrevisjon som virkemiddel i internkontrollen, og har vedtatt en revisjonsplan for perioden 2010 – 2012. Her inngår enkelte avgrensede problemstillinger rundt informasjonssikkerhet/ personvern, men ikke egne sikkerhetsrevisjoner i henhold til Normens krav.

5.1.5 Ledelsens gjennomgang

Kvalitetsrådgiver/informasjonssikkerhetsansvarlig rapporterer løpende til foretaksledelsen ved behov, og deltar i møter der enkeltsaker relatert til informasjonssikkerhet behandles. Normen krever også at ledelsen minimum årlig har en helhetlig gjennomgang av status for å sikre at informasjonssikkerheten ivaretas i samsvar med mål og strategi. I 2009 ble gjennomførte risikovurderinger benyttet som grunnlag for en statusgjennomgang. Direktøren ga uttrykk for at intensjonen videre er å gjennomføre en helhetlig gjennomgang med ledelsen i desember hvert år.

Observerte forbedringsområder – Generelt om internkontroll

- Beskrivelsen av ansvarsfordeling i Overordnet sikkerhetspolicy i Helse Finnmark HF er ikke oppdatert i samsvar med dagens organisering og sikkerhetsledelsens sammensetning.
- Helse Finnmark HF har ikke en samlet oversikt over behandlinger av helseopplysninger.
- Meldeplikten til Datatilsynet er ikke ivaretatt for alle meldepliktige registre.
- Avviksmeldinger kan med fordel benyttes mer aktivt i internt forbedringsarbeid. Avviksmodulen i Docmap er fortsatt under implementering.
- Helse Finnmark HF har ikke gjennomført sikkerhetsrevisjoner. Planlagte revisjonsaktiviteter tilfredsstiller ikke Normens krav til årlige sikkerhetsrevisjoner.

5.2 Risikovurderinger

Personopplysningsforskriftens § 2-4 pålegger virksomheten å fastlegge kriterier for akseptabel risiko i forbindelse med behandlingen av personopplysninger. Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Resultatet av risikovurderingen skal sammenlignes med fastlagte kriterier for akseptabel risiko og benyttes som del av grunnlaget for valg av konkrete sikkerhetstiltak.

I PR16505 Risikovurdering av informasjonssikkerhet i Helse Finnmark HF er foretakets metodikk for gjennomføring av risikovurderinger, definisjoner og akseptkriterier for risiko fastlagt.

Som et resultat av manglende gjennomføring av risikovurderinger innenfor området informasjons-sikkerhet ble Helse Finnmark i foretaksmøte høsten 2009 pålagt å gjennomføre nødvendige risiko-vurderinger innen 15.02.2010. Foretaket har i brev til Helse Nord RHF datert 14.02.2010 redegjort for de risikovurderinger som ble foretatt i 2009, samt andre utfordringer hvor de har igangsatt forbedrings-arbeid. Risikovurderingene som er gjennomført har fokusert på temaområder, ikke den enkelte kliniske applikasjon. Eksempler på risikoforhold som er vurdert er: papirutskrifter kommer uvedkommende i hende, uvedkommende får tilgang til sensitive opplysninger via PC/skjermbilde, pasientopplysninger lagres på feil pasient. Vurderingene er oppsummert i en felles rapport med anbefalinger som er behandlet i foretaksledelsen, og fulgt opp i klinikkene. Internrevisjonen vurderer den innfallsvinkel helseforetaket har benyttet som hensiktsmessig i forhold til risikoforholdene som er vurdert, men påpeker likevel at regelverket også krever risikovurderinger knyttet til det enkelte informasjonssystem.

Foretaket har ikke gjennomført ytterligere risikovurderinger i 2010, og det foreligger ingen planer om nye vurderinger.

Helse Finnmark ga i brev til Helse Nord RHF 14.02.2010 uttrykk for et ønske om tettere samarbeid med HNIKT om gjennomføring av risikovurderinger. Dette ble i hovedsak begrunnet med forhold relatert til kompetanse. Ut fra informasjon mottatt fra foretaket og fra HNIKT konstaterer vi at det i liten grad gjennomføres risikovurderinger i fellesskap mellom partene. Internrevisjonen stiller spørsmål ved om ikke et nærmere samarbeid om utførelse av risikovurderinger ville bidratt til å framskaffe et mer helhetlig risikobilde knyttet til behandling av helseopplysninger.

Observerte forbedringsområder – Risikovurderinger

- Det er ikke gjennomført risikovurderinger knyttet til den enkelte kliniske applikasjon.
- Helse Nord IKT og Helse Finnmark HF samarbeider i liten grad om utførelse av risikovurderinger.

5.3 Behandling av helseopplysninger

Journalforskriften sier i § 5: Det skal opprettes en journal for hver pasient. Det skal som hovedregel anvendes en samlet journal for den enkelte pasient selv om helsehjelp ytes av flere innen virksomheten.

Bestemmelser om muligheter for å fravike hovedregelen framgår av samme paragraf. Det vises også til definisjon av elektronisk pasientjournal utledet av KITH (Kompetansesenter for IT i helse- og sosialsektoren AS) på kith.no.

5.3.1 Utvalgte kliniske applikasjoner

Revisjonen har omfattet helseopplysninger som behandles med elektroniske hjelpemidler. Helse Finnmark benytter mange kliniske applikasjoner i forbindelse med slik behandling. Dette revisjonsprosjektet har sett nærmere på applikasjonene DIPS, Bupdata og ulike røntgenapplikasjoner.

5.3.1.1 DIPS

DIPS er den kliniske applikasjonen som benyttes som pasientadministrativt system (PAS) og elektronisk pasientjournal (EPJ) innenfor all somatisk og voksenpsykiatrisk behandling ved Helse Finnmark. Systemadministrasjon ivaretas av HNIKT. Dette inkluderer implementering av Helse Finnmarks organisasjonsoppsett, brukeradministrasjon, roller, tilgangskoder, maler og administrasjon av leverandørens tilgang.

Helse Finnmark fikk i 2006/2007 utarbeidet en rekke prosedyrer for bruk av DIPS. Disse prosedyrene ble ikke implementert, og har ikke blitt vedlikeholdt i samsvar med versjonsendringer i programvaren. Det er ikke definert hvem som har ansvar for utarbeidelse og vedlikehold av slike prosedyrer. Internrevisjonen har fått opplyst at oppgaver i DIPS i dag løses på ulike måter innenfor foretaket, og at enkelte av disse er dokumentert i avdelingsinterne prosedyrer. Det er et uttalt mål at det skal være felles prosedyrer for hele foretaket. Det er tatt initiativ for å få etablert arbeidsgrupper med sikte på å utarbeide slike prosedyrer, men initiativet er ikke fulgt opp.

Helse Finnmark har tre stillinger som EPJ-konsulent organisert i FFU/Personalavdelingen. Disse har som hovedoppgave å tilby opplæring, brukerstøtte og kvalitetssikring knyttet til foretakets bruk av DIPS. Det er en stilling dedikert til hver av klinikkene Hammerfest, Kirkenes og Psykiatri/rus. Stillingen som EPJ-konsulent i Klinikk Hammerfest har imidlertid vært vakant i omtrent ett år. Det har i denne perioden ikke vært tilbudt gjennomgående brukeropplæring i DIPS ved Klinikk Hammerfest. Den enkelte avdeling gjennomfører selv opplæringstiltak ved behov. Informasjon om versjonsendringer i DIPS blir her bare gjort kjent via melding fra HNIKT. Dette sikrer ikke at nye/endrede funksjoner tas i bruk gjennomgående. Brukerstøtte via telefon tilbys til en viss grad av EPJ-konsulent for Kirkenes.
I intervju ble det opplyst at ansettelsesprosess i forhold til EPJ-konsulent Hammerfest nå pågår.

Ut fra Internrevisjonens vurdering medfører den beskrevne situasjonen en risiko for at datagrunnlag i DIPS ikke er pålitelig og sammenlignbart. Sviktende datagrunnlag har betydning både for pasientbehandling og for ulike rapporteringer.

5.3.1.2 Røntgensystemer

De radiologiske avdelingene benytter flere fagsystemer i forbindelse med pasientadministrasjon og dokumentasjon av diagnostisk virksomhet. Systemene som har hatt fokus ved denne internrevisjonen ved Helse Finnmark, Klinikk Hammerfest er:

- DIPSRIS – en integrert del av DIPS/EPJ. Håndterer pasientadministrasjon, røntgenrekvisisjoner, digital diktering og distribusjon av røntgensvar. Benyttes bare ved Klinikk Hammerfest.
- Agfa Impax PACS – verktøy for granskning, vurdering og beskrivelse av røntgenbilder. Håndterer lagring og transport av bilder.
- Arcidis – system for sikker overføring av røntgenbilder og radiologisk informasjon mellom sykehus og mellom helseforetak.

Brukeradministrasjon i Impax for ansatte ved radiologisk avdeling ivaretas av avdelingen selv. Øvrig systemadministrasjon og administrasjon av leverandørens tilgang ivaretas av HNIKT.

5.3.1.3 Bupdata

Barne- og ungdomspsykiatrisk virksomhet (BUP) i Helse Finnmark benytter programvaren Bupdata som verktøy i forbindelse med pasientadministrasjon og dokumentasjon av behandling. Internrevisjonens undersøkelser ble utført ved Barne- og ungdomspsykiatrisk poliklinikk Hammerfest (BUP Hammerfest).

BUP Hammerfest ivaretar selv administrasjon av Bupdata, inkludert brukeradministrasjon, roller og maler via dedikert personell. HNIKT ivaretar teknisk drift. Leverandøren har ikke fjerntilgang ettersom vedlikeholdsavtale er utløpt. EPJ-konsulent psykiatri/rus er ikke involvert i spørsmål knyttet til bruk av Bupdata.

5.3.2 Pasientjournal

Spesialisthelsetjenestelovens § 3-2 pålegger helseforetaket å sørge for at journal- og informasjonssystemene i virksomheten er forsvarlige.

Helse Finnmark har et journalutvalg som ledes av medisinsk faglig rådgiver. Av mandatet framgår det at Journalutvalget har ansvar for å vedlikeholde, forbedre og fornye de standarder som er satt for pasientjournalen med hensyn til: tilgangskontroll, journalstruktur og malutforming. Utvalget hadde to møter i 2009, men har etter september 09 ikke vært aktiv. Av protokollene fra disse møtene framgår det at utvalget behandlet en rekke saker der videre oppfølging er påkrevd. Det er ikke definert hvem som skal ivareta oppgaver knyttet til saksforberedelser for utvalget, samt koordinere oppfølging av sakene mellom utvalgets møter. Dette gjelder blant annet maler i DIPS, nødrutiner og tilgangsmatrise. Av intervju framkom det at videreføring av arbeidet med tilgangsmatrise i DIPS nå er overlatt til den enkelte klinikksjef for beslutning vedrørende egen klinikk. Tilgangsstyring i DIPS omtales nærmere i pkt 5.3.4.2. Flere ga i intervju uttrykk for et ønske om et mer aktivt Journalutvalg som arena for diskusjon og avklaring av spørsmål relatert til pasientjournalen. Etter Internrevisjonens vurdering er det behov for å avklare Journalutvalgets mandat og sammensetning, herunder definere hvem som skal ivareta saksforberedelser og oppfølging relatert til utvalgets arbeid.

I journalforskriftens § 5 heter det blant annet: Dersom journalen føres delvis elektronisk og delvis som papirjournal, skal det klart fremgå av begge hvilken dokumentasjon som føres i den elektroniske journalen og hvilken dokumentasjon som føres som papirjournal.

Representanter fra ledelse og nøkkelpersonell i stab ga uttykk for at den enkelte pasient i dag har én samlet journal ved Helse Finnmark HF. Internrevisjonen konstaterer at en slik måte å definere pasientjournalen på gir utfordringer både i forhold til de adskilte DIPS-applikasjonene i foretaket (Hammerfest og Kirkenes), og i forhold til barne- og ungdomspsykiatrisk virksomhet (BUP).

Klinikk for psykiatri og rus har fire adskilte poliklinikker for barne- og ungdomspsykiatri. Hver poliklinikk fører og arkiverer pasientjournal adskilt fra hverandre, delvis elektronisk i Bupdata og delvis på papir. En pasient kan dermed ha flere journaler innenfor samme klinikk, for eksempel hvis vedkommende har flyttet.

I intervju framkom det ulike oppfatninger av om det er papirjournalen eller elektronisk journal som er hoved-journalen. Det framgår heller ikke klart av journalen hvilken dokumentasjon som føres hvor. Som eksempel fikk Internrevisjonen presentert en av flere journaler der epikrise bare inngikk i papirjournalen, uten at dette var angitt i Bupdata.

Innenfor somatisk virksomhet kan på tilsvarende måte en pasient ha adskilte journaler i Hammerfest og Kirkenes uten at det framgår gjensidig informasjon om dette i pasientens journal.

Internrevisjonen mener at Helse Finnmark HF ikke i tilstrekkelig grad har tatt hensyn til eksisterende infrastruktur og organisering når man har definert hvordan det samlede journalsystemet er organisert. Etter Internrevisjonens vurdering har pasienten i dag ikke en samlet journal i Helse Finnmark HF.

5.3.3 Journalansvar

Av journalforskriftens § 6 framgår det at det skal utpekes en person som skal ha det overordnede ansvaret for den enkelte journal (journalansvarlig person) og at det skal framgå av journalen hvem som er journalansvarlig.

Både DIPS og Bupdata har funksjonalitet for registrering av journalansvarlig person. I Bupdata er dette uttrykt i begrepet "Saksansvarlig". For at en person skal kunne registreres som journalansvarlig i DIPS må det på forhånd være oppgitt i vedkommendes tilgangsprofil at han/hun kan tildeles en slik rolle.

Test 2 viste at ingen av de utvalgte journalene i DIPS inneholdt navn på journalansvarlig person eller pasientansvarlig lege i aktuelt felt i menyen Pasientopplysninger/Roller overfor pasienten, eller i epikrisen.

Ved BUP Hammerfest ble det opplyst at saksansvarlig alltid utpekes i forhold til den enkelte pasient, og at dette journalføres. Saksansvarlig ivaretar oppgavene som i forskrift er tillagt journalansvarlig person og pasientansvarlig lege. Journalføring av saksansvarlig ble bekreftet i test 3.

5.3.4 Tilgangsstyring

Hovedregelen når det gjelder helseopplysninger er taushetsplikt. Dette er nedfelt i blant annet spesialisthelsetjenestelovens § 6-1, helseregisterlovens § 15 og helsepersonellovens § 21.

Helseforetakets styring av tilganger til helseopplysninger skal bidra til å sikre at:

- Tilgangen bare gis i den grad de er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt. Jf. helseregisterloven § 13.
- De som yter helsehjelp gis mulighet til å registrere i pasientens journal. Jf. lov om helsepersonell §§ 39 og 40.

- Helsepersonell som yter helsehjelp, med mindre pasienten motsetter seg det, gis tilgang til alle helseopplysninger som er nødvendig for å gi forsvarlig helsehjelp. Jf. lov om helsepersonell § 45.
- Pasientens rett til å sperre helseopplysninger for helsepersonells innsyn kan ivaretas.
- Bare den databehandlingsansvarlige, databehandlere og den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet, gis tilgang. Jf. helseregisterloven § 13.

5.3.4.1 Tildeling og tilbaketrekking av autorisasjoner og tilganger

Ved ansettelse signerer medarbeidere taushetserklæring og kvitterer for at han/hun har mottatt og lest: arbeidsreglement, IKT-reglement og etiske retningslinjer. Dette ivaretas av FFU/Personalavdelingen. Den enkelte leder gir autorisasjon for behandling av helseopplysninger ved å bestille tilganger til informasjonssystemet og aktuelle applikasjoner. Bestilling av tilganger gjøres på eget skjema som sendes HNIKT for effektuering. Saksgang fram til overlevering av dette skjemaet til HNIKT samsvarer ikke alltid med intern rutinebeskrivelse, PR20108. Flere har i intervju opplyst at bestillinger sendes direkte fra avdeling til HNIKT, ikke via FFU/Personalavdelingen som rutinebeskrivelsen tilsier.

Tilganger i Bupdata og Impax opprettes av brukeradministrator ved henholdsvis BUP og Radiologisk avdeling for ansatte i egen avdeling ut fra direkte kjennskap til tjenestelige behov.

Den enkelte leder er ansvarlig for å trekke tilbake autorisasjoner når medarbeidere slutter, går ut i permisjon eller går over i ny stilling. Rutinebeskrivelse, PR20108, fastsetter interne rutiner i denne forbindelse. Her framgår det blant annet at faste vikarer kun skal ha brukertilgang i de perioder de utfører arbeid i Helse Finnmark. Tilsvarende krav gjelder for ansatte med rotasjonsavtale (begrensede arbeidsperioder i helseforetaket).

Internrevisjonen har fått opplyst at rutinene i forbindelse med tilbaketrekking av tilganger ikke fungerer tilfredsstillende. Det vises til mangelfull etterlevelse i alle ledd; manglende varsel fra avdelingsleder, manglende oppfølging/videreformidling i FFU/Personalavdeling og manglende effektuering av melding om sluttdato hos HNIKT. Dette har medført at tilganger ikke har blitt stoppet ved opphør av tjeneste. Internrevisjonen er kjent med at det siste år er gjennomført et omfattende arbeid der tilganger det ikke lenger er tjenestelige behov for har blitt fjernet. Antallet slike tilganger var svært høyt sett i forhold til antall ansatte. Så langt er det i hovedsak tilganger i DIPS som har vært fokusert i oppryddingsarbeidet. I denne sammenheng har også risikoen for at det kan finnes arbeidsoppgaver i DIPS som ikke er fulgt opp blitt belyst. Oppryddingen pågår fortsatt med sikte på å skape samsvar mellom aktive tilganger og tjenestelige behov. Internrevisjonen vil påpeke at inntil man etterlever rutiner for løpende tilbaketrekking av tilganger vil det være behov for slike oppryddinger nærmest kontinuerlig.

5.3.4.2 Tilgangsstyring i DIPS

Tilgangsstyringen i DIPS er basert på brukerroller og maler for de vanligste stillingskategoriene. Beslutningsstyrt tilgang er ikke implementert. Hovedtilgangen styres av avdelingstilhørighet og at pasienten er aktiv/relevant ved den aktuelle enheten. Av protokoller fra møter i Journalutvalget, samt opplysninger gitt i intervju, framkommer det at det er behov for en gjennomgang av tilgangsmatrisen for å sikre at denne er oppdatert og i samsvar med tjenestelige behov. Per i dag er det ikke gitt at personell i samme roller har like tilgangsrettigheter. Mange brukertilganger er i dag opprettet med utgangspunkt fra annen brukers tilgangsprofil, i stedet for fra mal. Det har via Journalutvalget vært tatt initiativ til gjennomgang av tilgangsmatrisen. Av intervju framkom det at videreføring av arbeidet med tilgangsmatrise i DIPS nå er overlatt til den enkelte klinikksjef. Internrevisjon oppfatter dette slik at det nå gis rom for ulikheter i matrisene mellom klinikkene med hensyn på den enkelte brukertypes tilganger og rettigheter.

Ut fra denne forståelsen stiller Internrevisjonen spørsmål ved om slike ulikheter bidrar i ønsket retning i forhold til foretakets mål om felles praksis for bruk av DIPS, og framtidig sammenslåing av databaser.

Nødrettstilgang (blålystilgang) gir anledning til å lese journalopplysninger for pasienter som ellers ikke er aktive for den enkelte. Bruk av blålystilgang skal begrunnes i journalen i hvert enkelt tilfelle. Prinsipper for tildeling av rett til bruk av blålys i Helse Finnmark er fastsatt.

Internrevisjonen har undersøkt om registrerte tilganger i DIPS samsvarer med aktive ansettelsesforhold, inkludert faste vikarer, ved Akuttmottaket i Hammerfest (inkludert ambulanse) (test 4). Testen viste at det her var registrert 51 tilganger. 24 av disse tilhørte personer i aktivt tilsettingsforhold eller vikarer som tilkalles gjentatte ganger i løpet av året, 17 ble opplyst å tilhøre personer som var benyttet som korttids-vikar én til to ganger i året, mens de resterende 10 var ukjent for avdelingsleder (ansettelsesforhold ikke verifisert). Testen bekreftet at det fortsatt gjenstår en del arbeid før man har fått stoppet tilganger det ikke lenger er tjenestelige behov for.

5.3.4.3 Tilgang til røntgeninformasjon

Det er opprettet tilganger som gjør at ansatte ved røntgenavdelingene i UNN HF (Tromsø) og Nordlands-sykehuset HF (Bodø), som er autorisert for dette, kan logge seg inn i røntgenbildearkivet i Hammerfest, søke fram aktuell pasient og hente røntgenbilder. Ansatte ved Radiologisk avdeling i Hammerfest, som er autorisert for dette (opplyst å være to personer), har anledning til å hente røntgenbilder fra i UNN HF (Tromsø) og Nordlandssykehuset HF (Bodø). Det ble i intervju opplyst at røntgenbilder som hovedregel utveksles via forespørsel og elektronisk oversending, men at det også hentes bilder direkte i forbindelse med overføring av pasienter. Direkte henting av helseopplysninger er ikke tillatt i henhold til gjeldende regelverk. Praksisen har vært kjent for regionens ledelse over lengre tid. For å legge til rette for lovlig overføring av røntgenbilder og radiologisk informasjon mellom HF-ene ble Arcidis implementert i regionen i 2009. Klinikk Hammerfest har ikke tatt i bruk Arcidis.

Internrevisjonen har testet om registrerte tilganger i Impax samsvarte med personer i aktivt ansettelses-forhold, inkludert faste vikarer, ved Radiologisk avdeling, Klinikk Hammerfest (test 5). Testen viste at det var 2 registrerte tilganger for radiologer som har sluttet. Ut over dette var tilganger for radiografer, radiologer og assistenter (til sammen 24 tilganger) baserte på aktive tilsettingsforhold eller regelmessige vikariat. Testen viste imidlertid at det også var registrert tilgang for 6 ortopeder og 9 IKT-konsulenter. Hvorvidt det er tjenestelige behov for disse tilgangene ble ikke undersøkt.

Det framkom gjennom intervju at det er etablert en ordning med fjerntilgang til røntgensystemer fra Sverige for radiolog, uten at det er foretatt en konkret risikovurdering i denne forbindelse. Ordningen innebærer risikofaktorer ut over det som gjelder for ordinære hjemmetilganger. Ved standard løsning for hjemmetilgang benyttes VPN og terminalserver, slik at kun terminalserver er eksponert mot eksternt nett. Bruker har da kun tilgang til skjermbilde av aktuelle applikasjoner/data. Denne løsningen drar data ut fra foretakets nettverk, og gir nettverkstilgang til foretakets systemer fra utstyr fysisk plassert utenfor foretakets kontroll. Jf. redegjørelse fra Helse Nord IKT datert 15.09.2010.

5.3.4.4 Tilgang til BUP-journal

Systemadministrator ved BUP oppretter og inaktiverer tilganger i Bupdata ut fra tilgjengelige rollemaler. Personlige tilpasninger i tilgangsprofilen kan foretas ved behov. Test 6 bekreftet at registrerte tilganger i Bupdata (16 tilganger) samsvarer med aktive ansettelsesforhold, inkludert én fast vikar, ved BUP Hammerfest.

I Bupdata har den enkelte behandler kun tilgang til opplysninger om pasientene de er direkte involvert i behandlingen av. Journalen føres imidlertid delvis på papir (se pkt. 5.3.2). Papirjournalene oppbevares samlet på førstesekretærs kontor, og må hentes her. Internrevisjonen har fått opplyst at det gjentatte ganger er fokusert på at papirjournaler ikke skal oppbevares over natt på den enkelte behandlers kontor, men returneres til arkiv ved arbeidsdagens slutt. Det ble videre hevdet at man de senere år ikke har hatt situasjoner med papirjournaler på avveie. Det er imidlertid ikke etablert noe system for å kontrollere eller dokumentere hvem som henter hvilke pasientjournaler, og at disse blir fortløpende returnert. I forbindelse med ambulant virksomhet er det ikke uvanlig at aktuelle papirjournaler medbringes. Heller ikke i slike situasjoner dokumenteres uttak og retur av journaler. Etter Internrevisjonens vurdering utgjør dette en risikofaktor som med enkle tiltak kan reduseres.

5.3.4.5 Kontrolltiltak for å avdekke urettmessig tilegnelse av helseopplysninger

Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helseopplysninger som behandles etter denne loven uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift, jf. helseregisterloven § 13 a.

Helse Finnmark har nylig iverksatt rutinemessige stikkprøver av tilgangslogg for pasientjournal i DIPS, og det foreligger plan for videre gjennomføring av slike kontroller. Logg for bruk av nødrettstilgang (blålys) blir regelmessig gjennomgått, og eventuelle uregelmessigheter blir fulgt opp. Blant annet er det blitt påpekt overfor enkeltpersoner at begrunnelsesfeltet ikke er tilfredsstillende utfylt.

Internrevisjonen vurderer de innførte kontrolltiltakene som hensiktsmessige, spesielt i forhold til å forebygge misbruk av tilganger. Helseforetaket oppfordres til å dokumentere gjennomførte kontroller på en slik måte at en oversikt over disse enkelt kan legges fram.

Observerte forbedringsområder – Behandling av helseopplysninger

- Det er ikke lagt til rette for felles praksis i bruk av DIPS. Dette medfører en risiko for at datagrunnlag i DIPS ikke er pålitelig og sammenlignbart. Ansvar for utarbeidelse og vedlikehold av felles brukerprosedyrer er ikke definert.
- Det er behov for å avklare Journalutvalgets mandat og sammensetning, herunder definere hvem som skal ivareta saksforberedelser og oppfølging relatert til utvalgets arbeid.
- Pasienten har ikke en samlet journal i Helse Finnmark HF.
- Ved Klinikk Hammerfest framgår det ikke av journalen hvem som er journalansvarlig person.
- Tilganger til IT-systemer trekkes ikke tilbake når tjenestelige behov opphører.
- Det er behov for å gjennomgå og oppdatere tilgangsmatrise og rollemaler i DIPS.
- Det eksisterer gjensidige tilganger, som ikke er i samsvar med gjeldende lovverk, til å hente røntgeninformasjon på tvers av HF-grensene.
- En ordning med ekstern tilgang til røntgensystemene fra Sverige er etablert uten at det er foretatt en konkret risikovurdering i denne forbindelse. Ordningen innebærer risikofaktorer ut over det som gjelder for ordinære hjemmetilganger.
- Det er ikke etablert noe system for dokumentasjon eller kontroll av uttak og retur av papirjournal fra arkiv ved BUP Hammerfest.

5.4 Ivaretakelse av informasjonssikkerhet hos databehandlere og leverandører

Den behandlingsansvarlige er ansvarlig for at helseopplysninger blir behandlet i henhold til gjeldende krav. Dette gjelder selv om databehandlere og leverandører som behandler helseopplysninger eller benytter informasjonssystemet på vegne av den behandlingsansvarlige har et selvstendig ansvar for å ha tilfredsstillende informasjonssikkerhet. Den behandlingsansvarlige skal etablere klare ansvars- og myndighetsforhold overfor databehandlere og leverandører, beskrevet i en særskilt avtale. Den behandlingsansvarlige skal videre forsikre seg om at databehandlere og leverandører sørger for tilfredsstillende informasjonssikkerhet. Jf. helseregisterlovens § 16 og § 18, samt personopplysnings-forskriftens § 2-15. Normen krever eksplisitt at behandlingsansvarlig i forbindelse med sikkerhets-revisjoner skal gjøre en vurdering av ivaretakelse av informasjonssikkerhet hos kommunikasjons-partnere, databehandlere og leverandører.

Databehandleravtalen mellom Helse Finnmark og HNIKT omtaler HNIKTs plikter og Helse Finnmarks oppfølging. Det framgår her at Helse Finnmark har ansvar for å påse at HNIKTs informasjonssikkerhet er tilfredsstillende. Avtalen slår videre fast at Helse Finnmark skal ha tilgang til dokumentasjon hos HNIKT og har rett til å gjennomføre sikkerhetsrevisjoner, eventuelt via tredjepart, hos HNIKT.

Foretakets oversikt over behandlinger av helseopplysninger inneholder ikke opplysninger om eventuelle databehandlere (se pkt. 5.1.2). Gjennom intervju kom det fram at det i forbindelse med pasientjournal benyttes minst én ekstern databehandler (skrivetjeneste), i tillegg til HNIKT. Det er uklart om det foreligger undertegnet databehandleravtale i denne forbindelse. Internrevisjonen har etterspurt kopi av slik avtale, uten at dette er framskaffet.

Helse Finnmark har ikke gjennomført sikkerhetsrevisjoner hos kommunikasjonspartnere, databehandlere og leverandører (se også pkt. 5.1.4) eller iverksatt andre tiltak for å vurdere hvorvidt sikkerhetsstrategien hos databehandlere og leverandører gir tilstrekkelig sikkerhet for helseopplysninger som behandles.

Observerte forbedringsområder – databehandlere og leverandører

- Det er ikke bekreftet at det foreligger databehandleravtaler med alle foretakets databehandlere.
- Helse Finnmark HF har ikke iverksatt tiltak for jevnlig å forsikre seg om at sikkerhetsstrategien hos databehandlere og leverandører gir tilfredsstillende informasjonssikkerhet.

6 KONKLUSJON OG ANBEFALINGER

6.1 Konklusjon i forhold til revisjonens formål

Basert på de undersøkelser som er foretatt ved Helse Finnmark HF konkluderer Internrevisjonen med at behandlingen av helseopplysninger innenfor enkelte områder ikke er i samsvar med gjeldende regelverk.

Helse Finnmark HF sitt opplegg for internkontroll inneholder svakheter som bør forbedres for å sikre at helseopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på helseopplysninger.

6.2 Anbefalinger

Internrevisjonen anbefaler Helse Finnmark HF å iverksette følgende tiltak:

1. Videreutvikle oversikten over behandlinger av helseopplysninger, og etablere rutiner som sikret at oversikten kontinuerlig er oppdatert og fullstendig, inkludert informasjon om databehandlere.
2. Sørge for at meldeplikten til Datatilsynet etterleves for alle meldepliktige behandlinger av helse- og personopplysninger.
3. Benytte avviksmeldinger mer aktivt i internt forbedringsarbeid.
4. Videreføre og videreutvikle gjennomføring og bruk av risikovurderinger, gjerne i samarbeid med Helse Nord IKT.
5. Definere hvordan foretakets samlede journalsystem er organisert, og etablere rutiner som sikrer at informasjon i den enkelte pasientjournal samsvarer med dette.
6. Fullføre oppryddingsarbeidet for å skape samsvar mellom tilganger til IT-systemer og tjenestelige behov, sørge for at tilganger løpende inaktiveres når tjenestelige behov opphører, samt gjennomføre regelmessige kontroller av at samsvar mellom tilganger og behov opprettholdes.
7. Gjennomgå og oppdatere tilgangsmatrise og rollemaler i DIPS.
8. Legge til rette for felles praksis i bruk av DIPS og andre elektroniske journalsystemer, herunder innføre felles rutiner for registrering av journalansvarlig person i DIPS.
9. Sørge for at utveksling av røntgeninformasjon på tvers av HF-ene samsvarer med gjeldende lovverk (eventuelt i samarbeid med andre aktører i Helse Nord), og fjerne tilgangene for ansatte ved andre helseforetak til å hente røntgeninformasjon fra Helse Finnmark.
10. Foreta en konkret risikovurdering i forbindelse med etablert fjerntilgang til røntgensystemer, samt gjennomføre risikoreduserende tiltak dersom uakseptabel risiko avdekkes.
11. Vurdere etablering av system for dokumentasjon/kontroll av uttak og retur av papirjournal fra arkiv ved BUP.
12. Gjennomføre sikkerhetsrevisjon og ledelsens gjennomgang minimum årlig.
13. Iverksette tiltak for jevnlig å forsikre seg om at sikkerhetsstrategien hos databehandlere og leverandører gir tilfredsstillende informasjonssikkerhet.
14. Videreutvikle helseforetakets internkontrollrutiner med sikte på forbedring av øvrige svakheter Internrevisjonen har påpekt i denne rapporten.

7 VEDLEGG

Vedlegg 1 – Deltakeroversikt

Navn	Funksjon	Avd./enhet	Oppstartsmøte	Intervju	Oppsummeringsmøte
Eva Håheim Pedersen	Direktør		X	X	
Jan-Erik Hansen	Ass. direktør		X		
Leif Arne Asphaug-Hansen	Kvalitetsrådgiver	FFU/Personalavdeling	X	X	X
Geir Lindrupsen	IKT-bestiller	Klinikk for drift og eiendom		X	
Jens Herstad	Juridisk rådgiver	FFU/Personalavdeling		X	
Jes Westergaard	Medisinsk-faglig rådgiver			X	
Nils Petter Hallonen	EPJ-konsulent Kirkenes	FFU/Personalavdeling		X	
Erik Fjeldstad	Personalsjef	FFU/Personalavdeling		X	
Bodil Brox	Avdelingsleder	Klinikk Hammerfest, Akuttmottaket	X	X	
Karin Engstad	Avdelingsleder	Klinikk Hammerfest, Radiologisk avdeling	X	X	
Grete Norvang	Avdelingsoverlege	Klinikk Hammerfest, Radiologisk avdeling			X
Vivi B. Bech	Klinikksjef	Klinikk Hammerfest	X		X
Vigdis Kvalnes	Ass. klinikksjef	Klinikk Hammerfest		X	
Ingeborg Eliassen	Fagkonsulent	Klinikk Hammerfest			X
Kirsten Myhre Hansen	Avdelingsleder	BUP Hammerfest		X	
Marit Gagama	Førstesekretær	BUP Hammerfest		X	X
Tove Merethe Johnsen	EPJ-konsulent Psyk/rus	FFU/Personalavdeling		X	
Robert Ketcher	Leder	DPS Vest-Finnmark		X	
Roger Johansen	Konsulent	Helse Nord IKT, EPJ		X	

Fra Internrevisjonen i Helse Nord RHF:

Navn	Funksjon	Avd./enhet	Oppstartsmøte	Intervju	Oppsummeringsmøte
Hege Knoph Antonsen	Internrevisor	Helse Nord RHF	X	X	X

Vedlegg 2 - Dokumentoversikt

Dokumenter innsendt/levert av revidert enhet i forkant av, eller i forbindelse med, intervju.

Styrende dokumenter (retningslinjer, prosedyrer etc.):

- PR0015: Informasjonssikkerhet - Overordnet sikkerhetspolicy i Helse Finnmark HF, versjon 2.
- RL1910: Sikkerhetsledelse i Helse Finnmark – applikasjonsoversikt, versjon 1.
- RL1504: Hefte gjeldende informasjonssikkerhet. Følgende skal ansatte i Helse Finnmark HF etterleve om informasjonssikkerhet, versjon 1.2.
- PR4710: Arbeidsreglement for Helse Finnmark HF, versjon 1.
- SJ1003: Erklæring taushetsplikt, versjon 1
- PR0018: IKT-reglement, versjon 2.4.
- PR16915: Avviksbehandling Informasjonssikkerhet i Helse Finnmark, versjon 1.1.
- f)PR16508: Opplæring – informasjonssikkerhet i Helse Finnmark HF, versjon 1.
- PR18685: Tilgangsprinsipper EPJ i Helse Finnmark HF, versjon 1.
- PR16785: Sikkerhetspolicy gjeldene bærbare Pcer, hjemmekontor etc , versjon 1.3.
- via OL0908: Brukerregistrering Helse Finnmark (bestillingsskjema).
- PR20108: EPJ Helse Finnmark HF - Rutinebeskrivelse for innmelding og utmelding av brukere, versjon 1.
- PR16505: Risikovurdering av informasjonssikkerhet i Helse Finnmark HF, versjon 1.
- PR16506: Sikkerhetsrevisjon: Ledelsens gjennomgang og akseptabelt risikonivå i Helse Finnmark HF, versjon 1.
- PR16931: Taushetsplikt- ved innleie av eksternt ansatte, versjon 1.
- PR16502: Innsyn i pasientjournal, utlevering av journalkopi og journallogg, versjon 3.
- PR16499: Loggføring og kontroll av innsyn i pasientdokumenter journal, versjon 1.2.
- PR16503: Instruks pasientjournalen: Retting, sletting og sperring, versjon 1.1.
- Mandat for Journalutvalget (mottatt på e-post 02.09.2010).
- Mal for arbeidsavtale fra Personalavdelingen (mottatt i forbindelse med intervju).

Oversikter/planer:

- Organisasjonskart Helse Finnmark HF (fra Helse Finnmarks internettsider).
- Plan for internrevisjon 2010 – 2012, Helse Finnmark HF.
- Journalinndeling med tilgangskontroll (tilgangsmatrise DIPS), datert 14.08.2006.
- Oversikt over medlemmer i Journalutvalget, mottatt på e-post datert 14.04.2010.

Inngåtte avtaler:

- Databehandleravtale mellom Helse Finnmark HF og Helse Nord IKT
- Driftsavtale (SLA) mellom Helse Finnmark HF og Helse Nord IKT

Resultatdokumentasjon:

- Oversikt over registrerte avviksmeldinger i Docmap fra høsten 2008 til medio mars 2010 innenfor området informasjonssikkerhet/personvern.
- Rapport om informasjonssikkerhet, RoS-analyser Helse Finnmark 2009, datert 14.02.2010.
- Protokoller fra møter i Journalutvalget 2009.
- Registrerte meldinger om behandling av helse- og personopplysninger i Datatilsynets meldingsdatabase.
- Oversikt over gjennomførte kurs og undervisninger 2009 og 2010 – juridisk rådgiver.
- Presentasjon fra undervisning 29. og 30.10.2009: Pasientjournal; begrunnelse, ansvar og innhold.
- Presentasjon fra undervisning 13.11.2009: Taushetsplikt, informasjon, samtykke og litt om tvang.

Annet:

- Brev til Helse Nord RHF datert 14.02.2010: Informasjonssikkerhet i Helse Finnmark – ROS-analyser.
- Redegjørelse fra Helse Nord IKT til IKT-bestiller Helse Finnmark HF, e-post datert 15.09.2010, vedrørende ekstern tilgang til røntgeninformasjon.

Vedlegg 3

Oversikt over krav ifm internrevisjonen: Internkontroll ved behandling av helseopplysninger

Oversikten inneholder utvalgte krav sett i forhold til revisjonens formål og fokusområder utledet fra:

- Helseregisterloven (HR)
- Personopplysningsforskriften (POL)
- Helsepersonelloven (HP)
- Journalforskriften (JF)
- Norm for informasjonssikkerhet i helsesektoren (Norm)

Nr.	**Krav**	**Regel-verk**	**Ref.**	**Er kravet ivaretatt**		**Kravet er ivaretatt av:**		**Kommentar** IR = ikke undersøkt eller ikke relevant
				Ja	Nei	HF	HNIKT	
	Hjemmel for/meldeplikt om behandlingsrettet helseregister							
1.	Er det sendt pålagte meldinger til Datatilsynet om behandlingsrettet helseregister? Evt. til Personvernombud dersom virksomheten har dette.	HR POL	§ 29 § 7-12		X			Mangler for pasientjournal.
2.	Er meldingen(e) til Datatilsynet fornyet siste 3 år?	HR	§ 29					Se nr. 1. Bare meldinger siste 3 år er tilgjengelige.
	Grunnlag for internkontroll ved behandling av helseopplysninger							
3.	Er ansvar og oppgaver for informasjonssikkerhet dokumentert i et organisasjonskart/beskrivelse?	POL	§ 2-7	X		X		Kart ok. Beskrivelse ikke helt oppdatert.
4.	Oppfattes og praktiseres ansvars- og oppgavefordeling i samsvar med beskrivelse?	POL	§ 2-7	X		X		Med enkelte unntak der beskrivelse mangler oppdatering.
5.	Er det fastsatt sikkerhetsmål for virksomheten?	POL	§ 2-3	X		X		
6.	Er det utarbeidet sikkerhetsstrategi for å nå sikkerhetsmålene?	POL	§ 2-3	X		X		
7.	Er det dokumentert nivå for akseptabel risiko for konfidensialitet, tilgjengelighet, integritet og kvalitet?	POL Norm	§ 2-4 4.4	X		X		

Nr.	Krav	Regel-verk	Ref.	Er kravet ivaretatt		Kravet ivaretas av:		Kommentar
				Ja	Nei	HF	HNIKT	
	Risiko- og sårbarhetsanalyser							
8.	Er det gjennomført og dokumentert risikovurderinger av alle informasjonsbehandlingssystemer eller registre som inneholder helse- og personopplysninger?	POL Norm	§ 2-4 4.6		X			Gjennomført for utvalgte tema i 2009.
9.	Blir det gjennomført og dokumentert risikovurderinger før det iverksettes organisatoriske endringer som kan påvirke informasjonsbehandlingen?	POL Norm	§ 2-4 4.6					IR
10.	Blir det gjennomført og dokumentert risikovurderinger før det iverksettes tekniske endringer i utstyr og/eller programvare som kan påvirke informasjonsbehandlingen?	POL Norm	§ 2-4 4.6		X			Eksempelvis ekstern tilgang røntgen.
11.	Er resultatet av risikovurderingene sammenlignet med fastlagt nivå for akseptabel risiko?	Norm	4.6	X		X		
12.	Følges resultater fra risikovurderingene opp?	Norm	3.3.3	X		X		
	Journalansvar							
13.	Utpekes det alltid en person som har det overordnede ansvar for den enkelte journal?	JF	§ 6		X			Gjelder Klinikk Hammerfest.
14.	Framgår det av journalen hvem som er journalansvarlig?	JF	§ 6		X			Gjelder Klinikk Hammerfest.
	Tilgangsstyring							
15.	Er det bare den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet som kan gis tilgang til helseopplysninger?	HR	§ 13		X			Gjelder Rønrgen
16.	Autoriseres bruker selvstendig for hver enkelt rolle?	Norm	5.2.1	X		X		
17.	Har alle personer unike autentiseringskriteria?	Norm	5.2.1	X		X		
18.	Autoriseres kun teknisk personell med særskilt behov for tilgang for større mengder helse- og personopplysninger?	Norm	5.2.2					IR
19.	Gjennomføres det regelmessige analyser av tilgangslogg?	Norm	5.2.2	X		X		
20.	Er det etablert prosedyre for nødrettstilgang?	Norm	5.3.1	X		X		
21.	Følges all bruk av nødrettstilgang opp som avvik?	Norm	5.3.1		X			Men logg gjennomgås regelmessig.
22.	Grunngis og registreres bruk av nødrettstilgang i EPJ-systemet?	Norm	5.5.2	X		X		Mangler blir påpekt.

Nr.	Krav	Regel-verk	Ref.	Er kravet ivaretatt		Kravet ivaretas av:		Kommentar
				Ja	Nei	HF	HNIKT	
23.	Kontrolleres tilgangsstyring, herunder tildelte autorisasjoner, ved organisasjonsendringer, overflytting av personell til annen enhet/avdeling eller endring av arbeidsområde?	Norm	5.3.2		X			
24.	Kontrolleres tilgangsstyring minimum årlig ?	Norm	5.3.2		X			
	Informasjonsplikt/pasientens rettigheter							
25.	Får pasienten informasjon om virksomhetens behandling av helse- og personopplysninger, og sine rettigheter til innsyn i, retting, sletting og sperring av hele/deler av egen journal?	Norm	5.3.3	IA		X		
26.	Er pasientens rett til sperring av hele eller deler av egen journal ivaretatt?	Norm	5.3.3	X		X		
	Databehandlere og leverandører							
27.	Har den behandlingsansvarlige oversikt over hvilke databehandlere og leverandører som er involvert i behandling av helseopplysninger i det enkelte informasjonssystem?	POL Norm	§ 2-15 4.5		X			
28.	Er det inngått avtale med databehandler(e) iht kravene i Normen?	Norm	5.8.2		X			Avtale med skrivetjeneste ikke verifisert.
29.	Har databehandler gjennomført risikovurdering, ved etablering av skille mellom flere virksomheter, når databehandler er databehandler for flere virksomheter?	Norm	5.8.2					IR
30.	Er det inngått avtale med alle leverandører som har tilgang til helseopplysninger iht kravene i Normen?	Norm	5.8.3					IR
31.	Forsikrer den behandlingsansvarlige seg jevnlig om at sikkerhetsstrategien hos databehandlere og leverandører gir tilfredsstillende informasjonssikkerhet?	POL	§ 2-15		X			
	Avviksbehandling							
32.	Benyttes avvikssystemet iht intensjonen i forhold til behandling av helseopplysninger?	POL Norm	§ 2-6 6.3	X				Forventes flere meld. når Docmap er benyttes mer.
33.	Er det etablert prosedyre der det framgår at Datatilsynet skal varsles ved uautorisert utlevering av helseopplysninger?	POL Norm	§ 2-6 6.3	X				
34.	Varsles Datatilsynet ved uautorisert utlevering av helse- og personopplysninger?	POL Norm	§ 2-6 6.3		X			Ingen hendelser er varslet. Ingen klart meldepliktige hendelser avdekket.

Nr.	Krav	Regel-verk	Ref.	Er kravet ivaretatt		Kravet ivaretas av:		Kommentar
				Ja	Nei	HF	HNIKT	
	Ledelsens kontroll og oppfølging							
35.	Gjennomføres det sikkerhetsrevisjon minimum årlig?	POL Norm	§ 2-5 6.1		X			
36.	Foreligger det en plan for sikkerhetsrevisjoner?	Norm	6.1		X			Bare begrensede områder.
37.	Dokumenteres resultatet av sikkerhetsrevisjonene?	POL Norm	§ 2-5 6.1					IR
38.	Gjennomføres det ledelsens gjennomgang av internkontroll for behandling av helse- og personopplysninger minimum årlig? (omf. gj.gang av bl.a. risikovurd., sikkerhetsrev., avviksrapp., konfigurasjonskart, ansvar og organisering og sikkerhetsmål)	Norm	6.4	X				Gjennomført 2009. Intensjon om gjennomgang i desember hvert år.