PASIENTREISER

Saksframlegg

Referanse

Saksgang:

Styre	Møtedato
Styret Pasientreiser HF	13/09/2017

SAK NR 23-2017
Behandling av personopplysninger - oppfølging av styresak 05-2017

Forslag til vedtak:

1. Styret tar redegjørelsen om helseforetakets systemer, rutiner og kontroller for håndtering av krav til informasjonssikkerhet, herunder behandling av sensitive personopplysninger, personvern og tilgangssystemer, til etterretning.
2. Styret ber om at det iverksettes en rådgivende ekstern gjennomgang av helseforetakets etterlevelse av ansvar og rutiner relatert til personvernområdet med bakgrunn i gjennomgangen i foreliggende sak.

Skien 6. september 2017

Marit Kobro
Administrerende direktør

1. Hva saken gjelder

I styresak 05-2017 ble det gjort rede for utfordringsbildet for behandling av personopplysninger innenfor pasientreiseområdet. Den omfattende og varierte behandlingen, med mange ulike aktører, gjør at det er en høy iboende risiko for at det oppstår feil på personvernområdet. På bakgrunn av denne saken, ba styret om en nærmere redegjørelse for Pasientreiser HF sine systemer, rutiner og kontroller for håndtering av krav til informasjonssikkerhet, herunder behandling av sensitive personopplysninger, personvern og tilgangssystemer.

2. Hovedpunkter og handlingsalternativer

2.1 Forholdet mellom personvern og informasjonssikkerhet

Personopplysningsloven har som formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Personvern er spørsmålet om det foreligger rett til å bruke opplysningene som ønskes brukt, på den måten det er ønskelig å bruke dem. Informasjonssikkerhet handler om sikringen av de opplysningene som brukes. Informasjonssikkerhet er en del av personvernet, men personvern favner videre enn bare informasjonssikkerhet. Dette betyr at selv om informasjonssikkerheten er ivaretatt, kan det tenkes at kravene til personvern likevel ikke er oppfylt. Begge forhold må ivaretas for å sikre at Pasientreiser HFs behandling er forsvarlig og lovlig.

2.2 Internkontroll

2.2.1 Innledning

Personopplysningsloven § 14 og personopplysningsforskriften § 3-1 stiller krav til internkontroll av behandlingen av personopplysninger. Her fremgår bl.a. at det må gjennomføres en kartlegging av hvilke krav man må forholde seg til etter lov og forskrift på bakgrunn av de behandlinger som utføres. På dette grunnlaget skal det vurderes om det er behov for tiltak for å sikre etterlevelse av kravene. Det er ingen plikt til å iverksette tiltak etter alle krav, da loven kun krever tiltak som anses som «nødvendige». Internkontrollen skal inneholde nødvendige rutiner for oppfyllelse av virksomhetens plikter og de registrertes rettigheter, samt nødvendige rutiner og tekniske tiltak for informasjonssikkerhet.

2.2.2 Internkontroll innenfor pasientreiseområdet

I Pasientreiser HF inngår kravene til informasjonssikkerhet og personvern i foretakets alminnelige internkontroll. I tillegg er det opprettet en personverngruppe som skal styrke virksomhetens kompetanse innenfor personvern, og sørge for den daglige oppfølgningen av behandlingsansvaret og foretakets etterlevelse av personvernreglene.

Det er et lovpålagt krav at internkontrollsystemet skal være dokumentert. Datatilsynet har utviklet en veileder om internkontroll og informasjonssikkerhet. I tillegg er det utviklet en Norm for informasjonssikkerhet (Normen) for helse- og omsorgstjenesten som er utgitt med støtte av Direktoratet for e-helse. Ifølge disse bør dokumentasjonen deles inn i tre hoveddeler: Styrende, gjennomførende og kontrollerende dokumentasjon. Pasientreiser HF har tatt utgangspunkt i disse føringene ved utarbeidelse av foretakets internkontrollsystem.

Pasientreiser HF utfører halvårlige risikovurderinger for foretaket, samt årlige risikovurderinger for hele pasientreiseområdet. Sikkerhetsrevisjoner gjennomføres etter behov, på bakgrunn av disse risikovurderingene. Ledelsens gjennomgang skjer i ledergruppa årlig. Foretaket har også utarbeidet rapporter i informasjonsverktøyet RADAR på kjente utfordringsområder innenfor personvern, samt rutiner for avviksmelding, både internt i helseforetaket og eksternt fra pasientreisekontorene.

Når det gjelder internkontroll for informasjonssikkerhet, foreligger det omfattende dokumentasjon som viser at Pasientreiser HF har nødvendige rutiner og tiltak på dette området, og det meldes få avvik. Internrevisjonen har vurdert informasjonssikkerheten på pasientreiseområdet i flere revisjoner og konkludert med at det ikke er vesentlige svakheter i virksomhetsstyringen. Påpekte forbedringsforslag og utfordringer fra internrevisjonen har blitt håndtert gjennom påfølgende handlingsplaner og sluttrapporter til styret.

Som databehandleransvarlig, har Pasientreiser HF fulgt opp at internkontrollen er forsvarlig ved alle pasientreisekontor i 2010/2011 og 2015. Det var i tillegg en egen oppfølging av utvalgte pasientreisekontor i 2012/2013. I 2012 og 2014 ble det gjennomført egne gjennomganger av sentrale IKT-leverandører til foretaket. Fokuset var på informasjonssikkerhet generelt og at kravene som stilles i Normen blir ivaretatt på en betryggende måte.

Selv om kravene til informasjonssikkerhet er ivaretatt, viser interne gjennomganger at foretaket har enkelte utfordringer knyttet til personvernreglene. Høsten 2017 planlegges det en ny gjennomgang av IKT-leverandørene, hvor fokuset blant annet vil være personvern og tilgangsstyring.

2.3 Utfordringer

2.3.1 Dokumentasjon

Internkontrollsystemet hos Pasientreiser HF er godt dokumentert i TQM (elektronisk internkontrollsystem). Det er kun enkelte dokumenter som mangler for å ivareta alle krav til dokumentasjon, blant annet en oversikt over all behandling av personopplysninger som gjøres og en oversikt over formålene med disse behandlingene. Et konfigurasjonskart som gir en oversikt over informasjonssystemene må også utarbeides, samt en oversikt over partnere, leverandører og databehandlere som har tilgang til systemene. I tillegg bør noe av dokumentasjonen oppdateres. Foretaket har igangsatt et arbeid med å innfri alle krav til dokumentasjon. Handlingsplanen som ble vedlagt styresak 05-2017 er oppdatert med frister, se vedlegg. Når foretaket får personvernombud vil denne personen overta ansvaret for at dokumentasjonen er fullstendig og oppdatert til enhver tid.

2.3.2 Grunnkrav for behandling av personopplysninger

Personopplysningsloven § 11 stiller en rekke grunnkrav som må være på plass før behandling av personopplysninger starter. Det må foreligge et hjemmelsgrunnlag for behandlingen etter lovens §§ 8 og 9. I tillegg kan opplysningene bare brukes til uttrykkelig angitte formål, som er saklig begrunnet i den behandlingsansvarliges virksomhet.

Pasientreiser HF har utarbeidet rutiner som skal følges ved behandling av opplysninger. Likevel viser kartleggingen av virksomhetens behandling av personopplysninger at det ved enkelte av behandlingene ikke er avklart formålet med behandlingen, hvilket hjemmelsgrunnlag behandlingen har og hvem som er behandlingsansvarlig. Innen styremøtet i desember vil Pasientreiser HF ha gjennomført nødvendige avklaringer i forhold til hvem som er behandlingsansvarlig i samsvar med vedtaket fra styremøtet 7. juni. I dette arbeidet avklares også formål og hjemmelsgrunnlag for behandlingene. Det vil inngås nye og oppdaterte databehandleravtaler i samsvar med ansvarsforholdene som avklares.

2.3.3 Behandling av sensitive personopplysninger

Det følger av lov og personvernprinsipper at sensitive personopplysninger har krav på strengere beskyttelse enn andre personopplysninger. Dette fremgår også av foretakets policy for informasjonssikkerhet. I praksis har det likevel ikke blitt skilt mellom behandling av sensitive og andre personopplysninger. Dette håndteres ved at all behandling følger de strengere kravene som gjelder for behandling av sensitive opplysninger, da det er vurdert som uhensiktsmessig å skille på hvilke personopplysninger som behandles.

2.3.4 Tilgangsstyring

Formålet med tilgangsstyring er å sikre at personopplysninger bare er tilgjengelig for rett person til rett tid, altså etter tjenstlig behov. Pasientreiser HF baserer seg på rollebasert tilgangsstyring til foretakets systemer. For at tilgangsstyring skal være korrekt må tilgangen være tilpasset det tjenstlige behovet for informasjon rollen har, og denne vurderingen gjøres i forbindelse med opprettelse av roller i systemet.

Alle tilganger i PRO og NISSY ved pasientreisekontorene ble gjennomgått og oppdatert i forbindelse med gjennomgangen av internkontroll i 2015. I etterkant har disse tilgangene blitt gjennomgått av systemadministrator for å sikre at tilgangene er i samsvar med tjenstlig behov. Høsten 2017 vil det gjøres en tilsvarende gjennomgang av øvrige nasjonale systemer for å sikre at det også er god tilgangsstyring i disse systemene.

2.3.5 Ny forordning

I april 2016 vedtok EU en ny forordning om behandling av personopplysninger (personvernforordningen), som inkorporeres i norsk lov i slutten av mai 2018. Den nye forordningen inneholder enkelte skjerpede krav til behandlingsansvarlige. I dag er kravene etter regelverket mer generelle i uttrykksformen, noe som kan føre til at de er vanskelige å håndtere i det daglige. For eksempel sier Personopplysningsforskriften § 2-4 at det skal gjennomføres risikovurderinger ved behandling av personopplysninger, men den gir ingen veiledning i hva som må med i en risikovurdering. Den nye personvernforordningen stiller også krav til innholdet i en risikovurdering.

På områdene hvor Pasientreiser HF har fulgt anbefalingene fra datatilsynet angående personvern, i tillegg til kravene etter dagens regelverk, er kravene etter den nye forordningen allerede ivaretatt. I forbindelse med at databehandleravtaler oppdateres i forhold til nye systemer, ses det likevel på om det er behov for å gjøre tilpasninger for å tilfredsstille

forordningens krav til mer detaljerte databehandleravtaler. For eksempel sier dagens avtaler at pasientreisekontorene kan bruke helseopplysninger til administrasjon, men etter forordningens regler må dette konkretiseres.

3. Administrerende direktørs anbefalinger

Vesentlige sider ved virksomheten innenfor pasientreiseområdet innebærer større eller mindre grad av behandling av personopplysninger. Som gjengitt i saken er det således en høy iboende risiko for at det oppstår feil på personvernområdet. Dette er også gjenspeilet i gjennomførte risikovurderinger i foretaket. I den halvårlige risikovurderingen pr april (styresak 04-2017) var området "risiko for feil håndtering av person- og helseopplysninger" plassert i gul sone. Det var også angitt tidligere og nye tiltak. Neste halvårlige risikovurdering legges frem for styret i oktobermøtet.

På bakgrunn av skjerpet fokus og ny kunnskap om hvilke personopplysninger som behandles, samt forberedelse til ny forordning, vil det nå bli foretatt en gjennomgang og oppdatering av dokumentasjon, samt avklaring av ansvarsforhold og databehandleravtaler.

Den nye forordningen stiller som krav til Pasientreiser HF at det skal oppnevnes et personvernombud. Målet er å få denne rollen på plass fra og med 1.1.2018. En dedikert ressurs til arbeidet med personvern og informasjonssikkerhet vil tilrettelegge for økt fokus på området, nødvendig kontinuitet i arbeidet og at uklare ansvarsforhold i foretaket fjernes.

For å unngå utfordringer knyttet til ansvarsforhold er det administrerende direktørs anbefaling at Pasientreiser HF i fremtiden i større grad bør søke å være behandlingsansvarlig for informasjon i systemer som eies av foretaket. Foretaket vil ta kontakt med Helse- og omsorgsdepartementet for å se på muligheten for å regulere dette i forskrift. Et alternativ kan også være å vurdere om dette kan håndteres innenfor handlingsrommet som allerede ligger i organiseringen av pasientreiseområdet. For enkelte behandlinger vil foretaket se på muligheten for å etablere et behandlingsgrunnlag gjennom at brukerne aksepterer foretakets vilkår for bruk av systemene.

Som saken viser, har foretaket et systematisk fokus på personvernområdet. Arbeidet som er gjort så langt har avdekket enkelte svakheter som adresseres med relevante tiltak. Det er administrerende direktørs vurdering at arbeidet som gjøres vil rette opp svakhetene som er oppdaget og sørge for at foretaket jobber riktig med personvern og informasjonssikkerhet fremover.

Styret vedtok i juni å iverksette en ekstern gjennomgang av helseforetakets etterlevelse av ansvar og rutiner relatert til informasjonssikkerhet med bakgrunn i drøftingen i denne saken.

Tidligere gjennomført revisjon og drøfting i denne saken viser at informasjonssikkerheten i foretaket er godt ivaretatt, men at det er avdekket enkelte svakheter på personvernområdet. Administrerende direktør anbefaler derfor at det iverksettes en ekstern rådgivende gjennomgang av helseforetakets etterlevelse og ansvar med hovedvekt på personvernområdet.

Trykt vedlegg: oppdatert handlingsplan

Utrykt vedlegg: oversikt over dokumenter knyttet til internkontrollarbeidet