Datatilsynet

MOTTATT
26 APR. 2018

Sykehuset Innlandet HF
Saksnr 16/01990-25
26 APR 2018
Arkiv kode 000 U.off.
Max år
Bøn. HELSE

Sykehuset Innlandet HF
Postboks 104
2381 BRUMUNDDAL

Deres referanse	Vår referanse	Dato
	16/01531-87/GRA	19.04.2018

Vedtak om pålegg - overtredelsesgebyr til Sykehuset Innlandet HF

Vi viser til vårt varsel om vedtak av 24.10.2017 og deres svar datert 02.01.2018.

Datatilsynet gir med dette vedtak om overtredelsesgebyr i tråd med vårt varsel av 24. oktober 2017. Vedtaket er gitt med hjemmel i pasientjournalloven § 27. Nærmere begrunnelse gis i det følgende.

1. Kort oppsummering av saken

Datatilsynets varsel om vedtak gjelder pålegg mot Sykehuset Innlandet HF om å betale overtredelsesgebyr for brudd på bestemmelsene i pasientjournalloven, personopplysningsloven og personopplysningsforskriften i forbindelse med beslutningen om å tjenesteutsette driften av helseregionens IKT-infrastruktur.

Saksforholdet og Datatilsynets vurderinger er utførlig beskrevet i vårt varsel om vedtak og vi har valgt å ikke gjengi hele innholdet her.

Bakgrunnen for saken er at Datatilsynet i brev av 26. mai 2017 ba alle helseforetakene i Helse Sør-Øst RHF redegjøre for hvilke risikovurderinger og aksept av restrisiko som lå til grunn for beslutningen om å tjenesteutsette ansvaret for IKT-drift i regionen. Vi mottok likelydende svar fra alle helseforetakene datert 14. juni 2017 der det ble gjort rede for hvilke vurderinger som er gjort i forbindelse med at det ble inngått avtale med ekstern leverandør om strategisk samarbeid og IKT-drift.

Kort oppsummert er det fem forhold knyttet til den konkrete kontraktsinngåelsen som etter vår vurdering innebærer brudd på bestemmelsene i pasientjournalloven § 22 og personopplysningsloven §§ 13-15:

- De behandlingsansvarlige helseforetakene ikke har hatt tilstrekkelig eierskap til, eller kontroll med de planlagte endringene knyttet til informasjonssystemet.
- Helseforetakene har overlatt ansvaret for beslutninger som har betydning for pasientenes personvern og informasjonssikkerheten knyttet til behandling av personopplysninger, til databehandleren og til ansatte lenger ned i organisasjonen.

- Det ble ikke gjennomført nødvendige risiko- og sårbarhetsvurderinger før det ble besluttet å konkurranseutsette avtale om strategisk partnerskap, herunder drift og vedlikehold av IKT-infrastruktur.
- Det ble ikke gjennomført nødvendige risiko- og sårbarhetsanalyser i forkant av at det ble besluttet å velge underleverandør i Bulgaria.
- Valgt underleverandør har i et begrenset tidsrom hatt tilgang til pasientopplysninger i strid med ledelsens forutsetning om tilgangskontroll.

Datatilsynet mener det er svært alvorlig at denne avtalen ble inngått uten at det forelå tilstrekkelige risikovurderinger og uten at restrisiko ble vurdert og akseptert av de behandlingsansvarlige i forkant av avtaleinngåelsen. Vi varslet derfor i medhold av pasientjournalloven §§ 29 jf. 22 og 5 følgende pålegg i vårt vedtak av 24. oktober 2017:

Sykehuset Innlandet HF pålegges å betale et overtredelsesgebyr til statskassen, pålydende Kr. 800 000,- -kroner åttehundretusen- , for

1. *overtredelse av bestemmelsene i personopplysningsforskriften om sikkerhetsledelse og organisering av sikkerhetsarbeidet i virksomheten jf. §§ 2-3, 2-7 og 2-15,*
2. *brudd på krav om å gjennomføre risikovurdering ved endringer som har betydning for informasjonssikkerheten i samsvar med kravene i § 2-4 jf.2-1 pasientjournalloven § 22 samt*
3. *overtredelse av bestemmelsene om tilgangskontroll i personopplysningsforskriften §§ 2-11 og 2-13 til 2-15.*

2. Datatilsynets kommentarer til innspill fra helseforetaket

Vi har vurdert helseforetakets merknader i brev av 2. januar 2018 og gjennomgår disse kronologisk i det følgende.

Innledningsvis bemerker Sykehuset Innlandet HF at virksomheten ikke har vesentlige innsigelser til at foretaket, som databehandlingsansvarlig, har et selvstendig ansvar. Foretaket tar også til etterretning Datatilsynets vurdering om at foretaket burde vært mer aktiv med vurderinger og beslutninger i prosessen med å inngå avtale og etablere underleverandør for Sykehuspartner HF.

Sykehuset Innlandet har enkelt merknader som de ber Datatilsynet ta i betraktning i vurdering, utforming og utmåling av endelige vedtak.

2.1 Strukturelle forhold – felles i regionen

Sykehuset Innlandet viser til at Datatilsynet har lagt til grunn at «foretaket har utvist skyld ved å overlate beslutninger som betydning for virksomhetens plikter etter personopplysningsforskriften og pasientjournalloven til moderniseringsprosjektet uten å sikre at beslutninger som var akseptable i forhold til virksomhetens risikotoleranse og uten å sørge for ledelsesforankring før beslutninger ble tatt».

Det vises til styresak 069-216 i Helse Sør-Øst RHF september 2016 der styret i det regionale foretaket vedtok at det skulle inngås kontrakt med en ekstern partner. Styret i Helse Sør-Øst

RHF la til grunn at det fortsatt skulle være Sykehuspartner HF som skulle være ansvarlig for de samlede IKT-leveransene mot helseforetakene.

Sykehuset Innlandet merker seg Datatilsynets vurdering om at foretaket, som databehandlingsansvarlig, skulle vært mer aktiv og ansvarlig med vurderinger og beslutninger i prosessen med å inngå avtale og etablere underleverandør for Sykehuspartner. Foretaket vil følge opp dette med nødvendige tiltak og vil innføre forbedringer i system og rutiner på informasjonssikkerhets- og personvernområdet, slik at Sykehuset Innlandets databehandlingsansvar blir ivaretatt, også ved regionale løsninger og tjenester.

Foretaket orienterer videre om at det er iverksatt et felles arbeid i helseregionen der foretakenes selvstendighet og databehandleransvar skal sikres formelt og reelt ved endringer eller innføring av nye felles systemer, herunder tydeliggjøre og styrke metoden for gjennomføring av risikovurderinger. Inkludert i dette er vurdering i det enkelte helseforetak om for eksempel restrisiko kan aksepteres eller om det er behov for ytterligere tiltak før endring/ innføring av nytt system.

Datatilsynet tar foretakets merknader om strukturelle forhold til etterretning. Tiltakene som er iverksatt for å sikre ivaretakelse av de databehandlingsansvarliges ansvar og plikter vurderes som nødvendige for å sikre at helseregionens organisasjonsstruktur ivaretar de enkelte foretakenes selvstendige ansvar. Tiltakene har ikke betydning for vår vurdering av avvik og utmåling av overtredelsesgebyr.

Ut over at vi tar foretakets innspill til etterretning, oppfatter vi svaret fra Sykehuset Innlandet slik at det ikke gjøres innsigelser mot de vurderingene som ligger til grunn for vårt varsel om vedtak.

2.2 Databehandleravtalen mellom Sykehuset Innlandet HF og Sykehuspartner HF
Sykehuset Innlandet viser til databehandleravtalen de har med Sykehuspartner HF. Kapittel 8 i avtalen omhandler bruk av underleverandører. I henhold til avtalen har Sykehuset Innlandet HF det fulle ansvar som databehandlingsansvarlig, mens Sykehuspartner HF er hoveddatabehandler med en rekke underleverandører. Sykehuspartner er hovedansvarlig for driften som omfatter ansvar for tilgangsstyring med utøvende kontroll på at tilganger gis i henhold til lov, forskrift, gjeldende retningslinjer og akseptabel risiko. Databehandleren må oppfylle kravene og har det utøvende ansvaret for å ivareta informasjonssikkerheten, mens databehandlingsansvarlig har et kontrollansvar for databehandlerens utførelse av databehandlingen.

Avtalen beskriver rolle, oppgaver og ansvar knyttet til dem. Med bakgrunn i Datatilsynets varsel og erfaring fra den regionale prosessen så langt, innrømmer Sykehuset Innlandet at de må følge opp databehandleravtalen på en bedre måte. Det vil være nødvendig å forsterke og forbedre rutiner mellom Sykehuset Innlandet og Sykehuspartner HF, slik at alle endringer knyttet til behandling av personopplysninger, herunder nye eksterne databehandlere, skal forelegges foretaket til godkjenning før endring iverksettes. Sykehuset Innlandet må gjøre egne vurderinger av de gjennomførte RoS-analysene på alle endringene, før eventuell godkjenning. Som tiltak vil sykehuset Innlandet forsøke å få endret eksisterende

databehandleravtale til ny standard databehandleravtale med sjekkliste som Direktoratet for e-helse har utarbeidet. Databehandleravtalen mellom Sykehuset Innlandet og Sykehuspartner skal oppdateres og har som målsetting å være signert innen 1. april 2018.

Datatilsynet tar informasjonen om databehandleravtalen til etterretning. De tiltakene som beskrives oppfattes som nødvendige for å sikre tilstrekkelig kontroll med databehandlers virksomhet og sikre etterlevelse av sykehusets databehandlingsansvar.

2.3 Drift av dagens infrastruktur

Helseforetaket viser til punkt 6.3.3 om opplysninger fremkommet i saken der vi skriver at noen av representantene fra de ulike helseforetak var bekymret som følge av risiko knyttet til å «legge driften til Bulgaria». Helseforetaket gjør oppmerksom på at den planlagte overføring av drift av dagens infrastruktur til underleverandør, var driften i hovedsak planlagt fra Norge i den første fasen og med ressurser virksomhetsoverdratt fra Sykehuspartner.

Videre vises det til foretaket i sitt brev av 15. juni 2017 viste til at Sykehuset Innlandet i avtalen med underleverandør er sikret kontroll med risikovurderingene og eventuell aksept av restrisiko ved behandling av personopplysninger utenfor Norge, jf. avtalens Appendix 1-A-6 punkt 2.1. Det påpekes at dette bidrar til å sikre helseforetaket kontroll med informasjonssikkerheten.

Vårt vedtak er basert på at det ikke er foretatt risikovurderinger i forkant av beslutningen om å tjenesteutsette IKT-drift, vedlikehold og infrastruktur. Arbeidet med risikovurderinger er en kontinuerlig prosess og må derfor også være en del av avtaleforholdet med valgt underleverandør. At det finnes vedlegg i kontrakten som sikrer foretakenes kontroll er en nødvendighet, men endrer ikke vår vurdering når det gjelder avvik fra lovens krav i forkant av avtaleinngåelsen.

I etterkant av at vi sendte vårt varsel om vedtak er vi i brev av 9. november 2017 informert om at også IKT-medarbeidere i India har hatt tilgang til pasientopplysninger i forbindelse med tjenesten OEBS fra EVRY AS. Det er opplyst at det ikke er utført risiko- og sårbarhetsvurderinger relatert til denne tjenesten og databehandleravtaler mangler. Sykehuspartner har iverksatt tiltak for å lukke avviket.

Merknadene fra helseforetaket har ingen betydning for den vurderingen som ligger til grunn for vårt varslede vedtak. Saken det informeres om i brev av 9. november 2017 viser i tillegg at denne saken ikke er enestående og at det finnes flere liknende avvik.

2.4 Tilgangskontroll

Helseforetaket viser til punkt 6.2.3 Datatilsynets vurdering/tilgangen som ble gitt til tjenesteleverandør i Bulgaria der vi har skrevet at det er uklart om opplysninger har kommet på avveie.

Sykehuset viser til at det ikke foreligger indikasjoner eller bevis på at det har vært misbruk eller forsøk på misbruk av tilgang til helseopplysninger. Konklusjonen er basert på gjennomgang av de logger som finnes. Det opplyses også at det ikke er oppdaget fravær av

tjenester og at Sykehuspartners analyseplattform har en sentral funksjon for å sikre infrastrukturen og data i Helse Sør-Øst og oppdage kompromitterende angrep i tidlig fase. Det vises til at angrep så langt har vært avverget.

Vår kommentar er at vi i senere tid har også sett at alvorlige angrep har blitt oppdaget og at det ikke finnes systemer for å avdekke hva som skjer når uvedkommende er inne i systemet.

I og med at det er uklart hvilke konsekvenser tilgangen har fått, er vårt vedtak kun basert på at det er gitt tilgang til pasientopplysninger i strid med ledelsens forutsetning om at ekstern leverandør ikke skulle ha tilgang til pasientopplysninger.

Vi viser til vår konklusjon i varsel om vedtak punkt 6.2.4 andre avsnitt og fastholder at det er gitt tilgang til pasientopplysninger i strid med ledelsens forutsetninger og dermed uten forankring i ledelsen. Dette innebærer overtredelse av personopplysningsforskriften §§ 2-11 og 2-13 til 2-15.

Helseforetakets merknad har ingen betydning for vår vurdering.

2.5 Tilsynets henvisning til helseforetakenes vurdering av krav til tidspunkt for risikovurdering

Helseforetaket viser til vårt varsel punkt 5.4 om Helseforetakenes redegjørelse, avsnitt 3 og påpeker at det er gjort et feilsitat fra foretakets brev av 15. juni. Datatilsynet har skrevet at helseforetakene legger til grunn at det ikke er et krav at risikovurderinger skal gjennomføres før behandling av personopplysninger iverksettes eller før man iverksetter endring som kan ha betydning for informasjonssikkerheten. Det vises til at foretaket i sitt brev har skrevet at «Risikovurdering må foretas før behandling av personopplysninger iverksettes eller før man iverksetter endring som kan ha betydning for informasjonssikkerheten og at dette innebærer at sykehuset skal kunne akseptere restrisiko før endringer i tjenester og drift kan gjennomføres».

Vår kommentar til detter er at vi viser til vårt varsel der vi i punkt 6.3 redegjør for hvorfor risikovurderinger må gjennomføres i forkant av beslutningen om å tjenesteutsette IKT-drift og i forkant av beslutningen om å legge driften til utlandet. Det er selve beslutningen om å tjenesteutsette som innebærer endring av betydning for informasjonssikkerhet og personvern. Det er åpenbart at man også må vurdere om nødvendige sikkerhetstiltak er på plass før man iverksetter behandling av personopplysninger i regi av databehandler, men før dette må det vurderes om tjenesteutsetting i det hele tatt kan finne sted.

Merknaden om feilsitat har ingen betydning for vår vurdering.

2.6 Styringssystem for informasjonssikkerhet og organisering av arbeidet med informasjonssikkerhet og personvern ved Sykehuset Innlandet

Sykehuset Innlandet forklarer i dette avsnittet at sykehuset har et omfattende styringssystem for informasjonssikkerhet. Vi tar dette til etterretning. Det vises også til at det gjennom databehandleravtale med Sykehuspartner er etablert et sikkerhetsrammeverk for behandling av personopplysninger på vegne av foretaket og databehandlere også har et selvstendig ansvar for å påse at behandlingen skjer i overensstemmelse med lovpålagte krav.

Datatilsynets kommentar til denne merknaden er at våre funn i denne saken ikke betyr at de enkelte helseforetakene isolert sett, eller generelt ikke har retningslinjer eller systemer som tilfredsstiller kravene i regelverket. Vårt vedtak er ikke basert på at vi har gjennomført tilsyn med helseforetakenes internkontroll og informasjonssikkerhet generelt. De avvikene som er avdekket i vår rapport er relatert til avtaleinngåelsen med DXC, det sikkerhetsfaglige arbeidet og vurderingene som ikke ble utført i forkant av beslutningen om å tjenesteutsette oppdraget, i forkant av anskaffelsesprosessen og før avtaleinngåelsen var et faktum.

Vår vurdering er basert på forhold som er avdekket fordi vi ba om en redegjørelse fra de databehandlingsansvarlige om deres rolle i prosjektet og forankringen av de beslutninger som ble tatt.

Saken har vist at det til tross for at helseforetakene har systemer for å sikre tilfredsstillende informasjonssikkerhet er åpenbart at organiseringen av prosjektet har bidratt til at gjennomføringen ikke har skjedd i samsvar med disse rutinene., Det kan også være at eksisterende rutiner for konsernovergripende prosjekter ikke har vært gode nok, eller at de ikke har vært godt nok forankret i et prosjekt i denne størrelsesorden. Resultatet er at de behandlingsansvarlige ikke har oppfylt sine plikter etter regelverket. Overtredelsene har skjedd innledningsvis, før og i forbindelse med anskaffelsesprosessen, før avtale ble inngått og før endringene ble implementert og satt i drift. Som forklart i vårt varsel er det ikke tilstrekkelig i denne type saker at det utføres risikovurderinger under vegs i prosjektet, etter at avtale er inngått.

Vi tar derfor deres kommentarer til etterretning, men ser ikke at forholdene som påpekes endrer vår vurdering.

2.7 Forberedelse til ny personvernregulering
Sykehuset Innlandet informerer om sitt arbeid med forberede overgangen til ny personopplysningslov og at Sykehuspartner fortsatt vil ha en sentral rolle i arbeidet med å sikre felles rutiner og prosedyrer i regionen, samtidig som man sikrer den enkelte databehandlingsansvarlige muligheten til å ivareta sitt ansvar etter loven. Vi tar informasjonen til etterretning.

2.8 Fremtidig tjenesteutsetting av infrastruktur i Helse Sør-Øst
Sykehuset Innlandet gjengir i dette avsnittet deler av det som er førende og gjengitt i utkast til mandat for fremtidige tjenesteutsetting av infrastruktur. Dette for å synliggjøre nødvendige endringer som vil skje fremover i slike saker.

Det skal gjennomføres en rekke aktiviteter med det formål å avdekke hvorvidt den informasjonssikkerhetsmessige- og personvernmessige risiko ved tjenesteutsetting av infrastruktur i Helse Sør-Øst er innenfor akseptabelt risikonivå. Sykehuspartner skal gjennomføre en overordnet risikovurdering av tjenesteutsetting av infrastruktur, inkludert vurdering mot sikkerhetsloven § 29 a, jf. rapport om tjenesteutsetting til privat sektor fra Direktoratet for e-helse av desember 2017. Sykehuspartner skal også fullføre nødvendig dokumentasjon av eksisterende risikonivå, som skal inngå i vurderingsgrunnlaget ved

risikovurdering av alternativene innenfor og utenfor kontrakt. Sykehuspartner skal aktivt og ofte involvere det enkelte behandlingsansvarlige helseforetak.

De behandlingsansvarlige helseforetakene skal i samarbeid med Sykehuspartner HF legge opp til tett dialog med Datatilsynet. Særlig hensynet til gjennomføring av eventuelle forhåndsdrøftelse må diskuteres. De behandlingsansvarlige helseforetakene skal etter mottak av risikovurderinger og personvernkonsekvensvurderinger aktivt vurdere og godkjenne risikovurderinger inkludert restrisiko. Vurderingene skal være et grunnlag for beslutninger om tjenesteutsetting og overdragelse av databehandleroppgaver.

I rapporten «Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten» anbefales videre utredning av utfordringer vedrørende databehandlingsansvaret som tilligger helseforetakene når føringer og beslutninger for helseforetakene, som har direkte konsekvens for databehandleransvaret, vil tas av sentrale myndigheter og Helse Sør-Øst som eier.

Informasjonen om hvordan helse Sør-Øst vil behandle saker om tjenesteutsetting i fremtiden tas til etterretning.

2.9 Vurdering av om gebyr skal ilegges og vurdering av gebyrets størrelse
Sykehuset Innlandet anfører at det foreligger formildende omstendigheter i saken som Datatilsynet bør legge vekt på i vurderingen av selve overtredelsesgebyret og gebyrets størrelse.

For det første vises det til at sykehuset har stor oppmerksomhet på informasjonssikkerhet og personvern og et omfattende styringssystem knyttet til dette. Foretaket er underlagt et regionalt system for IKT, men databehandleravtalen har betingelser som skal sikre foretaket kontroll med informasjonssikkerheten.

Datatilsynet anser det ikke som formildende at helseforetakene har gode rutiner for informasjonssikkerhet generelt, når det i denne saken så tydelig fremkommer at ledelsesforankring og sikkerhetsarbeid ikke har vært utført i samsvar med lovens krav.

Datatilsynet er klar over at helseforetakene er underlagt regional styring når det gjelder system for IKT- drift og infrastruktur. Konsekvensen av den regionale styringen er at de behandlingsansvarlige sitter med ansvaret etter personopplysningsloven, til tross for at det regionale helseforetaket er de som har tatt beslutningene i prosjektet. Etter gjeldende rett er det den databehandlingsansvarlige som er pliktsubjekt etter personopplysningsloven. Det er helseforetakene som med hjemmel i lov har behandlingsgrunnlag for å behandle pasientopplysninger.

Denne saken har vist at det er svært viktig å ha klarhet i hvilke virksomheter som er ansvarlig for etterlevelse av regelverket.

Sykehuset viser videre til at de ikke har hatt noen interesse av eller fordeler som følge av avvikene eller som motivasjon for å unnlate å følge lovpålagte krav. De viser også til at det ikke er funnet bevis for at pasientopplysninger har vært misbrukt eller kommet på avveie.

Hvorvidt foretaket har hatt eller kunne ha oppnådd fordeler ved overtredelsen viser vi til vårt varsel punkt 7.2.4 og 7.2.5. Hvorvidt det er den behandlingsansvarlige eller helseregionen som drar nytte av fordeler ved gjennomføring av felles prosjekter kan sikkert diskuteres, men objektivt sett må vi legge til grunn at det er en fordel for det enkelte foretak at store anskaffelser gjennomføres en gang fremfor at hvert helseforetak må uføre en egen anskaffelsesprosess. Ut over dette er heller ikke dette forholdet tillagt avgjørende vekt i vår vurdering.

Når det gjelder betydningen av at det ikke er dokumentert eller bevist at pasientopplysninger er kommet på avveie viser vi til punkt 2.4 over.

Når det gjelder gebyrets størrelse bemerker foretaket for ordens skyld at avtalen som ble inngått og verdien av denne gjelder for hele helseregionen og ikke bare for sykehuset Innlandet.

Når det gjelder utmåling av gebyrets størrelse viser vi til vår vurdering i varsel om vedtak kapittel 7.3.

For å understreke hvorfor vi ikke har gått langt i å vurdere om det individuelle forskjeller mellom helseforetakene og deres økonomiske bæreevne som tilsier at gebyrets størrelse bør individualiseres, viser vi til at gebyrets størrelse først og fremst har en signaleffekt. Vi legger dette til grunn fordi gebyrets samlede størrelse for helseforetakene i Helse Sør-Øst utgjør 1 promille av kontraktens verdi og om lag 0,1 promille av Helse Sør-Østs årlige omsetning.

For det enkelte foretak utgjør 800.000,- uavhengig av helseforetakets størrelse, en svært liten del av den totale omsetningen. Gebyret anses ikke å være i en størrelsesorden som påvirker det enkelte helseforetak på en måte som setter det i en vanskelig økonomisk sitasjon.

Sunnaas sykehus hadde som eksempel i 2016 en årlig omsetning på ca. 580.000.000,- og et positivt driftsresultat på 23.000.000,-. Gebyrets størrelse utgjør 1,4 promille av sykehusets omsetning og 3,5 prosent av det positive driftsresultatet.

Et annet eksempel er Oslo Universitetssykehus HF, som hadde en årlig omsetning på i overkant av 22 milliarder og et driftsresultat på ca. 285 millioner. Gebyret utgjør 0,004 promille av omsetningen til helseforetaket og 2,8 promille av driftsresultatet.

Det er derfor riktig at det er åpenbare forskjeller mellom helseforetakenes økonomiske evne, men vi kan ikke se at det er dokumentert forhold som skulle tilsi at gebyrets størrelse skal justeres ned for noen av foretakene.

Konklusjon
Vi har vurdert kommentarene fra Sykehuset Innlandet HF og tar disse til etterretning.

Vår konklusjon er at det ikke er gjort innsigelser som påvirker vår vurdering av avvik. Det er ikke kommet innspill som påvirker vår vurdering av om overtredelsesgebyr bør ilegges og vi kan heller ikke se at det foreligger omstendigheter som tilsier at gebyrets størrelse skal endres.

3. Vedtak om overtredelsesgebyr

Sykehuset Innlandet HF pålegges å betale et overtredelsesgebyr til statskassen, pålydende Kr. 800 000,- -kroner åttehundretusen- , for

1. *overtredelse av bestemmelsene i personopplysningsforskriften om sikkerhetsledelse og organisering av sikkerhetsarbeidet i virksomheten jf. §§ 2-3, 2-7 og 2-15,*
2. *brudd på krav om å gjennomføre risikovurdering ved endringer som har betydning for informasjonssikkerheten i samsvar med kravene i § 2-4 jf.2-1 pasientjournalloven § 22 samt*
3. *overtredelse av bestemmelsene om tilgangskontroll i personopplysningsforskriften §§ 2-11 og 2-13 til 2-15.*

Overtredelsesgebyret forfaller til betaling fire uker etter at vedtaket er endelig. Vedtaket er tvangsgrunnlag for utlegg. Inndrivelse av kravet vil bli gjennomført av Statens innkrevingssentral.

4. Klagemulighet

Dere kan klage på vedtaket. En eventuell klage må sendes til oss **innen tre uker** etter at dette brevet er mottatt (jf. forvaltningsloven §§ 28 og 29). Dersom vi opprettholder vårt vedtak vil vi sende saken videre til Personvernnemnda for klagebehandling.

5. Innsyn og offentlighet

Dere har rett til innsyn i sakens dokumenter (jf. forvaltningsloven § 18). Vi vil også informere dere om at alle dokumentene i utgangspunktet er offentlige (jf. offentlighetsloven § 3), men understreker samtidig at sikkerhetsdokumentasjon som hovedregel er unntatt offentlighet (jf. offentlighetsloven § 13, jf. personopplysningsloven § 45).

Med vennlig hilsen

Bjørn Erik Thon
direktør

Grete Alhaug
seniorrådgiver

Kopi til: Helse Sør-Øst RHF, Postboks 404, 2303 HAMAR
Helsetilsynet, Postboks 8128 Dep, 0032 OSLO
Sykehuspartner HF, Postboks 3562, 3007 DRAMMEN