NORDLANDSSYKEHUSET
NORDLÁNDA SKIPPIJVIESSO

Direktøren

Styresak 037-2018
Orienteringssak - Informasjonssikkerhet - status pr mai 2018

Saksbehandler:	Alisa Larsen
Dato dok:	30.04.2018
Møtedato:	23.05.2018
Vår ref:	2015/1426

Vedlegg (trykt): Rapport prosess risikovurderinger informasjonssikkerhet

Vedlegg (ikke tr.): Oppdragsdokument 2018
Styresak 107-2017 Orienteringssak - Informasjonssikkerhet – status pr desember 2017

Innstilling til vedtak:

1. Styret er tilfreds med gjennomføring av risikoanalyser og resultat og tar saken til orientering.
2. Styret ber om å bli presentert en redegjørelse for fjernlagerløsningen jf. 107-2017 ved neste statusrapportering til styret om informasjonssikkerhet.

Bakgrunn:

Oppdragsdokument for 2018 stiller krav om at foretakene skal styrebehandle status på risiko- og sårbarhetsanalyser om informasjonssikkerhet innen 1. juni 2018, jf punkt 4.2.3. Styret har tidligere fått forelagt orienteringssaker om arbeidet med informasjonssikkerhet i Nordlandssykehuset i 2015, 2016 og 2017.

Beskrivelse:

Helse Nord RHF fremmet i november 2015 bestilling til foretakene om gjennomføring av ROS-analyser innenfor informasjonssikkerhet med følgende innhold:

Risiko- og sårbarhetsvurderinger rundt hvert enkeltregister innen kategoriene nedenfor:

1. *Applikasjoner som hovedjournalsystem og spesialistmoduler*
   - *Hovedjournalsystem (DIPS)*
   - *Laboratoriesystemer*
   - *Røntgensystemer*
   - *Spesialistmoduler som er egne applikasjoner med et spisset medisinsk spesialistfokus*
2. *Registre som etableres av resultater/prøver/tester fra medisinsk teknisk utstyr, og som lagres i egne strukturerte registerløsninger levert av samme leverandør som har levert MTU.*
3. *Enkle databaser/registre/skåringsverktøy som i begrenset grad kan kalles en applikasjon, men som klart er behandlingsrettede registre. Dette dekker registre/databehandlinger ned til 2-3 brukere. Disse inneholder fokuserte og strukturerte deler av journalen, der nødvendig*

struktur på informasjonen ikke kan oppnås i de mer generelle og overordnede journalapplikasjonene. De er i noen grad etablert i foretakets registerstøtteverktøy, men også i enkle databaser/Excel-ark som den enkelte kliniker selv har etablert. Mange slike småsystem registreres som kvalitetssystem. Relevante data registreres også i DIPS, som er den formelle journalen.

Rapportering på kategori 1 og 2
Gjennomføring og resultat av kategori 1 i bestillingen ble rapportert i styresak 040-2017. Videre ble gjennomføring og resultat av kategori 2 i bestillingen rapportert i styresak 107-2017.

Fremdrift kategori 3 i bestillingen
Arbeidet med risikovurderinger innenfor kategori 3 av bestillingen har blitt gjennomført løpende siden bestillingen ble fremmet.

Alle risikovurderinger som var planlagt ble gjennomført i perioden fra november 2015 til april 2018. Samlet rapport ligger som vedlegg 1. Det er utformet rapport til hver enkelt risikovurdering. På bakgrunn av overnevnte anser vi at bestillingens punkt 3 er gjennomført.

Status på tiltak
Tiltak har blitt lukket løpende i perioden risikovurderingene har blitt gjennomført. Det foreligger noen tiltak som ikke er lukket for de risikovurderingene som er gjennomført sist. Lukking av disse tiltakene følges opp.

Resultater fra risikovurderingene som er gjennomført viser at Nordlandssykehuset har god kontroll på informasjonssikkerhet og personvern.

I 2018 innføres ny personvernlovgivning i Norge og Europa. I Helse Nord pågår det for tiden arbeid med å revidere prosedyrer knyttet til det nye regelverket. I reviderte prosedyrer presiseres foretakenes ansvar om internkontroll, inkludert krav om gjennomføring av risikovurderinger. Det nye regelverket har som formål å beskytte borgernes rettigheter til personvern ytterligere og setter strengere krav til virksomheter som behandler personopplysninger.

For foretaket betyr dette at vi i fremtiden må ha stort fokus på personvern og informasjonssikkerhet for å kunne ivareta regelverket. Fortsettelse av arbeidet med kontinuerlige risikovurderinger vil være en viktig del av ivaretagelsen.

Redegjørelse for fjernlagerløsningen
Ved behandling av styresak 040-2017 Orienteringssak - Informasjonssikkerhet - status pr april 2017 ba styret i vedtakspunkt 4 om følgende:

4. *Med henvisning til aktuell global virus-hendelse ønsker styret ved Nordlandssykehuset en redegjørelse fra Helse Nord RHF mht hvilket behov og løsning man har for fjernlagerløsning for de kliniske data som driftes ved de regionale datasenter.*

Dette gjelder den regionale løsningen etablert av Helse Nord. Nordlandssykehuset ba, med utgangspunkt i anmodningen fra styret, i brev av 22.09.2017 om en redegjørelse fra Helse Nord for å få beskrevet hvordan en slik løsning er etablert. Slik redegjørelse er nødvendig for at vi skal kunne gjøre en vurdering av om dette dekker vårt beredskapsbehov og krav til informasjonssikkerhet.

Da det ikke var mottatt svar på vår henvendelse ved statusrapportering i desember 2017, fattet styret i forbindelse med behandling av styresak 107-2017 Orienteringssak - Informasjonssikkerhet - status pr desember 2017 nytt vedtakspunkt 3:

3. *Styret ber om å bli presentert en redegjørelse for fjernlagerløsningen jf styresak 040-2017.*

Nordlandssykehuset har purret på tilbakemelding fra Helse Nord i brev av 12.02.2018. Svar fra Helse Nord er fremdeles ikke mottatt.

Rapport prosess risikovurderinger informasjonssikkerhet

Innhold

1. Bakgrunn

Riksrevisjonen har gjennomført flere revisjoner ved Helseforetakene i Norge. Revisjoner har vist manglende evne til å oppfylle de lovmessige forpliktelser som regulerer blant annet området informasjonssikkerhet. Følgende er hentet fra innstilling til Stortinget fra kontroll- og konstitusjonskomiteen s.179 (2014-2015)

«Helseforetakene mangler eller har mangelfulle risiko- og sårbarhetsanalyser og beredskapsplaner for IKT, vann og strøm. Disse innsatsfaktorene er avgjørende for sykehusdriften. Helseforetakene gjennomfører få beredskapsøvelser, og ledelsen i helseforetakene følger i liten grad opp dette arbeidet. Videre er helseforetakene lite bevisst sin rolle som eier av dataene og databehandlingsansvarlig. Selv om Helse- og omsorgsdepartementet og de regionale helseforetakene har lagt til rette for beredskapsarbeidet, har oppfølgingen vært for svak»

På bakgrunn av overnevnte har Helse Nord RHF i november 2015 fremmet følgende bestilling til foretakene om gjennomføring av risiko- og sårbarhetsvurderinger innenfor informasjonssikkerhet med følgende innhold:

Risiko- og sårbarhetsvurderinger rundt hvert enkeltregister innen kategoriene nedenfor:

1. *Applikasjoner som hovedjournalsystem og spesialistmoduler*
    - *Hovedjournalsystem (DIPS)*
    - *Laboratoriesystemer*
    - *Røntgensystemer*
    - *Spesialistmoduler som er egne applikasjoner med et spisset medisinsk spesialistfokus*
2. *Registre som etableres av resultater/prøver/tester fra medisinsk teknisk utstyr, og som lagres i egne strukturerte registerløsninger levert av samme leverandør som har levert MTU.*
3. *Enkle databaser/registre/skåringsverktøy som i begrenset grad kan kalles en applikasjon, men som klart er behandlingsrettede registre. Dette dekker registre/databehandlinger ned til 2-3 brukere. Disse inneholder fokuserte og strukturerte deler av journalen, der nødvendig struktur på informasjonen ikke kan oppnås i de mer generelle og overordnede journalapplikasjonene. De er i noen grad etablert i foretakets registerstøtteverktøy, men også i enkle databaser/Excel-ark som den enkelte kliniker selv har etablert. Mange slike småsystem registreres som kvalitetssystem. Relevante data registreres også i DIPS, som er den formelle journalen.*

2. Avgrensninger

Denne rapporten gir en beskrivelse av status for Nordlandssykehuset med fokus på punkt tre i bestillingen. For punkt en og to er det gjennomført og rapportert egne risikovurderinger og disse er ikke beskrevet i denne rapporten.

Enkle databaser, registre og skåringsverktøy er i bruk i en rekke kliniske miljøer ved Nordlandssykehuset. I all hovedsak dreier dette seg om enkle fremstillinger, gjerne i Excel-format. Det ansees at det ikke er innholdet i de enkelte filene som er problematiske med tanke på risiko knyttet til informasjonssikkerhet og personvern. I den grad risiko skal vurderes, må denne ses opp mot hvordan de enkelte databasene, registrene og data i skåringsverktøyene er lagret.

Når det gjelder registre har det blitt utarbeidet egne rutiner som ivaretar informasjonssikkerhet ved lagring av data. Denne typen informasjon omfattes av foretakets rutiner for kvalitetssikringsprosjekter og kvalitetsregister (DS9948 Kvalitetssikringsprosjekter/kvalitetsregister.) Dersom filens innhold tilsier det, etableres det også en KEY-mappe. Dette innebærer at nøkler som kan kobles mot pasient-ID lagres atskilt fra selve filene. Da systemet ble etablert, var det gjenstand for en ROS-analyse, der også representanter fra Helse Nord IKT deltok[1].

Som nevnt ovenfor, er vi av den oppfatning at eventuell risiko som slike registre utgjør, ikke er relatert til filene som sådan, men til hvordan disse håndteres og lagres. På dette området har foretaket iverksatt en rekke tiltak som ivaretar sikkerhet på en grundig, forutsigbar og systematisk måte. På bakgrunn av overnevnte har vi valgt å ikke gjennomføre flere analyser vedrørende registre i excel-format.

[1] Se nedenfor pkt 5.1 Sikker lagring av forskningsdata

3. Personopplysningsforskriftens føringer for informasjonssikkerhet og risikovurderinger

Personopplysningsforskriften (pof) kapittel 2 omhandler informasjonssikkerhet og stiller krav til sikkerhet ved behandling av personopplysninger.

§ 2-1. Forholdsmessige krav om sikring av personopplysninger

Reglene i dette kapittelet gjelder for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler der det for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet er nødvendig å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene. Der slik fare er til stede skal de planlagte og systematiske tiltakene som treffes i medhold av forskriften, stå i forhold til sannsynligheten for og konsekvens av sikkerhetsbrudd.

§ 2-4. Risikovurdering

Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.

§ 2-10. Fysisk sikring

Det skal treffes tiltak mot uautorisert adgang til utstyr som brukes for å behandle personopplysninger etter forskriften her. Sikkerhetstiltakene skal også hindre uautorisert adgang til annet utstyr av betydning for informasjonssikkerheten. Utstyr skal installeres slik at ikke påvirkning fra driftsmiljøet får betydning for behandlingen av personopplysninger.

§ 2-11. Sikring av konfidensialitet

Det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig. Sikkerhetstiltakene skal også hindre uautorisert innsyn i annen informasjon med betydning for informasjonssikkerheten. Personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig.

§ 2-12. Sikring av tilgjengelighet

Det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig. Sikkerhetstiltakene skal også sikre tilgang til annen informasjon med betydning for informasjonssikkerheten. Alternativ behandling skal forberedes for de tilfeller informasjonssystemet er utilgjengelig for normal bruk. Personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk, skal kopieres.

§ 2-13. Sikring av integritet

Det skal treffes tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig.

Sikkerhetstiltakene skal også hindre uautorisert endring av annen informasjon med betydning for informasjonssikkerheten. Det skal treffes tiltak mot ødeleggende programvare.

§ 2-14. Sikkerhetstiltak

Sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk. Forsøk på uautorisert bruk av informasjonssystemet skal registreres. Før man etablerer nye tjenester som involverer sensitive personopplysninger, skal det i henhold til kapittel 2 i personopplysningsforskriften gjennomføres risikovurdering.

4. Prosess

Høsten 2014 ble felles styringssystem for informasjonssikkerhet for Helse Nord godkjent. Informasjonssikkerhetsansvarlig gjennomførte i den forbindelse møter med hver klinikk for å orientere om innholdet i styringssystemet. I forbindelse med orienteringen fikk klinikkene i oppdrag å gjennomgå de systemene som brukes av klinikken og som inneholder personopplysninger.

På bakgrunn av tilbakemeldingene fra klinikkene ble det utformet en oversikt over alle systemer som benyttes hos Nordlandssykehuset HF. For hver av systemene ble det gjort en vurdering på hvilke systemer som er å anse som kritiske.

Formålet med systemoversikten er at virksomheten skal ha oversikt over hvilke behandlinger av helse- og personopplysninger som foretas, og hvilke opplysninger som inngår i disse. Oversikten er nødvendig for at virksomheten skal kunne ivareta pliktene sine etter personopplysningsloven med forskrift og helseregisterloven. Oversikten danner også grunnlag for prioritering av risikovurderinger.

Nordlandssykehuset HF har sammen med Fagråd for informasjonssikkerhet (FRIS) tatt utgangspunkt i Norm for informasjonssikkerhet[2](Normen), med tilhørende faktaark 6B som grunnlag for risikovurderingene[3].

I perioden fra bestillingen fra Helse Nord ble fremmet har det blitt gjennomført løpende risikovurderinger som faller inn under dette punkt. Rapporten representerer et utvalg av de risikovurderinger som er gjennomført. De risikovurderinger som presenteres har følgende uttrekk.

[2] https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet

[3] Norm for informasjonssikkerhet i helse og omsorgstjenesten (Normen) er et omforent sett av krav til informasjonssikkerhet basert på lovverket.

Føringer/metodikk for gjennomførte risikovurderinger

Nordlandssykehuset HF sin definisjon av akseptkriterier for akseptabel risiko (PR25911 Risikovurdering og risikostyring, kapittel 4.1.2) har vært lagt til grunn for risikovurderingene som beskrives. Akseptkriteriene er gjengitt nedenfor. Disse er også i tråd med føringer fra Normens faktaark 5 – Nivå for akseptabel risiko.

- Grønn: Tiltak vurderes å ikke være nødvendig
- Gul: Tiltak må vurderes
- Rød: Tiltak anses som nødvendig

4.1.1 Matrise

Matrisen som er valgt er hentet fra Norm for informasjonssikkerhet (normen.no) faktaark nr. 5 – nivå for akseptabel risiko. Den er også gjengitt i faktaark 7 - Risikovurdering.

Svært stor sannsynlighet				
Stor sannsynlighet				
Middels sannsynlig				
Liten sannsynlighet				
	Lav konsekvens	**Middels konsekvens**	**Alvorlig konsekvens**	**Svært alvorlig, kritisk konsekvens**

4.1.2 Klassifisering sannsynlighet og konsekvens

I denne prosessen har vi valgt å følge fagråd for informasjonssikkerhet i Helse Nord sin inndeling av sannsynlighet og konsekvens. Denne er gjengitt i tabell nedenfor.

4.1.2.1 Sannsynlighet

Kategori NLSH	Kategori What IF[4]	Frekvens
Svært stor sannsynlighet	Svært sannsynlig	Hendelsen inntreffer flere ganger ukentlig/daglig
Stor sannsynlighet	Meget sannsynlig	Hendelsen inntreffer flere ganger årlig
Middels sannsynlig	Sannsynlig	Hendelsen inntreffer årlig
Liten sannsynlighet	Lite sannsynlig	Hendelsen inntreffer sjeldnere enn annethvert år

[4] For flere av risikovurderingene ble verktøyet Whatif benyttet. Klassifisering av sannsynlighet og konsekvens i Whatif er tatt med i tabellene.

4.1.2.2 Konsekvens

Kategori NLSH	Kategori What IF[5]	Lovregulering	Anseelse, rykte, tillit	Kvalitet på helsehjelp	Pasientenes personvern
Svært alvorlig, kritisk	Katastrofal	Lovbrudd. Fengselsstraff/ foretaksstraff. Tap av rett til å utøve virksomhet	Ødeleggende virkning på tillit og respekt	Uforsvarlig helsehjelp for flere pasienter, med mulighet for tap av liv	Alvorlig tap av anseelse mht. personvern for et stort antall pasienter. Påvirker liv, helse eller økonomi
Alvorlig	Alvorlig	Lovbrudd. Bøtestraff/ foretaksstraff (bot)	Alvorlig tap av anseelse. Langvarig virkning på tillit og respekt	Helsehjelp med utilstrekkelig kvalitet for flere personer, med mulighet for alvorlig nedsatt helse.	Store mengder sensitive opplysninger tilgjengelig for uvedkommende
Middels	Moderat alvorlig	Lovbrudd. Advarsel/ pålegg (som første reaksjon). F.eks. sensitive opplysninger for et mindre antall pasienter på avveier	Tap av anseelse. Virkning på tillit og respekt.	Hinder for utøvelse av effektiv helsehjelp. Varig nedsatt helse, av mindre alvorlig karakter	Brudd på personvernet for noen pasienter pga. kompromittering av sensitive opplysninger
Lav	Lite alvorlig	Forseelse. Advarsel/ pålegg (som første reaksjon).	Tap av anseelse. Kortvarig virkning på tillit og respekt	Kortvarig hinder for utøvelse av effektiv helsehjelp for et lite antall pasienter. Ikke fare for helse.	Kompromittering av lite følsomme opplysninger

[5] For flere av risikovurderingene ble verktøyet Whatif benyttet. Klassifisering av sannsynlighet og konsekvens i Whatif er tatt med i tabellene.

4.2 Avgrensninger i forhold til de enkelte risikovurderingene

I de gjennomførte risikovurderingene har det vært deltakere fra utvalgte klinikker/avdelinger som brukere av systemet. Deres bidrag inn mot risikovurderingene har primært vært å beskrive hvordan de opptrer i dag i forhold til systemet. Dette gir oss en god indikasjon på hvordan sannsynlighetsbildet for mange av de ulike uønskede hendelsene er. Når det gjelder konsekvens i forhold til brudd på lovkrav, forskrifter mm. har vurderingen blitt gjort av informasjonssikkerhetsansvarlig og personvernombud.

5. Risikovurderingene

5.1 Sikker lagring av forskningsdata

I 2015 ble det etablert et sikkert lagringsområde for lagring av forskningsdata. Med sikkert menes en logisk adskilt lagrings-struktur som kan behandles slik at det for en bruker ikke vil være tvil om at data lagres separat og er av annen karakter enn data som kan lagres på andre områder (personlig lagringsområde, lokal disk og fellesområder). Dataene som skal lagres vil være dokumenter, regneark, databaser og multimedia materiale i forbindelse med forskningsprosjekter. Sensitiviteten på materialet vil være alt fra anonymisert data til konfidensielle rapporter og personopplysninger. I forbindelse med etableringen ble det gjennomført en risikovurdering av løsningen.

Det ble identifisert to høye trusler som omhandlet manglende systemeier og manglende systemansvarlig. I etterkant av risikovurderingen ble det etablert prosedyrer som sikrer at truslene ikke anses som høye lenger. Tiltakene er derfor lukket.

5.2 Bruk av klinisk lync/Skype

Denne risikovurderingen ble gjennomført i forbindelse med pilotprosjekt for å kunne kommunisere med Lync/Skype mellom behandlere og pasienter eller samarbeidspartnere. Det ble gjennomført to tiltak som skulle dekke opp tuslene som ble avdekket. Det første var å utforme en intern prosedyre for bruk av klinisk lync. Denne prosedyren skulle bl.a. dekke opp tuslene som ble avdekket på behandler sin side. Det andre tiltaket var at det skulle utformes en samarbeidsavtale som samarbeidspartner skulle signere og gjøre seg kjent med. Dette ville dermed for utenforstående personer dekke opp de truslene som ble avdekket for bruk utenfor foretaket.

5.3 Q-Interactive

Q- interactive er en web-tjeneste/ digital testplattforms tjeneste som leveres av Pearson hvor brukere logger seg direkte på Pearson for å få tilgang til Q-interactives tester av IQ for barn.

Det ble avdekket en trussel vurdert som høy. Det gjaldt manglende databehandleravtale. Videre ble det avdekket to middels trusler. De omhandlet vern av pasienters rettigheter samt systemeierskap. Alle truslene har blitt møtt med tiltak som er lukket.

5.4 Eir

Eir er ett elektronisk web basert verktøy for symptomkartlegging og beslutningsstøtte. Pasienten registrerer selv aktuelle symptomer på et nettbrett. Pasientens svar leses i EIRs helsepersonell del som åpnes på intern PC i en webleser og gir behandler mulighet til å følge utvikling over tid og anbefale behandling for aktuelle symptomer. EIR benyttes som en del av det nasjonale forskningsprosjektet PALLION ved flere sykehus i Norge. EIR vil bli benyttet ved Avdeling for kreft og lindrende behandling, på Enhet for blodsykdommer og kreft (poliklinikk), Enhet for stråleterapi og av Palliativt Team ved tilsyn på sengeposter. I Pallion-studien skal de inkludere 30 pasienter, men EIR skal også brukes på alle andre pasienter som erstatning for manuelt ESAS skjema for symptomkartlegging.

I denne risikovurderingen ble ingen trusler vurdert til å ha høy risiko. Det ble avdekket tre trusler som ble vurdert til å ha middels risiko. Dette gjaldt hendelsesregistrering i form av logging av bruk av applikasjonen, oppfylling av krav til dokumentasjonsplikt og uautorisert bruk av nettbrettet for tilgang til andre systemer i nettverket. Alle disse har blitt møtt med tiltak i form av rutiner for bruk av nettbrett og overføring av dokumentasjon til DIPS.

5.5 Ednor

Ednor er et behandlingsregister der pasient besvarer kartleggingsskjema. I tillegg registreres administrativ informasjon i Ednor slik som henvisning, tiltak, vedtaksparagrafer osv.

Det er avdekket to trusler som anses som høye og som det skal gjennomføres tiltak på. Dette omfatter sperring av innsyn fra ansatte dersom pasient ønsker dette. Ednor har pr. i dag ikke denne funksjonen. Videre ble det avdekket at det mangler en driftsavtale med HN-IKT som sikrer forsvarlig drift.

Denne risikovurdering er gjennomført rett før denne rapport er utformet og tiltakene er dermed ikke utført, men er under oppfølging. Det er utarbeidet egen rapport fra risikovurderingen. Denne inneholder også tiltaksplan for å redusere risiko. Tiltaksplan beskriver tiltak, ansvarlig for tiltak og tidsfrist.

5.6 Imatis

Imatis er en programvareløsning som består av moduler med ulike bruksområder. Imatis Visi er et digitalt verktøy for informasjonsflyt, prosess- og beslutningsstøtte. Visi gir oversikt over pasienter (ventede og innleggende) og viser informasjon og status på pasient og kommuniserer med blant annet med DIPS. I systemet har ansatte mulighet til å oppdatere status for pasient og oppgaver knyttet til behandling av pasient. Informasjonen er tilgjengelig for ansatte på elektroniske tavler på sengepostene og via mobile enheter.

Scenario hvor risiko ble vurdert til høy er knyttet til tilgangsstyring i NLSH og etterlevelse av overordnede dokumenter når ansatte skifter organisasjonsenhet. Når ansatte skifter arbeidssted internt er det en risiko for at tilgangsrettigheter ikke endres og ansatte dermed har tilgang til mer informasjon enn de har behov for. Det er etablert overordnet prosedyre for tilgangsstyring men det er usikkerhet knyttet til i hvilke grad prosedyren følges.

Denne risikovurdering er gjennomført rett før denne rapport er utformet og tiltakene er dermed ikke utført, men er under oppfølging. Det er utarbeidet egen rapport fra risikovurderingen. Denne

inneholder også tiltaksplan for å redusere risiko. Tiltaksplan beskriver tiltak, ansvarlig for tiltak og tidsfrist.

5.7 Checkware

Checkware er et klinisk verktøy som skal brukes til å innhente pasientinformasjon utenfor domenet HN. Pasientene fyller selv ut tilsendte spørreundersøkelser (tester). Disse lagres og bearbeides i Checkware utenfor domenet og sendes til Nordlandssykehuset og Dips arbeidsflyt som en foreløpig rapport. Denne rapporten brukes av behandler som grunnlag for videre behandling. Det er avdekket to trusler som måtte lukkes før verktøyet kunne benyttes dette omfattet opplæring samt utarbeidelse av prosedyrer. Begge tiltakene er lukket.

6. Oppsummering

Oppsummert kan vi ut fra risikovurderingene som er gjennomført se at Nordlandssykehuset har god kontroll på informasjonssikkerhet og personvern.

For å kunne oppnå tilfredsstillende informasjonssikkerhet må den behandlingsansvarlige gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. For å kunne oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige dokumentere informasjonssystemene og sikkerhetstiltakene (jfr. Personopplysningsloven § 13). Gjennomføring av risikovurderinger er et viktig tiltak

I 2018 innføres ny personvernlovgivning i Norge og Europa. I Helse Nord pågår det for tiden arbeid med å revidere prosedyrer knyttet til det nye regelverket. I reviderte prosedyrer presiseres foretakenes ansvar om internkontroll, inkludert krav om gjennomføring av risikovurderinger. Det nye regelverket har som formål å beskytte borgernes rettigheter til personvern ytterligere og setter strengere krav til virksomheter som behandler personopplysninger.

For foretaket betyr dette at vi i fremtiden må ha stort fokus på personvern og informasjonssikkerhet for å kunne ivareta regelverket. Og ved å fortsette arbeidet med kontinuerlige risikovurderinger vil være en viktig del av ivaretagelsen.