Helseforetakenes tilgangsstyring av elektronisk pasientjournal (EPJ), jf. § 22, jf. § 19.

Er kravet til tilgangsstyring av EPJ som fremgår av pasientjournalloven § 22, jf. § 19 er tilstrekkelig innrettet på en måte som både ivaretar pasientens personvern, og gir helsepersonell den tilgangen de trenger for å yte forsvarlig helsehjelp

Kandidatnummer: 209

Antall ord: 12 768

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10.05.2019

Innholdsfortegnelse

1 Innledning

1.1 Problemstillingen og dens aktualitet

I flere år har det vært et økende fokus på personvern i helsevesenet. Etter at GDPR ble innført i norsk rett har fokuset på personvern blitt massivt, også innenfor helsetjenesten. Debatten rundt problemstillinger knyttet til pasientsikkerhet og personvern, forsvarlig helsehjelp, tilgjengelighet og tilgangsstyring av elektronisk pasientjournal i helsetjenesten, er jevnlig oppe i media med både politikere, Datatilsynet, jurister, helseforetakene og helsepersonell som deltakere.[1] Den 1. juli 2019 trer også ny pasientjournalforskrift i kraft, og i høring til forslag til pasientjournalforskriften uttaler Helse- og omsorgsdepartementet at:

> «Tilgangsstyring er viktig i arbeidet med å forvalte taushetsplikten for opplysningene i den elektroniske pasientjournalen (EPJ). God tilgangsstyring er komplisert og gir utfordringer på mange nivåer. Tilgang til helseopplysninger skal i utgangspunktet bare gis til helsepersonell i den grad det er nødvendig for å yte helsehjelp til pasienten og i den grad pasienten ikke motsetter seg det. Helsepersonell som ikke yter helsehjelp til en pasient, skal heller ikke gis tilgang til helseopplysninger om pasienten. Overholdelse av disse pliktene forutsetter ikke bare gode IKT-løsninger, men også et velfungerende styringssystem i virksomheten.»[2]

Det rettslige utgangspunktet etter pjl. § 19 er at relevante og nødvendige opplysninger skal være tilgjengelige og at det skal skje ved hensiktsmessig tilgangsstyring til EPJ etter pjl. § 22. Utfordringene består i avveining mellom at helsepersonell må ha tilgang til nødvendige opplysninger for å yte forsvarlige helsehjelp opp mot at det ikke skal gis mer tilgang enn det som er nødvendig. Oppgavens problemstilling er om kravet til tilgangsstyring av EPJ som fremgår av pasientjournalloven § 22, jf. § 19 er tilstrekkelig innrettet på en måte som både ivaretar pasientens personvern, og gir helsepersonell den tilgangen de trenger for å yte forsvarlig helsehjelp.

---

[1] https://www.op.no/nyheter/larvik-kommune/helse/bekymret-for-taushetsplikten-na-stoppes-all-elektronisk-oversendelse-av-helseopplysninger-i-larvik/s/5-36-754560
https://www.aftenposten.no/meninger/debatt/i/21O7yl/Sykehuset-ivaretar-bade-pasientsikkerhet-og-personvern--Solvi-Andersen
https://www.aftenposten.no/meninger/debatt/i/m6mEdp/Den-vanskelige-rollen-som-personvernombud--Cecilie-Ronnevik-og-Thomas-Olsen

[2] Helse- og omsorgsdepartementet: Høring: Forslag til ny forskrift om pasientjournal (pasientjournalforskriften), se s. 32

1.2 Kilder og metode

1.2.1 Lov, lovforarbeider og forskrift

Lov, lovforarbeider og forskrift er de primære rettskildene i behandlingen av oppgavens tema. Spesielt vil det være lov av 20. juni 2014 nr. 42 om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven – pjl.) §§ 19 og 22 fremstillingen tar utgangspunkt i. Videre vil lov av 2. juli 1999 nr. 64 om helsepersonell mv. (helsepersonelloven) brukes. I tillegg vil lov av 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven – popplyl.) og EUs nye personvernforordning 2016/679 vedtatt 27. april (General Data Protection Regulation – GDPR) utgjøre en sentral rettskilde. Pasientjournalloven, personopplysningsloven og GDPR vil kunne regulere de samme rettslige spørsmålene. Det fremkommer av både pjl. § 5 og popplyl § 2 første ledd, annet punktum at dersom ikke annet fremgår av særlovgivning vil personopplysningsloven og GDPR være gjeldende. I tilfeller der det oppstår kollisjon med den nasjonale lovgivningen og GDPR vil forordningen ha forrang, jf. popplyl. § 4 ledd og lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske samarbeidsområde (EØS) m.v. (EØS-loven) § 2.

Lovforarbeidene til både pasientjournalloven, personopplysningsloven og tidligere personopplysningslov vil brukes i fremstillingen. Reguleringen i helselovgivningen utgjør en videreføring av rettstilstanden som i det vesentlige samsvarte med de nye kravene som gjelder etter GDPR, og derfor vil lovforarbeidene til tidligere lovgivning ha relevans.[3][4]

Helselovgivningen legger opp til en vid bruk av forskrifter. Som følge av innføringen av personopplysningsloven og GDPR, har det skjedd endringer i tilhørende forskrifter, f. eks personopplysningsforskriften[5]. Dagens pasientjournalforskrift er på sin side ikke oppdatert opp mot det nye lovverket.[6] Dette gjør at man må være varsom med å tillegge forskriften for

[3] Dette er blant annet tilfelle ved pjl. § 22 og kravet til tilgangsstyring som er en videreføring av den tidligere personopplysningsloven § 13, jf. Prop 56 LS (2017-2018) s. 232.
[4] Forvaltningslovutvalget overleverte sin utredning av ny forvaltningslov til Justis- og beredskapsdepartementet, NOU 2019:5, 14. mars 2019. Utredningen vil imidlertid ikke i nevneverdig grad bidra til å løse den aktuelle problemstillingen.
[5] Forskrift av 15. juni 2018 nr. 876 om behandling av personopplysninger
[6] Forskrift av 20. desember 2000 nr. 1385 om pasientjournal

mye vekt når innholdet av en rettsregel skal tolkes i fremstillingen. Den 1. mars 2019 ble ny pasientjournalforskrift vedtatt, og vil tre i kraft fra og med 1. juni 2019.[7]

1.2.2 Forvaltningspraksis

For å illustrere hvordan tilsynsmyndighetene og helseforetakene forstår og praktiserer regelverket, skal det brukes avgjørelser fra Statens helsetilsyn, Datatilsynet og Personvernnemnda.[8] Jeg har begjært innsyn i saker hos Statens Helsetilsyn vedrørende helsepersonelloven § 21a, som gjelder helsepersonells urettmessige tilegnelse av taushetsbelagte opplysninger i tidsrommet 2014-2018. De har hatt 55 tilsynssaker, hvor det er begått lovbrudd etter § 21a i 48 av dem, 24 i helseforetak.[9] Jeg har videre bedt om innsyn i avgjørelser fattet etter pjl. §§ 19 og 22 hos Datatilsynet. Hos Statens helsetilsyn har jeg bedt om innsyn i tilsynssaker knyttet til sphl. § 3-2, hvor det ofte inngår en vurdering etter både pjl. §§ 19 og 22. Fra Statens helsetilsyn fikk jeg utlevert til sammen åtte saker, og Datatilsynet henviste meg til deres hjemmesider.[10] Sakene kan være egnet til å vise hvilke utfordringer som dukker opp i forbindelse med tilgangsstyring til EPJ i praksis. Sakene vil for øvrig kunne bidra til å belyse viktige problemstillinger når gjeldende rett skal klarlegges. I fremstillingen er det først og fremst sakene fra Statens helsetilsyn og Datatilsynet som brukes.

Hvor mye vekt skal forvaltningspraksis tillegges?

Høyesterett har anerkjent forvaltningspraksis som en relevant rettskilde. Dette var f. eks tilfelle i Rt. 1997 s. 527 hvor lov og forarbeider ga liten veiledning. Det ble derfor utslagsgivende at «dels enkelte reelle hensyn, *dels sentrale myndigheters praksis* og i lys av denne praksis – nyere lovgivning» (uthevet her).[11] Videre ble det uttalt om den aktuelle

[7] Forskrift av 3. mars 2019 nr. 168 om pasientjournal (pasientjournalforskriften)
[8] Statens helsetilsyn er underlagt Helse- og omsorgsdepartementet, og er den sentrale tilsynsmyndigheten for blant annet helse- og omsorgstjenesten. Deres oppgave, sammen med Fylkesmannen, er å drive tilsyn og kontroll med hjemmel i lov av 30. mars 1984 nr. 15 om statlig tilsyn med helse- og omsorgstjenesten mm. (tilsynsloven) Datatilsynet er underlagt kommunal- og moderniseringsdepartementet, og fungerer som både tilsyn og ombud. Deres oppgaver består i å føre kontroll med at personvernregelverket etterleves og medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem, se https://www.datatilsynet.no/om-datatilsynet/oppgaver/. Datatilsynet kan etter kapittel 5 i pasientjournalloven utføre tilsyn og gi sanksjoner, f. eks gi overtredelsesgebyr. Personvernnemnda skal behandle klager på vedtak som er fattet av Datatilsynet i medhold av personopplysningsloven og andre lover, f. eks. helsepersonelloven og forvaltningsloven.
[9] Av disse gjelder 23 saker ulovlige oppslag i EPJ.
[10] Datatilsynet: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/, sist sjekket 09.05.19
[11] Rt. 1997 s. 529, på s. 532

praksis, blant annet fra Statens helsetilsyn, at «statlige myndigheters praksis på vanlig vis må komme inn som en rettskildefaktor».[12]

Spørsmålet er hvilken vekt forvaltningspraksis skal tillegges der den kolliderer med andre rettskilder, f. eks lov, uttalelser i forarbeider, reelle hensyn og juridisk teori.

Det er klart at forvaltningspraksis vil tillegges mindre rettskildemessig vekt enn lov, forarbeider og forskrift. Hvis det oppstår et kollisjonstilfelle der forvaltningspraksis taler for et annet resultat enn både lov og forarbeider, vil sistnevnte klart gå foran. Et eksempel på dette er blant annet Høyesterettsdom inntatt i Rt. 2006 s. 1601. Høyesterett kom enstemmig frem til at «entydig ligningspraksis» ikke kunne forhindre at den riktige lovforståelsen etter «[l]ovteksten sett i sammenheng med […] lovhistorien» måtte legges til grunn.[13] Et annet moment av betydning for vurderingen av de aktuelle rettskildene, var at den riktige lovforståelsen var til gunst for skatteyteren. Så lenge det ikke er tale om forvaltningsskjønn, vil Høyesterett ha det siste ordet i rettsanvendelsen.[14]

Per dags dato er det ikke avsagt noen dom i norsk rett vedrørende tilgangsstyring til EPJ. Dette gjør at avgjørelser fra forvaltningspraksis vedrørende spørsmål om tilgangsstyring til EPJ vil kunne være førende for hvordan regelverket skal forstås. Det må imidlertid tas hensyn til sakens faktum og dens særpreg. Likevel vil generelle uttalelser om hvordan lovverket skal forstås kunne være av prinsipiell betydning for forvaltningen, og gi veiledning. Dersom det skulle oppstå konflikt mellom innholdet i forvaltningspraksis og reelle hensyn, vil det være sentralt å se hvilket utfall som er til gunst for borgeren. Et annet moment vil være å se om avgjørelsen fra den aktuelle saken er et resultat av langvarig og ensartet forvaltningspraksis, og det vil med hensyn til likebehandling være hensiktsmessig at forvaltningspraksis går foran innholdet av et annet reelt hensyn. Når det gjelder juridisk teori vil vurderingen være tilnærmet lik, men et moment av betydning for vurderingen, er hvor mange som stiller seg bak den aktuelle oppfatningen, og hvordan den stiller seg til andre rettskilder som lov og forarbeider.

[12] Rt. 1997 s. 529, på s. 533
[13] Rt. 2006 s. 1601, avsnitt 31
[14] Grunnloven § 88

Jeg har videre fått god hjelp, innblikk i praktiske problemstillinger og bidrag til oppgaveskrivingen av jurister som jobber i helseforetak i Helse Sør-Øst RHF.

1.2.3 Norm for informasjonssikkerhet

Norm for informasjonssikkerhet (heretter Normen) i helse- og omsorgstjenesten er det en kaller en atferdsnorm. Normen består av faktaark og veiledere med et omforent sett med krav til informasjonssikkerhet basert på lovverket. Siste utgave av Normen, versjon 5.3 ble utgitt 20. juli 2018, etter at ny personopplysningslov og GDPR trådte i kraft. Den nye versjonen var det første skrittet i et omfattende utviklings- og tilpasningsarbeid som blant annet skal sikre at Normen samsvarer med det nye lovverket. Normen er utarbeidet av representanter fra helse-, omsorg og sosialsektoren, forvaltes av Styringsgruppen for Norm for informasjonssikkerhet og er utgitt med støtte fra Direktoratet for e-helse.[15] Styringsgruppen er et bransjeorgan som består av representanter fra blant annet helseforetakene, Helsedirektoratet og Den norske legeforening. Helse- og omsorgsdepartementet, Datatilsynet og Difi[16] opptrer i styringsgruppen som observatører og veiledere.

I GDPR art. 40 nr. 1 er det fastslått at medlemsstatene og tilsynsmyndighetene skal «oppmuntre til at det utarbeides atferdsnormer som skal bidra til riktig anvendelse av denne forordning». Ved utarbeidelse av atferdsnormene skal det tas hensyn til særpreget den aktuelle sektoren man befinner seg på, og den ferdige atferdsnormen skal godkjennes av tilsynsmyndigheten som har kompetanse etter GDPR art 40 nr. 5, jf. art 55 nr. 1. Datatilsynet som er tilsynsmyndighet, jf. popplyl § 20[17] har enda ikke gjort en slik godkjenning og Normen er derfor i dag ikke formelt en atferdsnorm etter art. 40 nr. 1. Dette skyldes at

[15] Direktoratet for e-helse er et fag- og myndighetsorgan underlagt Helse- og omsorgsdepartementet. Direktoratets to hovedoppgaver er å sørge for nasjonal styring og koordinering i samarbeid med blant annet helseforetak, samt å realisere og forvalte digitale løsninger som forbedrer og forenkler helse- og omsorgssektoren, se https://ehelse.no/om-oss/om-direktoratet-for-e-helse.

[16] Direktoratet for forvaltning og IKT (Difi): Difi har som samfunnsoppdrag å modernisere og omstille offentlig sektor. Difi er et fagorgang for Kommunal- og moderniseringsdepartementet og Nærings- og fiskeridepartementet innen fagområdene ledelse, organisering, offentlige anskaffelser og digitalisering i offentlig sektor. Difis strategiske satsningsområder er effektivisering, brukerorientering og samordning av offentlig sektor.

[17] Se også GDPR art. 4 nr. 21 og 22, samt fortalens punkt 20, 36 og 91.

European Data Protection Board (EDPB)[18] har levert forslag til retningslinjer for hvordan atferdsnormer skal godkjennes, på høring. Datatilsynet ønsker derfor ikke å godkjenne foreliggende atferdsnormer før disse er vedtatt.[19]

Spørsmålet blir med det hvor mye vekt Normen skal tillegges som rettskilde.

Et argument mot at den skal tillegges vekt er at den ikke innehar den demokratiske legitimiteten etter GDPR art. 40, ettersom den ikke er godkjent av Datatilsynet. På den andre side bidrar Normen til særkunnskap og detaljer om informasjonssikkerhet innenfor helsetjenesten. Normen benyttes videre i helsetjenesten for å skape likhet, og den anses derfor å gi uttrykk for hvordan forvaltningen selv forstår lovverket. Bruk av Normen skal også bidra til effektivisering i helsetjenesten. Det fremgår av normen at alle kravene er i tråd med GDPR.[20] Kravene i Normen vil imidlertid ikke selvstendig fungere som rettslig grunnlag for å iverksette tiltak for å ivareta informasjonssikkerhet, som f. eks tilgangsstyring og har derfor begrenset rettskildemessig vekt. De vil på den annen side kunne bidra til å klarlegge å supplere innholdet av den aktuelle regelen, og illustrere/gi eksempler på hvordan den skal brukes i praksis.

1.2.4 Grunnleggende prinsipper

Innenfor helseretten og personvern er det en rekke grunnleggende prinsipper. De prinsippene som spesielt gjør seg gjeldende for oppgavens tema er forsvarlighetskravet, taushetsplikten og personvernprinsippene. Disse vil løpende trekkes inn underveis i vurderingen.

1.2.5 Juridisk litteratur

Tilgangsstyring er omtalt i kommentarutgaver til både pasientjournalloven og helsepersonelloven. Det er også et svært aktuelt tema i fagbøker knyttet til innføringen av GDPR. Disse vil det gjennomgående vises til gjennom oppgaven.

[18] Rådgivende organ for EU-kommisjonen i personvernspørsmål. Tidligere kalt Artikkel 29-gruppen.

[19] Datatilsynet: https://www.datatilsynet.no/regelverk-og-verktoy/atferdsnorm/

[20] Direktoratet for e-helse: https://ehelse.no/Documents/Normen/Publisering/Normen%205.3.pdf s. 9

1.3 Begrepsavklaringer

Før det foretas en drøftelse av innholdet i pjl. § 22 skal det gis en kort deskriptiv beskrivelse av de mest relevante begrepene innenfor oppgavens tema, og de vil utdypes senere i oppgaven.

Informasjonssikkerhet handler om tilstrekkelig og balansert sikring av konfidensialitet, integritet og tilgjengelighet på informasjon i en virksomhets informasjonsbehandling. Dette er ingen statisk tilstand, trusler og risiko endres både raskt og over tid, og tiltak må systematisk tilpasses i takt med utviklingen.[21]

Tilgangsstyring eller *tilgangskontroll* er «regler for å styre hvem som skal ha tilgang til hvilke opplysninger eller systemer.» [22]

Elektronisk pasientjournal (EPJ) er en elektronisk samling av registrerte opplysninger om en pasient i forbindelse med helsehjelp.[23] Formkrav og krav til innholdet i EPJ fremkommer av helsepersonelloven § 40 og ny pasientjournalforskrift § 3. EPJ er videre et arbeidsverktøy for helsepersonell i tilknytning til at helsehjelp gis. Den skal gi oversikt over hvilke tiltak som er iverksatt, observasjoner og vurderinger, og bidra til kommunikasjon mellom helsepersonell.[24]

Helseopplysninger er definert i GDPR art. 4 nr. 15 som «personopplysninger om en fysisk persons fysiske eller psykiske helse, herunder om ytelse av helsetjenester som gir informasjon om vedkommendes helsetilstand». Dette kan for eksempel være legemiddelliste, en epikrise fra et opphold på sykehus eller en diagnose. Helseopplysninger kan være av svært sensitiv karakter, og at det er inntatt en egen kategori skilt fra personopplysninger i GDPR understreker hvilken særstilling helseopplysninger står i med hensyn til personvern.

1.4 Avgrensninger

[21] Difi: https://internkontroll-infosikkerhet.difi.no/ledelsens-gjennomgang/hvorfor-internkontroll-pa-informasjonssikkerhetsomradet

[22] Datatilsynet: https://www.datatilsynet.no/regelverk-og-verktoy/verktoy/ordbok-a-til-a/#D

[23] Direktorat for e-helse: https://ehelse.no/standarder-kodeverk-og-referansekatalog/elektronisk-pasientjournal-epj#informasjonskategorier-og-styring-av-tilgang-til-journalopplysninger

[24] Prop 91 L (2010-2011) s. 95

Oppgaven er ikke ment å være en uttømmende fremstilling om tilgangsstyring til EPJ, men vil ha fokus på tilgangsstyring til EPJ knyttet til helsepersonell som arbeider i helseforetak. Helseforetakene er som virksomheter forpliktet etter spesialisthelsetjenesteloven (sphl.) § 3-2 til å sørge for at de journal- og informasjonssystemene som brukes, er forsvarlige. Videre er helseforetaket også forpliktet til å påse at ansatte overholder sine lovpålagte plikter, jf. spesialisthelsetjenesteloven § 2-2. Sentrale bestemmelser i vurderingen av om helseforetaket har overholdt sine forpliktelser etter sphl. §§ 3-2, er pjl. §§ 19 og 22.

Det trer som nevnt i punkt 1.2.1 i kraft en ny pasientjournalforskrift 1. juni. I fremstillingen er det fokus på denne fremfor den utgående forskriften fra 2000.

1.5 Oppgavens oppbygning

Oppgaven består av totalt fem deler. Etter de innledende kapittel 1, redegjør kapittel 2 for det rettslige utgangspunktet om tilgang til helseopplysninger ved helsehjelp etter pjl. § 19, og deretter klarlegges innholdet i pjl. § 22. Kapittel 3 går nærmere inn på kravet til tilgangsstyring. Kapittel 4 beskriver sentrale og dagsaktuelle utfordringer knyttet til tilgangsstyring. I oppgavens siste del, kapittel 5 og 6 foretar jeg en de lege ferenda drøftelse og jeg kommer med noen avsluttende refleksjoner.

2 Pasientjournalloven § 19

2.1 Bakgrunn og presentasjon

Pasientjournalloven ble innført den 1. januar 2015. I lovforarbeidene er det uttalt at formålet med innføringen av pasientjournalloven er en modernisering som tar sikte på å bedre helse- og omsorgstjenester til pasientene og brukerne, og at den nye loven skulle tilpasses dagens informasjonsbehov ved samhandling og koordinering av helsehjelp til den enkelte pasient.[25] Den enorme teknologiske utviklingen de siste årene er trukket frem flere ganger av departementet, og blant annet pekes det på at denne utviklingen har skapt et behov og forventning i befolkningen til informasjonsutvikling og tilgang til egne helseopplysninger. Da den nye pasientjournalloven ble innført i 2015, kom begrepet «tilgangsstyring» for første gang uttrykkelig inn i lovteksten ved pjl. § 22. Frem til da var det slik at tilgangsstyring var innfortolket i kravet om informasjonssikkerhet i den tidligere helseregisterloven.[26] Den europeiske menneskerettighetsdomstolen har også i sak no. 20511/3, avsagt 17. juli 2008, konkludert med at krav til informasjonssikkerhet skal inkluderes i EMK art. 8 om retten til privatliv. Saksøkeren var en pasient som anla sak mot et sykehus eid av den finske staten. Samtidig som en sykepleier arbeidet på et sykehus gikk hun til behandling på en poliklinikk for smittsomme sykdommer ved det samme sykehuset, etter å ha fått diagnosen som hiv-positiv. På bakgrunn av kommentarer hun fikk fra kolleger ved sykehuset, mente hun at de urettmessig hadde lest i hennes pasientjournal. Det var av hennes oppfatning at sykehuset ikke hadde gjort tilstrekkelig for å sikre mot urettmessige oppslag i pasientjournaler og anla derfor sak for EMD. EMD kom i denne saken enstemmig frem til at det forelå brudd på EMK art. 8.[27]

Våren 2018 ble det foretatt endringer i ordlyden til pjl. § 22 som følge av innføringen av den nye personopplysningsloven og GDPR, og etter bestemmelsen følger det nå at:

> «Den dataansvarlige og databehandleren skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. personvernforordningen

[25] Prop. 72 L (2013-2014) s. 15

[26] Prop. 72 L (2013-2014) s. 184

[27] EMD sak 20511/3 avsnitt 38-40

> artikkel 32. Den dataansvarlige og databehandleren skal blant annet sørge for tilgangsstyring, logging og etterfølgende kontroll.
>
> Departementet kan i forskrift fastsette nærmere krav til informasjonssikkerhet ved behandling av helseopplysninger»

2.2 Forholdet mellom tilgangsstyring og taushetsplikten

Helseopplysningene som er i EPJ, er underlagt taushetsplikt, jf. § 19. Tilgangsstyring er et arbeidsverktøy som benyttes for å forvalte denne taushetsplikten. Før man tar stilling til kravet om tilgangsstyring i EPJ, er det derfor hensiktsmessig å gjøre rede for bestemmelsen i § 19 om helseopplysninger ved helsehjelp. I Befring m.fl. legges det til grunn at «taushetsplikten danner grunnlag for såkalt tilgangskontroll til helseopplysninger i en helsevirksomhet.» [28] Tilsvarende oppfatning er lagt til grunn av Statens helsetilsyn i sak 2016/1808.[29] Det følger av pjl. § 19 første ledd:

> «Innenfor rammen av taushetsplikten skal den dataansvarlige sørge for at relevante og nødvendige helseopplysninger er tilgjengelig for at helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte»

En alminnelig forståelse av «innenfor rammen av taushetsplikten» tilsier at helsepersonell kun skal få tilgang til helseopplysninger dersom det er i samsvar med taushetsplikten. Ordlyden innebærer med andre ord en anvisning på regler om taushetsplikt. En slik forståelse av ordlyden legges også til grunn i lovforarbeidene, hvor det fremgår at regelen skal ses i sammenheng med helsepersonells regler om taushetsplikt. [30] Det er med andre ord lagt opp til samspill mellom reglene i pjl. og hlp.

Helsepersonellovens regler om taushetsplikt følger av hlp §§ 21 til 38a, jf. pasient- og brukerrettighetsloven § 3-6, og hlp. § 45. De relevante bestemmelsene knyttet til tilgangsstyring i EPJ og oppgavens problemstilling er hlp. §§ 21, 21a, 25 og 45, og vil kort

[28] Befring og Ohnstad (2018) s. 260.

[29] Statens helsetilsyn sak 2016/1808 dokument 74, 11. juni 2017 s. 5-6.

[30] Prop. 72 L (2013-2014) s. 182

omtales i det følgende. Den mest sentrale bestemmelsen er hovedregelen om taushetsplikt som følger av hlp. § 21:

> «Helsepersonell skal hindre at andre får adgang eller kjennskap til opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold som de får vite i egenskap av å være helsepersonell»

Formålet med taushetsplikten er «å verne pasientenes integritet og sikre befolkningens tillit til helsetjenesten og helsepersonell» og å «hindre at pasienter unnlater å oppsøke helsetjenesten ved behov for helsehjelp». Med andre ord kan tillit til helsepersonell og helsetjenesten være avgjørende for at befolkningen faktisk oppsøker helsehjelp og gir helsepersonell nødvendig informasjon. Den skal sørge for at pasienter «skal føle seg trygg på at opplysninger som gis i forbindelse med helsehjelp ikke nyttes i andre sammenhenger». Av de samme forarbeidene følger det at taushetsplikten også omfattes av integritetsvernet for pasienter i forbindelse med helsehjelp. [31] Med det menes at respekten for enkeltindividets personlige integritet, herunder deres interesse av å ikke få sin anseelse forringet er et bærende motiv i de overveielser som ligger til grunn for bestemmelsene om taushetsplikt og dens grenser. [32] Personvernet er med andre ord også et grunnleggende formål bak helsepersonells taushetsplikt.[33]

Videre gir ordlyden «skal hindre» uttrykk for helsepersonells aktivitetsplikt. I forarbeidene forklares aktivitetsplikten som følgende:

> «taushetsplikten er ikke bare en passiv plikt til å tie, men også en aktiv plikt til å hindre uvedkommende i å få tilgang til taushetsbelagt informasjon. Forsvarlig håndtering og oppbevaring av pasientopplysninger er en forutsetning for å etterleve den lovbestemte taushetsplikten.»[34]

Forarbeidsuttalelsen vedrørende aktivitetsplikten ble vektlagt i dom fra Høyesterett inntatt i Rt. 2013 s. 1442, hvor en lege hadde gnidd en pose som inneholdt narkotika på hendene for å kunne overholde taushetsplikten.

[31] Ot.prp.nr 13 (1998-1999) s. 227

[32] Befring m.fl. (2015) s. 137

[33] Ibid s. 136

[34] Rt. 2013 s. 1442 avsnitt 22

Helsepersonelloven § 21a

For å styrke taushetsplikten ble det i 2008 inntatt en regel om forbud mot urettmessig tilegnelse av taushetsbelagte opplysninger i pjl. § 21a:

> «Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte opplysninger som nevnt i § 21 uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift.»

Etter lovforarbeidene er bestemmelsen ment å styrke vernet om taushetsbelagte helseopplysninger, og hindre snoking i EPJ. [35] Bestemmelsen har det samme formålet og verner de samme interessene som hovedregelen i § 21. Etter ordlyden synes terskelen for å begå brudd på pjl. § 21a å være lavere, ettersom det etter pjl. § 21 kreves at den taushetsbelagte informasjonen også videreformidles. I sak fra Statens helsetilsyn er det uttalt at taushetsplikten i utgangspunktet ikke skal være til hinder for at kollegaer skal kunne drøfte faglige spørsmål seg imellom, og derfor ikke et brudd på hlp. § 21. Men når legen hadde tilegnet seg informasjon fra andre avdelinger ved helseforetaket i EPJ i strid med hlp. 21a, måtte det anses som et brudd på taushetsplikten etter hlp. § 21.[36]

Det er videre i de samme lovforarbeidene forklart at regelen innebærer at helsepersonell ikke har tillatelse til å lese i journalen til en pasient uten at det kan begrunnes med helsehjelp til pasienten. Dette betyr at helsepersonell ikke uten videre kan lese i journalen til en pasient de tidligere har hatt ansvar for å behandle, for eksempel i læringsøyemed. Dersom man likevel skal gis tilgang til journalen må det foreligge hjemmel i lov, ved for eksempel hlp. § 22 om samtykke og § 26 om opplysninger til virksomhetens ledelse og til administrative systemer.

Høyesterett kom i dom inntatt i HR-2018-2452-A med generelle uttalelser om bestemmelsen i hlp. § 21a. En professor, og tidligere overlege hadde gjort oppslag i EPJ-system ved sykehuset han tidligere var ansatt på, men fortsatt i rollen som professor hadde kontor på sykehuset. Helseopplysningene ble innhentet uten at det var gitt samtykke fra pasienten, som han heller ikke hadde hatt behandlingsansvar for tidligere. Oppslaget var gjort for å innhente opplysninger til sak han var engasjert som privat sakkyndig for et forsikringsselskap. Høyesterett kom enstemmig frem til at det forelå overtredelse av helsepersonelloven § 67, jf.

[35] Ot.prp.nr 25 (2007-2008) s. 69

[36] Statens helsetilsyn sak. 2016/1808 dokument 55, 14. juni 2017 s. 7

§ 21a. Det ble lagt avgjørende vekt på at det var tale om tungtveiende verdier og interesser som ligger til grunn for taushetsplikten, herunder taushetspliktens vern av pasienters integritet og tilliten til helsepersonell og helsetjenesten.[37] Selv om det ikke var tale om et oppslag der hensikten anses å ha vært «snoking», var interessene som ble krenket i kjernen av det bestemmelsen er ment å verne om.

Helsepersonelloven §§ 25 og 45

I hlp. §§ 25 og 45 reguleres kommunikasjon av pasientopplysninger mellom helsepersonell ved samarbeid om en pasient. Bestemmelsene utgjør et unntak fra hovedregelen om taushetsplikt i hlp. § 21, i og med at taushetsplikten også gjelder mellom helsepersonell.

Det følger av hlp. § 25 første ledd at «med mindre pasienten motsetter seg det, kan taushetsbelagte opplysninger gis til samarbeidende personell når dette er nødvendig for å gi forsvarlig helsehjelp.» Tilsvarende regel for deling av helseopplysninger i EPJ fremgår av hlp. § 45 første ledd, første punktum hvor det fremgår at:

> «Med mindre pasienten motsetter seg det, skal helsepersonell som skal yte eller yter helsehjelp til en pasient etter denne lov, gis nødvendige og relevante opplysninger i den grad dette er nødvendig for å kunne gi forsvarlig helsehjelp til pasienten på forsvarlig måte. Det skal fremgå av journalen at annet helsepersonell er gitt opplysninger»

I lovforarbeidene uttales det at begrunnelsen for regelen i hlp. § 25 er «å ivareta pasientens behov for oppfølgning og for å bidra til forsvarlige, rasjonelle og hensiktsmessige forhold i helsetjenesten.»[38] Befring og Ohnstad legger videre til grunn at det ikke vil være nødvendig å be pasienten om samtykke med mindre helsepersonell «har grunn til å være i tvil om pasienten ønsket slik informasjonsutveksling.» Herunder trekkes situasjoner der det dreier seg om særskilt sensitiv informasjon om pasienten, eller om det av andre grunner er tvil om hvorvidt pasienten vil gi sitt samtykke til informasjonsutveksling.[39]

Helsepersonell skal videre kun gis tilgang til «relevante og nødvendige helseopplysninger». En alminnelig forståelse av ordlyden i vilkåret tilsier at de helseopplysningene som gjøres

[37] HR-2018-2452-A avsnitt 23

[38] Ot.prpr.nr 13 (1998-1999) s. 229

[39] Befring/Ohnstad (2018) s. 185

tilgjengelig for helsepersonell, må være en forutsetning for at den aktuelle helsehjelpen kan ytes.

Formuleringen «relevante og nødvendige helseopplysninger» er også brukt i hlp. § 40 om helsepersonells dokumentasjonsplikt som regulerer krav til innholdet av EPJ. I bestemmelsens forarbeider er det presisert at det med «relevante og nødvendige helseopplysninger» siktes til opplysninger i den aktuelle undersøkelses- eller behandlingssituasjonen som det er behov for å ha tilgjengelig for at helsepersonell skal kunne gjennomføre den. [40] Det følger av forarbeidene til pjl. § 19 at den samme forståelsen av vilkåret skal legges til grunn i pasientjournalloven.

Vilkåret blir i forarbeidene formulert som et krav til at helsepersonell må ha et «tjenstlig behov» for å få tilgang til helseopplysninger.[41] I flere tilsynssaker fra Statens Helsetilsyn har vurderingstemaet vært om helsepersonell uten tjenstlig behov, og i strid med hlp. § 21a, har gjort oppslag i EPJ.[42] Engelschiøn og Vigerust beskriver tjenstlig behov som at bare de helseopplysningene helsepersonell trenger for å yte forsvarlig helsehjelp, skal gjøres tilgjengelige, og de må også være nødvendig for at helsepersonell skal kunne utføre arbeidet. I den forbindelse trekker de også frem at det må foreligge en pasientrelasjon mellom helsepersonellet og den aktuelle pasienten. [43] Befring og Ohnstad viser til at det må foretas en konkret vurdering av hvilke opplysninger som på noe tidspunkt kan ha betydning for pasienten eller pasientbehandlingen. [44]

En alminnelig forståelse av ordlyden «tilgjengelige» tilsier at helseopplysningene må kunne søkes opp i EPJ f. eks i helseforetakene, eller for øvrig er oppbevart på en måte som gjør at helsepersonell faktisk har en mulighet til å hente dem fram og bruke dem når det er behov. Lovforarbeidene viser til at «tilgjengelige» både omfatter tilgang til helseopplysninger, ved at personell gis adgang til å søke opp de aktuelle helseopplysningene i systemet, og at opplysningene gjøres tilgjengelige ved at de utleveres og er tilgjengelige når det er behov.[45]

[40] Ot.prp.nr 14 (2000-2001) s. 51

[41] Prop. 72 L (2013-2014) s. 90

[42] Dette var tilfelle i Statens helsetilsyn sak 2015/1502 dokument 3 og sak 2017/1783 dokument 13.

[43] Engelschiøn og Vigerust (2015) s. 94

[44] Befring og Ohnstad (2018) s. 256

[45] Prop. 72 L (2013-2014) s. 59

Dette er svært viktig del av informasjonssikkerheten ettersom godt tilrettelagt tilgjengelighet er en forutsetning for å kunne yte forsvarlig helsehjelp.

Oppsummert må helsepersonell foreta vurdering av om de har et tjenstlig behov som kan gi dem tilgang til helseopplysningene, og vurdere konkret hvilke helseopplysninger som er nødvendig å få innsyn i, for at de skal kunne yte forsvarlig helsehjelp.[46] Etter bestemmelsen er det da også en forutsetning at helseforetaket sørger for løsninger som gjør at helseopplysningene er tilgjengelige i samsvar med det tjenstlige behovet, og dette vil da vurderes i neste kapittel om tilgangsstyring.

[46] Kravet til forsvarlig helsehjelp fremgår av hlp. § 4 og sphl. § 2-2

3 Pasientjournalloven § 22

3.1 Utgangspunktet etter ordlyden

3.1.1 Tilgangsstyring

Kravet til tilgangsstyring følger av pjl. § 22 første ledd, andre punktum jf. første punktum, hvor det fremgår at «dataansvarlig og databehandler» skal «sørge for *tilgangsstyring*, logging og etterfølgende kontroll» (uthevet her).

Ordlyden av «tilgangsstyring» tilsier at helseforetaket skal gjennomføre kontrolltiltak som både ivaretar taushetsplikten i EPJ, og samtidig gir helsepersonell den tilgangen de trenger for å yte helsehjelp. Det er brukt en vid ordlyd i utformingen av kravet til tilgangsstyring, og den er taus om hva dataansvarlig og databehandler faktisk må foreta seg. Utgangspunktet etter ordlyden er derfor at det er opp til helseforetakene selv å finne løsninger som gir forsvarlig tilgangsstyring. Dette krever at innholdet i bestemmelsens krav om tilgangsstyring i stor grad må fastlegges nærmere gjennom tolkning i lys av andre rettskilder.

Vigerust og Engelschiøn trekker frem at det mest effektive virkemiddelet for å motvirke uberettiget innsyn er god tilgangsstyring, og videre at formålet med tilgangsstyring i størst grad er å begrense mulighetene for urettmessig tilegnelse og endring av opplysninger.[47] I Normen påpekes det at tilgang skal styres slik at reglene om taushetsplikt ivaretas og tilgang til helse- og personopplysninger ikke gis til andre enn de som har tjenstlig behov.[48]

3.1.2 Dataansvarlig og databehandler

Det må også avklares hva som menes med «dataansvarlig og databehandler», jf. pj. § 22 første ledd, første punktum. Det fremkommer av pjl. § 2 bokstav e og GDPR art. 4 nr 7 at en «dataansvarlig» er:

> «En fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ, som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for

[47] Vigerust/Engelschiøn (2015) s. 113
[48] Direktorat for e-helse: Normen s. 29

> behandling er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriterier for utpeking av vedkommende, fastsettes i unionsretten eller medlemsstatenes nasjonale rett.»

Denne definisjonen er en videreføring av innholdet i EU sitt tidligere personverndirektivet, der hensikten med å ha en behandlingsansvarlig var å allokere hvem som skulle ha ansvaret for å sørge for at personopplysningene ble behandlet etter loven.[49] I lovforarbeidene til den nye personopplysningsloven er det også lagt til grunn at ansvaret for personvern ligger hos den dataansvarlige.[50] Når det gjelder behandling av helseopplysninger i EPJ er det leder av virksomheten, i denne fremstillingen administrerende direktør i helseforetaket, som er dataansvarlig. I lovforarbeidene til den nye pasientjournalforskriften fremgår det at sentrale plikter for den dataansvarlige er:

> «…blant annet å sørge for at all behandling av helseopplysninger er i tråd med lover, forskrifter og eventuelle godkjenninger og sørge for tilfredsstillende informasjonssikkerhet blant annet innbygd personvern.»[51]

Tett sammen med dataansvarlig henger rollen som «databehandler». I pjl. § 2 bokstav d og GDPR art. 4 nr. 7 er databehandler:

> «En fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.»

I GDPR bruker man behandlingsansvarlig. I pasientjournalloven og personopplysningsloven har man imidlertid ønsket å forenkle ordbruken, og valgt å bruke dataansvarlig i stedet for behandlingsansvarlig.[52] Dataansvarlig har instruksjonsmyndighet over databehandleren, og samarbeidet etableres gjennom databehandlingsavtaler. Dette er en avtale mellom databehandler og behandlingsansvarlig om setter opp rammene for hvordan

---

[49] Artikkel 29-gruppen, Opinion 1/2010 on the concept of «controller» and «processor», Adopted on 16 february 2010, WP s. 5.

[50] Dette ble også lagt av Personvernnemnda i sak PVN-2015-07 (Tromsø kommune) pkt. 5.1

[51] Helse- og omsorgsdepartementet: Høring: Forslag til ny forskrift om pasientjournal (pasientjournalforskriften), se s. 13
https://www.regjeringen.no/contentassets/bc66ebd8e7714bf6b0f3753e7c1dcdca/hoerings_pasientjournalforskriften.pdf, sist sjekket 9. mai 2019

[52] Prop. 56 LS (2017-2018) s. 184

personopplysninger skal behandles.[53] Kravene til innholdet av databehandleravtale fremgår av GDPR art. 28.

3.2 Hvordan skal tilgangsstyring gjennomføres?

3.2.1 De ulike verktøyene for tilgangsstyring

I lovforarbeidene er hensikten med tilgangsstyring at det skal fungere som et verktøy for å begrense urettmessig tilegnelse og endring av de opplysningene som fremgår av EPJ. For å operere med tilgangsstyring som et slikt verktøy, må dataansvarlig på bakgrunn av en risikovurdering av trusler mot urettmessig tilegnelse og endring, etablere et system for tilgangsstyring.[54] Et system for tilgangsstyring skal blant annet være egnet til å kontrollere hvem som har behandlet helseopplysninger, og med hvilket formål tilgangen er gitt. Logging fremheves som et sentralt hjelpemiddel i et slikt system. De samme forarbeidene lister opp en rekke andre hjelpemidler som anses å være en forutsetning for god tilgangsstyring, i tillegg til logg. Dette er autorisasjon, autentisering og selvbestemmelse med begrunnelse for oppslaget. [55] I den nye pasientjournalforskriften § 13 inntatt en egen bestemmelse om tilgangsstyring. Denne inneholder presiseringer knyttet til autentisering og autorisering. Videre er det inntatt regler om loggføring i pasientjournalforskriften § 14.

Disse hjelpemidlene og hvilke krav som stilles til helseforetaket i sammenheng med dem, er også nøye beskrevet i Normen.

[53] Datatilsynet: https://www.datatilsynet.no/regelverk-og-verktoy/verktoy/ordbok-a-til-a/#D, sist sjekket 09.05.19.

[54] Jf. pjl. § 22 jf. GDPR art. 32 nr. 1

[55] Prop. 72 LS (2013-2014) s. 59

3.2.2 Logging

Logging er definert som «eit trygleikstiltak som inneber å etterkontrollere informasjonssystemer».[56] Om logging er det videre uttalt:

> «Innsynslogginga (som på fagspråket blir kalla klientbasert logging) er den som skjer internt i et system. Innsynslogginga omfattar mange ulike typar loggar. Typiske innsynsloggar er dei 'som dokumenterer vellykkede og mislykkede innloggingsforsøk, brudd på rettigheter tildelt brukeren, oppnådd adgang til filområder, og andre hendelser på systemet'. Med klientbasert logging kan ein mellom anna avdekkje såkalla snoking i registera.»

I lovforarbeidene er det videre uttalt at hensikten med logging er at den dataansvarlige skal være i stand til å avdekke tilfeller av uautorisert tilgang til person- og helseopplysninger, å forhindre at sikkerhetsbrudd i informasjonssystemene skjer, samt legge til rette for pasientenes innsyn. Videre følger det av de samme lovforarbeidene at om det er nødvendig å dele person- og helseopplysninger mellom helseforetak, må dette også være sporbart hos de helseforetakene det gjelder.[57] Det er i ny pasientjournalforskrift § 14 inntatt nærmere regler om loggføring, og hvordan den skal skje:

> «Tilgjengeliggjøring av opplysninger skal dokumenteres automatisk hos virksomheten. Dokumentasjonen skal minst inneholde informasjon om
>
> a) identitet og organisatorisk tilhørighet til den som har hentet fram helseopplysninger
> b) grunnlaget for tilgjengeliggjøringen
> c) tidsperioden for tilgjengeliggjøringen.
>
> Den registrerte har rett til innsyn i dokumentasjonen.
>
> Dersom oversikten viser at noen urettmessig har hentet frem journalopplysninger, skal virksomheten opplysningene er hentet fra og den registrerte, varsles, jf. personvernforordningen artikkel 33 og 34.»

Innsynsloggen vil vise hvem som har gjort oppslag i EPJ, hvordan opplysningene er behandlet, for eksempel om det er lagt til opplysninger eller foretatt endringer. Hvilket tidspunkt det er gjort oppslag, og dens varighet vil også fremgå av loggen. Logg er nødvendig fordi helsepersonell har teknisk tilgang til flere opplysninger enn de juridisk sett har lov til å slå opp i. Innsynsloggen vil derfor være et sentralt verktøy som del av helseforetakets

[56] Meld. St. 11 (2012-2013) Personvern – utsikter og utfordringar punkt 9.3.2 s. 86-87.

[57] Prop. 72 L (2013-2014) s. 59

internkontroll for å avdekke uberettigede oppslag. Dette vil bidra til etterlevelse av helsepersonells taushetsplikt, og forebygge snoking. Et annet relevant moment knyttet til innsynsloggen er pasienters innsyn i egen journal og logg. Pasienter har krav på innsyn i egen logg etter pasient- og brukerrettighetsloven § 5-1 jf. GDPR art. 15 jf. hlp § 41, samt den nye pasientjournalforskriften § 14 andre ledd. Kravet på innsyn i egen logg vil fungere som et kontrolltiltak overfor helsepersonell ettersom pasienten selv vil kunne avdekke urettmessige oppslag. Statens helsetilsyn bemerket i sak 2016/1808 at de tilsynssaker som er blitt behandlet etter ikrafttredelsen av hlp. § 21a, i det alt vesentlige er oppstått etter klage fra pasienter om urettmessig tilegnelse av deres helseopplysninger.[58]

I Normen er det utarbeidet en rekke retningslinjer som skal veilede helseforetak, herunder helsepersonell, om hvordan loggingen skal utføres.[59] Overordnet fremgår det som sentralt i loggen at tiltakene skal bidra til at loggene enkelt skal analyseres med henblikk på å oppdage brudd på regler om tilgang til EPJ. Det første eksempelet er å ha analyseverktøy som er i stand til å fange opp avvik senest en uke etter at det har skjedd. Videre skal man kunne sammenholde loggene med et autorisasjonsregister, slik at det er mulig å identifisere hvem avviket kan kobles til.[60] Hvilke reaksjoner som skal iverksettes ved brudd er også inntatt i Normen, dette er personalmessige reaksjoner, for eksempel om det skal gis en advarsel til arbeidstakeren og om helsetilsynet skal varsles.[61] Om dette ikke er tilstrekkelig er det angitt i Normen at det skal iverksettes ytterligere tekniske tiltak, men det kan stilles spørsmål til hvor gjennomførbart dette er.

3.2.3 Autentisering

Det første steget i å gi tilgang er autentisering. Dette er en metode for å verifisere en påstått identitet før det gis tilgang til et informasjonssystem[62], f. eks EPJ. Lovforarbeidene legger til grunn at autentisering er et bevis for at oppgitt identitet er korrekt, og at når det gis tilgang til helseopplysninger, er det viktig at det er stor grad av sikkerhet for personen er den

[58] Statens helsetilsyn sak 2016/1808 dokument 74, 11. juli 2017 s. 6
[59] Direktoratet for e-helse: Bransjenorm for informasjonssikkerhet og personvern i Helse- og omsorgstjenesten s. 31
[60] Direktoratet for e-helse: Bransjenorm for informasjonssikkerhet og personvern i Helse- og omsorgstjenesten s. 35
[61] Direktoratet for e-helse: Bransjenorm for informasjonssikkerhet og personvern i Helse- og omsorgstjenesten s. 35
[62] Håndboka OUS: https://ehandboken.ous-hf.no/document/666, sist sjekket 09.05.19

vedkommende gir seg ut for å være.[63] De samme forarbeidene stiller krav til at dette skal skje ved hjelp av autentiseringsmekanismer på et høyt sikkerhetsnivå, og det uttales videre at autentiseringen også skal sikre at loggen viser identiteten til vedkommende helsepersonell som har hatt tilgang til opplysningene. I den nye pasientjournalforskriften § 13 andre og tredje ledd følger det at:

> Journalopplysninger kan bare gjøres tilgjengelig for personell som gjennom autentisering kan bekrefte sin identitet på en sikker måte.
>
> Den dataansvarlige skal ha oversikt over hvem som har tilgang til hvilke typer opplysninger og kunne kontrollere i ettertid hvem som har benyttet seg av tilgangen

Etter ordlyden av første ledd blir det i stor grad lagt opp til helseforetaket selv å vurdere hva som er «en sikker måte» å bekrefte sin identitet gjennom autentisering. Videre legger stiller tredje ledd krav til at helseforetaket eksempelvis har et autentiseringsregister, som kan brukes til å kontrollere tilganger og sammenholde disse med logg.

Autentisering kan gjøres gjennom en av tre typer autentiseringsfaktorer. Det er noe personen vet, for eksempel et passord, noe personen har, for eksempel en passordkalkulator eller noe personen er, for eksempel et fingeravtrykk.[64] En problemstilling som kan knytte seg til autentisering er at helsepersonell låner bort passordet sitt eller forlater PCen uten å logge av slik at andre urettmessig i helseforetaket kan få tilgang. Den informasjonen som fremgår i innsynsloggen vil da ikke være korrekt, og hensikten med autentisering forfeiler

3.2.4 Autorisering

Etter autentisering gjøres autorisering for å verifisere hvilke rettigheter en bruker har i et informasjonssystem; for eksempel hvilke filer som kan åpnes, endres, slettes m.v.[65] I autorisasjon ligger det etter forarbeidene at «helsepersonell og annet personell må være autorisert for å få tilgang til helseopplysninger». [66] I de samme forarbeidene stilles det krav til at det skal angis hvilke plikter og rettigheter den enkelte har. Videre må en autorisasjon omfatte informasjon om den autoriserte kan registrere beslutninger om helsehjelp, noe som

[63] Prop. 72 LS (2013-2014) s. 59

[64] Håndboka OUS: https://ehandboken.ous-hf.no/document/666, sist sjekket 09.05.19

[65] Håndboka OUS: https://ehandboken.ous-hf.no/document/666, sist sjekket 09.05.19

[66] Prop. 72 LS (2013-2014) s. 59

innebærer at det kan åpnes for at også annet helsepersonell kan få tilgang til opplysninger ved å beslutte dette selv ved å oppgi formålet med tilgangen, og på hvilken måte dette skal gjennomføres. Muligheten til at helsepersonell selv kan beslutte tilgang, er et sentralt risikoreduserende tiltak i akutte situasjoner der hurtig tilgang til helseopplysningene er avgjørende for pasientens liv og helse. Med den nye pasientjournalforskriften, er det i § 13 innført en rekke krav til autorisasjonen:

> Behandling av journalopplysninger skal baseres på bestemte tildelte tillatelser til å lese, registrere, redigere, rette, slette, sperre eller på annen måte behandle opplysninger i journalen (autorisasjon). Autorisasjonen skal
>
> a) beskrive rettighetene og pliktene som autorisasjonen omfatter
> b) angi hvilke virksomheter autorisasjonen omfatter
> c) dokumenteres i virksomhetens oversikt over helsepersonells autorisasjoner
> d) være tidsbegrenset
> e) vurderes på nytt når det oppstår endringer i ansvarsområder eller ansettelsesforhold.

Det skilles på rett til å lese, skrive, endre og på andre måter behandle person- og helseopplysninger, jf. journalforskriftens første ledd, første punktum. Et slikt skille mellom de ulike rettighetene ved tildeling av autorisasjon er av stor betydning. Det vil for eksempel være et stort skille mellom en rett til å lese og rett til å skrive, ettersom det å skrive innebærer å endre virkelighetsbildet av helse- og personopplysningene i EPJ. Videre angir bokstav a til e presiseringer og krav til hva autorisasjonen.

Delegering av autorisering

Det overordnede ansvar for å tildele, administrere og kontrollere autorisasjoner, ligger hos den dataansvarlige i helseforetaket og hensynet til den lovpålagte taushetsplikten sentral.[67] Leder av helseforetaket kan delegere myndighet til å autorisere videre til en leder av den enkelte enhet eller avdeling ved et sykehus. Lederen med delegert ansvar og myndighet innen den aktuelle organisasjonsenheten er ansvarlig for å sikre at helsepersonell har nødvendige tilganger for å ivareta sine oppgaver. Tilgangen som gis skal være i samsvar med helsepersonellets faglige ansvarsområde, eksempelvis om den ansatte er lege eller sykepleier.

[67] Direktoratet for E-Helse: Bransjenorm for informasjonssikkerhet og personvern i Helse- og omsorgstjenesten v. 5.3, se punkt. 5.2.1, s. 26

Helsepersonells ulike roller og autorisering

Det er viktig at helsepersonell har klart definerte roller. I en rolle som lege eller sykepleier, kan en autoriseres og få tildelt tilgang til EPJ i tråd med taushetsplikten på sitt faglige ansvarsområde/deres tildelte oppgaver gjennom rollen, som nevnt over. Problematikken oppstår når helsepersonell ikke skiller på disse, og derved misbruker den rollen man har på sykehuset til å urettmessig tilegne seg opplysninger i en annen rolle. Saken fra Høyesterett inntatt i HR-2018-2452 er egnet til å illustrere problematikken rundt nettopp dette.

Den pensjonerte legen hadde ikke hatt noen form for behandlingsansvar for pasienten. Følgelig hadde han ikke tjenstlig behov til å slå opp i EPJ, og heller ikke samtykke fra pasienten. Han misbrukte derfor rollen han tidligere hadde hatt ved sykehuset for å få ut opplysningene. Det må på den andre siden kunne stilles spørsmål til om det er kritikkverdig fra sykehusets side at det ikke er gjennomført tilstrekkelig tilgangsstyring ved å ikke endre vedkommendes autorisasjon og adganger, når han går av ved pensjon, men fortsatt beholder kontoret på sykehuset. Det er klart at hans rolle ble endret, og ved å beholde denne tilknytningen til den tidligere arbeidsplassen, er det en potensiell risiko for at ulovlige oppslag i EPJ.

I vedtak om pålegg fra Datatilsynet etter tilsyn hadde et helseforetak blitt kritisert av for å ikke ha foretatt en god nok vurdering av tildeling av roller. Det regionale helseforetaket hadde gjort en samlet regional vurdering av hvilke tilganger som skulle gis de ulike rollene ved alle sykehusene, og ikke en selvstendig vurdering ved hvert enkelt sykehus.[68] Som et resultat av at det ikke var gjort en selvstendig vurdering i hvert helseforetak, mente Datatilsynet at tilgangene var for vide. Det enkelte helseforetak ble pålagt å gjøre en selvstendig vurdering.

Selvautorisering

Det kan gis adgang for helsepersonell til å gjennomføre selvautorisering. I dette ligger det en mulighet for autoriserte brukere å gi seg selv tilgang til helse- og personopplysninger, det forutsettes imidlertid at det er etablert prosedyrer for dette, både for den tekniske løsningen og hvordan helsepersonell utfører dette funksjonelt. Videre skal årsaken til selvautoriseringen

[68] Datatilsynet sak 17/00243 dokument 28, 22. februar 2018 s.

grunngis og dokumenteres i EPJ.[69] Vigerust og Engelschiøn viser til at «helsepersonell må kunne få tilgang til informasjon om personellet i en gitt situasjon selv må vurdere om det er nødvendig å få innsyn i.»[70] Adgangen til selvautorisering kan begrunnes i behovet for effektivitet, det å raskt kunne få tilgang til helseopplysninger for å yte helsehjelp. Videre uttaler de at det å gi helsepersonell selvautorisering og dermed anledning til søke frem relevante og nødvendige helseopplysninger, krever at den databehandlingsansvarlige setter inn tiltak for å sikre god tilgangsstyring, slik at det kun gis tilgang til helsepersonell med tjenstlig behov og innenfor gjeldende bestemmelser om taushetsplikt.[71]

Et eksempel på utfordring som kan oppstå ved selvautorisering er at mange helseforetak opererer med ulike journalsystemer parallelt. Ikke alle systemene er koblet sammen, og de kommuniserer derfor ikke med hverandre. Dette fører til at yrkesgrupper som i utgangspunktet ikke har tilgang til journal må foreta en ekstraordinær selvautorisering fordi de likevel har et tjenstlig behov. Et eksempel kan være at en lege beslutter seg tilgang til en EPJ for å forberede helsehjelpen. Legen gjør dette i forkant av at pasienten er kommet til avdelingen og at han formelt er autorisert for tilgang til pasientens journal. Dersom den ordinære autoriseringen er for streng, kan imidlertid konsekvensen bli at selvautoriseringen blir så omfattende at det blir vanskelig å skille ut hvilke oppslag som er reelle tjenstlige behov, og hva som er snoking. Det er derfor viktig at helseforetakene foretar tilstrekkelig og risikobasert tilgangsstyring slik at selvautorisering skjer unntaksvis og ikke som en hovedregel.

3.2.5 Selvbestemmelsesretten

En viktig del av tilgangsstyringen er pasientens rett til å selv bestemme hvem som skal ha tilgang til EPJ, dette kan gjelde hele eller deler av EPJ eller enkeltpersoner eller grupper av helsepersonell. Selvbestemmelsesretten kan sees i sammenheng med hlp §§ 25 og 45 om deling av pasientopplysninger mellom helsepersonell. Et eksempel som kan illustrere problematikk rundt selvbestemmelsesretten som en del av tilgangsstyringen, er uttalelse fra Sivilombudsmannen SOM-2018-303 knyttet til § 25. I dette tilfellet hadde en pasient reservert

[69] Direktoratet for E-Helse: Bransjenorm for informasjonssikkerhet og personvern i Helse- og omsorgstjenesten v. 5.3, s. 15

[70] Vigerust/Engelschiøn (2015) s. 113

[71] Ibid s. 112

seg mot at en bestemt lege skulle involveres i hans behandling ved sykehuset. Legen ble likevel involvert, og pasienten påklaget dette til Fylkesmannen som ikke gav medhold. I uttalelsen fra Sivilombudsmannen ble det konkludert med at pasientens anmodning om vurdering av brudd på taushetsplikten, ikke kunne vurderes som «åpenbar grunnløs»[72] og Fylkesmannen ble vurdert om å vurdere saken på nytt.[73] Det var ikke gitt tilgang til EPJ, men sett at legen var gitt tilgang til EPJ i strid med hlp. § 45, ville den manglende tilgangsstyringen bestått i at sykehuset ikke sørget for at selvbestemmelsesretten, i form av reservasjon mot legen, var respektert av sykehuset.

3.3 Personvernforordningen art. 32

3.3.1 Innledning

Kravet til tilgangsstyring må også vurderes i lys av GDPR art. 32 om sikkerhet ved behandlingen, jf. pjl. § 22, første ledd, første punktum. Av artikkelens nr. 1, første avsnitt følger det at:

> «Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet […]»

3.3.2 Tekniske og organisatoriske tiltak

Av bestemmelsens første ledd, første punktum følger det at dataansvarlig og databehandler «skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. personvernforordningen artikkel 32»

Bestemmelsens første ledd, første punktum er en henvisning til GDPR art. 32, som er en generell regel om sikkerhet ved behandling av personopplysninger. Fordi man står overfor en bestemmelse med direkte henvisning til art. 32 i pjl. § 22, må også artikkelen drøftes. Det fremkommer av art. 32 nr. 1 at:

[72] Jf. Ot.prp.nr 13 (1998-1999) pkt. 23.2.5
[73] Sivilombudsmannens uttalelse: SOM-2018-303

> «Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet […]»

Deler av artikkelen siteres direkte i lovteksten. Det er imidlertid inntatt en rekke momenter i art. 32 nr 1, som må anses å ha en veiledende karakter idet det skal fastlegges hvilke tiltak som skal iverksettes for å ivareta informasjonssikkerheten. Videre angir også bestemmelsen en rekke punkter tiltakene må være egnet til å tilfredsstille:

«…

a) pseudonymisering og kryptering av personopplysninger,
b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og – tjenestene,
c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,
d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.»

Det første av vurderingsmomentene er behandlingens art, formål, omfang og sammenheng den behandles i. Ved helseopplysninger i EPJ er det tale om opplysninger som kan være av svært sensitiv karakter. Helseopplysninger om den enkelte pasient skal nedtegnes i EPJ.[74] Helseopplysningene i EPJ er av stort omfang, noe som sammen med at det dreier seg om sensitiv informasjon bidrar til stor sårbarhet. Dette er bakgrunnen for behovet for kravene til tilgangsstyring.

Tilgjengelig teknologi er neste moment av betydning for vurderingen. Dataansvarlig og databehandleren må sørge for at den teknologien som brukes, er oppdatert og egnet til å håndtere behandlingen av helseopplysningene til enhver tid. I art. 32 nr. 1 bokstav a) er det gitt som eksempel at tiltakene skal kunne være egnet til pseudonymisering og kryptering, med andre ord å gjøre opplysninger ugjenkjennelige. Hvis dataansvarlig og databehandler står overfor flere valgalternativer for å gjennomføre denne type tiltak, må det som er best egnet velges, selv om det kan bety vesentlige endringer.

[74] Forskrift av 1. juli 2015 nr. 853 om IKT-standarder i helse- og omsorgstjenesten § 3

Momentet som gjelder kostnader av gjennomføringen av tiltakene, må forstås som et krav til at dataansvarlig og databehandler må kunne dokumentere at alvoret av et eventuelt informasjonssikkerhetsbrudd, er vurdert opp mot kostnadene ved å forebygge at et slikt brudd kunne oppstå. Hvis det et brudd ikke er gjennomført enkle og lite kostnadskrevende tiltak for å redusere risikoen, vil det enklere kunne konstateres brudd på informasjonssikkerheten.

Et siste moment det vises til i art. 32 nr. 1 er sannsynligheten og konsekvensene for at uønskede- og ulovlige hendelser skal inntreffe ved behandlingen av personopplysninger, i denne sammenheng helseopplysninger. Sannsynligheten for at slike hendelser skal inntreffe og opplysningenes sårbarhet, øker med omfanget av helseopplysninger om den enkelte pasient, og med antall helsepersonell og andre ansatte som kan ha tilgang til dem. Kombinert med at det dreier seg om helseopplysninger av betydelig sensitiv karakter, vil uønskede og/eller ulovlige hendelser kunne ha svært alvorlige konsekvenser for den enkelte pasients personlige integritet.

Videre må første ledd ses i sammenheng med momentene som er nevnt i bokstav a-d. Ordlyden av «alt etter hva som er egnet» kan synes å gi alternativene i a-d en status som minstekrav, fordi tiltakene som må gjennomføres, må være i stand til å ivareta disse momentene.

Tiltakene må være egnet til kryptering og pseudonymisering, jf. bokstav a). I GDPR art. 4 nr. 5 defineres pseudonymisering som:

> «behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert bruk av tilleggsopplysninger, forutsatt at nevnte tilleggsopplysninger lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar fysisk person»

Videre legger Datatilsynet til grunn at det med kryptering menes «metode for å gjøre data (for eksempel tekst uleselig for andre ved hjelp av en matematisk funksjon (krypteringsteknikk/-algoritme) og en forhåndsbestemt nøkkel».[75] Med andre ord skal tiltakene kunne generere helseopplysningene slik at de blir ugjenkjennelige. Hvis dataansvarlig og databehandler står overfor flere valgalternativer for å gjennomføre denne type tiltak, må det som er best egnet fra et teknisk ståsted velges. Dette er et moment som er på siden av oppgavens problemstilling

[75] Datatilsynet: https://www.datatilsynet.no/regelverk-og-verktoy/verktoy/ordbok-a-til-a/#K, sist sjekket 09.05.19

som gjelder tilgangsstyring, men et viktig moment for å ivareta informasjonssikkerheten i sin helhet.

I bokstav b) er det angitt en rekke egenskaper tiltakene skal verne. Dette er konfidensialitet, integritet, tilgjengelighet og robusthet.[76] Den tidligere lovbestemmelsen i pjl. § 22 hadde overskriften «konfidensialitet, tilgjengelighet, integritet og kvalitet». Sammen med at det i forarbeidene presiseres at dagens bestemmelse i pjl. § 22 er en videreføring av gjeldende rett, samtidig som de fremgår av art. 32, så viser det hvilken sentral plass dette må har i helseforetakenes vurderinger av informasjonssikkerhetstiltak. Spesielt er det tilgjengelighet og konfidensialitet som spiller en sentral rolle når det skal foretas tilgangsstyring, fordi det må foretas en avveining mellom dem for å sikre forsvarlig tilgangsstyring.

Å sikre tilgjengelighet til helseopplysningene er helt grunnleggende for at helsepersonell skal kunne yte forsvarlig helsehjelp. Lovforarbeidene presiserer at helseopplysninger kun skal være tilgjengelig når det er legitimt behov for dem. [77] Engelschiøn og Vigerust viser til at sikring av tilgjengelighet innebærer at det må sørges for at de opplysningene som skal behandles av autorisert helsepersonell, er tilgjengelig til den tid og på det sted det er behov for dem. [78] Helsepersonell kun gis adgang dersom taushetsplikten gir adgang til det og de har et tjenstlig behov. Det må derfor foretas en avveining mellom konfidensialitet og tilgjengelighet når et tiltak skal iverksettes. Tiltakene som innføres kan ikke være så strenge at det trenerer helsepersonells mulighet til å effektivt kunne yte forsvarlig helsehjelp, men på den andre siden kan det heller ikke gis for vide tilganger. En utfordring knyttet til dette er at helsepersonell gjennom sine yrker, som for eksempel sykepleier og leger, blir gitt en type adgang som gjelder for deres roller. Fordi tilgangsstyringen gis for grupper med roller, og ikke skreddersys for den enkelte i gruppen, kan adgangen oppleves som for vid. Det er også her risikoen for snoking i EPJ lett oppstår.

Med konfidensialitet menes at personopplysningene ikke skal være tilgjengelig for uvedkommende, med andre ord at uvedkommende ikke skal få kjennskap til opplysningene. [79] I sammenheng med helseopplysninger i EPJ betyr dette at helsepersonell kun skal ha tilgang

[76] Dette er også en del av personvernprinsippene som fremgår av GDPR art. 5.
[77] Prop. 72 L (2013-2014) s. 183

[78] Engelschiøn/Vigerust (2015) s. 111

[79] Prop. 72 L (2013-2014) s. 183

dersom de har tjenstlig behov. Konfidensialiteten er blant annet sikret gjennom regler om taushetsplikt, som er både et lovpålagt og et organisatorisk tiltak, og ved å etablere tekniske sikkerhetsbarrierer i EPJ som et teknisk tiltak. [80]

Med integritet menes at helseopplysninger i EPJ til enhver tid skal være korrekte dvs ikke være urettmessig endret. I lovforarbeidene uttales det at «krav til integritet betyr at helseopplysninger skal være sikret mot uautorisert endring eller sletting under transport eller lagring.» [81] Regler om taushetsplikt, og etablering av sikkerhetsbarrierer vil også være egnet til å verne om integriteten til helseopplysningene i EPJ. Dette er ikke bare av betydning for informasjonssikkerheten, opplysningene i EPJ må være korrekt for at helsepersonell skal kunne yte forsvarlig helsehjelp.

Ved innføringen av GDPR ble disse egenskapene supplert med begrepet robusthet. En alminnelig forståelse av begrepet tilsier at en med robusthet mener at tiltakene må være etterrettelige og holdbare. Wessel og Ødegård forklarer begrepet som virksomhetens evne til å gjenopprette normaltilstand ved sikkerhetsbrudd.[82] Med andre ord skal tilgangsstyringen være så robust at den ved sikkerhetsbrudd verner helseopplysningenes konfidensialitet og integritet. I tillegg skal de igjen kunne gjøres tilgjengelig innen en forsvarlig tidsramme beskrevet av helseforetaket. Dette er nærmere beskrevet i neste punkt.

Etter bokstav c) skal tiltakene som brukes ha «evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse». I ordlyden ligger det at dataansvarlig og databehandler må ha konkrete planer og rutiner for hvordan man skal gjenopprette til tilgjengelighet og tilgang til EPJ dersom det oppstår svikt. For eksempel ved serversvikt, strømbrudd eller datainnbrudd ved hacking. Dette er med andre ord et krav helseforetakene må forholde seg konkret til innen en beredskapssituasjon.

Etter bokstav d) skal til sist tiltakene være egnet til å legge til rette for «prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er». Eksempler på slike tiltak er at dataansvarlig og databehandler har gode systemer for logging av hvem som slår opp i EPJ, og jevnlig foretar stikkprøver.

[80] Engelschiøn/Vigerust (2015) s. 111

[81] Prop. 72 L (2013-2014) s. 183

[82] Wessel/Ødegård (2018) s. 217

Etter en samlet vurdering anses det som er av størst betydning og mest sentralt for tilgangsstyringen, å være en balansert avveiningen mellom tilgjengelighet og konfidensialitet på bakgrunn av en oppdatert risikovurdering. Samtidig som uvedkommende ikke skal gis tilgang til EPJ, er sikring av tilgjengelighet en svært sentral del av informasjonssikkerheten. Hensikten med oppbevaring og behandling av helseopplysninger i EPJ er nettopp å gi forsvarlig helsehjelp. Dette forutsetter en effektiv tilgjengeliggjøring av opplysningene for helsepersonellet som trenger dem når de trengs, samtidig som konfidensialiteten blir ivaretatt. Dette forutsetter effektfulle iverksatte risikobaserte tiltak som sikrer både konfidensialitet, tilgjengelighet, integritet og robusthet. Det er i forlengelsen av dette sentralt at helseforetakene kan dokumentere at det er gjort vurderinger av hvilke opplysninger de ulike helsepersonellgruppene trenger tilgang til ved ytelse av helsehjelp.

3.3.3 Kravet til gjennomføring av risikovurdering

Ordlyden i art. 32 nr. 1 «med hensyn til risikoen» tilsier at tiltakene som skal iverksettes, også tilgangsstyring, må tilpasses det aktuelle risikobildet, og gir derfor anvisning på en risikovurdering. I art. 32 nr. 2 er det nærmere angitt at det:

> «ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.»

Risiko som er forbundet med «utilsiktet eller ulovlig tilintetgjøring, tap og endringer» sikter til hendelser som kan utgjøre en trussel for helseopplysningenes i EPJs integritet, og utfordrer dens robusthet. Dette kan for eksempel være helsepersonell som foretar urettmessige endringer eller sletter helseopplysninger i EPJ. Videre må omfatte ikke-autorisert utlevering eller tilgang til personopplysninger som en trussel mot helseopplysningenes konfidensialitet. Dette kan for eksempel være datainnbrudd.

Høsten 2016 mottok Datatilsynet flere bekymringsmeldinger fra ansatte i Helse Sør-Øst RHF og pasienter vedrørende utkontrakteringen av drift- og vedlikeholdstjenester til utenlandsk leverandør, som blant annet brukte underleverandører i Bulgaria. Det ble blant annet pekt på mulige konsekvensene dette kunne ha for informasjonssikkerheten i helseforetakene og personvernet for pasientene. Dette fordi de eksterne databehandlerne i Bulgaria hadde tilgang

til å gjøre oppslag i EPJ til pasientene i Norge. Helse Sør-Øst RHF lagrer pasientopplysninger om ca. halvparten av alle innbyggere i Norge. Datatilsynet slo fast at helseforetakene ikke hadde oppfylt pliktene de hadde som behandlingsansvarlig til å sørge for sikkerhetsledelse, risikovurdering og tilgangsstyring i forbindelse med tjenesteutsettingen. Datatilsynet varslet derfor i 2017 at ni helseforetak ville ilegges overtredelsesgebyr på 800 000 kroner, og samlet 7,2 millioner kroner.[83]

Gebyret ble ilagt i medhold av både tidligere pjl § 22 og den tidligere personopplysningsloven. Avgjørelsen retter kritikk mot manglende tilgangsstyring knyttet til outsourcing og eksterne aktører som driver datasupport. Faktum i saken faller derfor på utsiden av tilgangsstyring knyttet til helsepersonells tilgang til EPJ. Datatilsynet kommer imidlertid med generelle betraktninger knyttet til risikovurdering, som kan være egnet til å bidra til redegjørelsen.[84] På tidspunktet for avgjørelsen hadde ikke GDPR enda trådt i kraft, men Datatilsynet peker på at den nye regelen i GDPR art. 32 er en videreføring av gjeldende rett i pjl. § 22.[85]

Datatilsynet uttaler at tilgangsstyring er et sårbarhetsreduserende tiltak som implementeres på grunnlag av en risikoanalyse. [86] Videre utdypes det at formålet med en risikovurdering er å sikre at virksomhetene, i det foreliggende tilfellet helseforetakene, klarlegger sannsynligheten for og konsekvensene av sikkerhetsbrudd og sammenligner resultatet av vurderingen med virksomhetens fastlagte kriterier for akseptabel risiko.[87]

Datatilsynet peker på at en tilstrekkelig risikovurdering krever at det må kartlegges hvilke opplysninger som skal behandles, og hvilken verdi disse opplysningene har for virksomheten. Videre må det kartlegges hvilken verdi opplysningene potensielt kan ha for uvedkommende. i. Ved denne vurderingen er det også sentralt, hvilken skade det kan utgjøre for eierne av de

[83] Datatilsynet: https://www.datatilsynet.no/aktuelt/2017/ni-helseforetak-er-varslet-om-gebyr/

[84] Det er tatt utgangspunkt i varselet om vedtaksgebyr til Sykehuset i Telemark HF, Datatilsynet sak 16/01531 dokument 52, 24.oktober 2017

[85] Vedtakets s. 18

[86] Vedtakets s. 11

[87] Vedtakets s. 13

aktuelle opplysningene, om noen skulle misbruke dem. Derfor tillegges opplysningenes karakter, verdi og omfang stor betydning i risikovurderingen.[88]

Risikobildet er ingen statisk tilstand, men vil endre seg over tid. Faktorer det pekes på i denne sammenheng er rettssikkerhet, finansiell- og politisk stabilitet, teknisk infrastruktur, hendelseshåndtering, levestandard og samfunnsstruktur.[89] Fordi risikobildet stadig er i endring, må helseforetakene både gjennomføre og kontinuerlig oppdatere sine risikovurderinger for å oppfylle lovens krav.

Datatilsynet viser i sitt vedtak til at risikovurderinger, for å oppfylle lovens krav, må gjøres når det er nødvendig for å ta stilling til et endret risikobilde. Endret risikobilde kan forårsakes av ytre faktorer eller av planlagte endringer internt. I en situasjon som i det foreliggende, der det er tale om en anskaffelse, er det nødvendig at helseforetaket på forhånd gjennomfører en risikovurdering for å klarlegge forhold som kan påvirke helseforetakenes evne til å sikre etterlevelse av regelverket. Når en slik risikovurdering gjøres på forhånd av anskaffelsen, blir det tydelig for oppdragsgiveren hvilke risikoreduserende tiltak som må gjennomføres eller kreves, for at tjenesten skal kunne leveres av en ekstern leverandør.[90]

I følge Datatilsynets vedtak, er også teksten i GDPR art. 32 mer utfyllende enn den tidligere ordlyden i pjl. § 22, når det gjelder risikovurderinger. Det må tydelig fremgå at for å oppnå formålet med slike vurderinger, må de gjennomføres før tiltakene besluttes og gjennomføres. Forventet effekt av tiltakene må vurderes og det må fortløpende kontrolleres om og i hvilken grad de har nødvendige reell effekt i form av tilstrekkelig og akseptabel sikkerhet også over tid. Det fremgår klart av teksten at sannsynligheten for, og hvor alvorlige konsekvenser et tiltak kan få for enkeltindividers rettigheter og friheter skal vurderes.

I tillegg til en risikovurdering, er også dataansvarlig forpliktet til å vurdere personvernkonsekvenser for sine behandlinger av personopplysninger for å avgjøre om de skal foreta en personvernkonsekvensanalyse, jf. art. 35 nr. 1. Dersom behandling av personopplysninger medfører høy risiko for fysiske personers rettigheter og friheter, plikter den dataansvarlige å foreta en slik personkonsekvensanalyse av den aktuelle behandlingen, jf. GDPR art. 35 nr. 7. Etter GDPR art. 35 nr. 1 skal det foretas en personkonsekvensvurdering:

[88] Vedtakets s. 14
[89] Vedtakets s. 14
[90] Vedtakets s. 5 og 16

> «Dersom det er trolig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet.»

Wessel-Aas og Ødegaard viser til at kravet etter art. 35 nr. 1 særlig vil gjøre seg gjeldende i situasjoner der man tar i bruk ny teknologi.[91]

3.3.4 Atferdsnormer som informasjonssikkerhetstiltak

Det følger av art. 32 nr. 3 at man for å påvise at kravene i artikkelens nr. 1 er oppfylt, kan gjøre dette ved å overholde «godkjente atferdsnormer som nevnt i artikkel 40 eller godkjent sertifiseringsmekaniske som nevnt i 42». Artikkelen åpner for at man i den enkelte bransje kan utarbeide og benytte atferdsnormer som skal bidra til at reglene i GDPR blir overholdt. Normen er som nevnt i punkt 1.2.3, under oppdatering og enda ikke godkjent av Datatilsynet. Bruk av Normen forutsetter at den ikke er i strid med GDPR og særlovgivningen i helseretten.

3.3.5 Dataansvarliges instruksjonsmyndighet

Etter art. 32 nr. 4 pålegges den dataansvarlige og databehandleren å «treffe tiltak for å sikre at enhver fysisk person som handler for den behandlingsansvarlige eller databehandleren, og som har tilgang til personopplysninger, behandler nevnte opplysninger bare etter instruks fra den behandlingsansvarlige» med mindre annet fremgår av forordningen eller nasjonal lovgivning. Etter ordlyden «behandler nevnte [person]opplysninger bare etter instruks fra behandlingsansvarlige» er det dataansvarlig som trekker grenser/bestemmer hvordan behandlingen av helseopplysningene skal foregå.

Dataansvarlig er etter ordlyden forpliktet til å sørge for at oppdragstakere blir gitt instrukser utarbeidet av den dataansvarlige. Instruksene skal gis gjennom en databehandleravtale, se punkt. 3.1.2. Dataansvarlig og databehandler skal også påse at instruksjonene blir fulgt opp av de ansatte. I forlengelsen av dette er dataansvarlig og databehandler indirekte pålagt å gi tilstrekkelig opplæring i hvordan instruksene skal forstås og etterleves. Det må imidlertid

[91] Wessel-Aas/Ødegaard (2018) s. 229

påpekes at det endelige ansvaret for behandlingen av helseopplysningene foreligger hos den dataansvarlige, som nevnt i punkt 3.1.2.

3.4 Kort om personvernforordningen art. 24 nr. 2

I forarbeidene er det inntatt en henvisning til GDPR art. 24 nr. 2 om innebygd personvern og tilgangsstyring.[92] Regelen i artikkelen beskriver ansvaret den behandlingsansvarlige har for internkontroll:

> «Dersom det står i et rimelig forhold til behandlingsaktivitetene, skal tiltakene nevnt i nr. 1 omfatte den behandlingsansvarliges iverksetting av egnede retningslinjer for vern av personopplysninger».

Regelen må ses i sammenheng med artikkelens nr. 1, som fastsetter at behandlingsansvarlig må gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandling av personopplysninger er i samsvar med GDPR. I artikkelen vises det videre til en rekke momenter som skal tas i betraktning når disse retningslinjene skal utarbeides. Med andre ord må helseforetaket kunne dokumentere at de har prosedyrer for gjennomføring og kontroll av tilgangsstyring, herunder logg, autorisering og autentisering, herunder at de etterleves av helsepersonell og er i tråd med GDPR.

3.5 Oppsummering av kravet til pjl. § 22

Oppsummert må man etter gjeldende bruke både pjl. § 22, GDPR art. 32 og pasientjournalforskriften §§ 13 og 14 når innholdet skal klarlegges. Dette utgjør et komplisert rettskildebilde, og det bærer preg av å presisere hvilke krav som skal oppfylles, uten at det gis noen god veiledning for hvordan kravene skal oppnås.

[92] Prop. 56 LS (2017-2018) punkt. 38.2

4 Hva er utfordringene i dag?

Dom fra Høyesterett som nevnt i punkt 2.2.1 om forholdet mellom tilgangsstyring og taushetsplikten, illustrerer flere utfordringer knyttet til tilgangsstyring, i tillegg til problematikk rundt helsepersonells ulike roller. Det kan for eksempel stilles spørsmål ved hvorfor legen fortsatt hadde tilgang etter at han hadde gått av ved pensjon som overlege ved avdelingen. Han fortsatte som professor og beholdt sitt kontor, samtidig som han hadde et eget firma der han tilbydde tjenester som sakkyndig. Det må anses å være en systemsvikt fra sykehusets side at hans autorisasjon ikke ble endret, slik at den var i samsvar med hans rolle som professor emeritus. Det illustrerer svakhet ved digitalisering og EPJ, ved at det foreligger en juridisk sperre, men at det er mangel på teknisk sperre slik at barrieren som skal hindre at helsepersonell uten tjenstlig behov får tilgang til EPJ. Den nye pasientjournalforskriften vil gjennom mer detaljerte krav kunne bidra til en forbedring i tilgangsstyringen, herunder autorisering, i helseforetakene.

På den andre siden i lys av kravet til forsvarlig helsehjelp, vil det ikke være mulig å ha en tilgangsstyring som gjør at helsepersonell teknisk ikke har tilgang til mer enn de har rett til å slå opp i. For eksempel har en sykepleier på sengepost tilgang til alle pasienter på sengeposten. Sykepleieren har kun lov til å gjøre oppslag i EPJ til pasienten hun skal yte helsehjelp til. Det er imidlertid viktig at sykepleieren likevel har tilgang til samtlige pasienter på sengeposten fordi det kan oppstå en situasjon der vedkommende skal delta i helsehjelpen. Da er ikke de tekniske løsningene innrettet tilstrekkelig målrettet for å ivareta hensynet til tilgjengelighet.

I følge informasjonssikkerhetsdebatten, oppleves regelverket rundt tilgangsstyring i EPJ som komplisert i helseforetakene. Dette kan medføre at de prosedyrene som foretakene gir sine ansatte ikke er tydelige nok eller ikke er i samsvar med regelverket. I ytterste konsekvens kan det føre til advarsel:

Sak 2016/1808 fra Statens Helsetilsyn (heretter Helsetilsynet) illustrerer noen problemstillinger knyttet til tilgangsstyring til EPJ. Saken er vurdert etter regelverket før GDPR og den nye pjl. § 22 trådte i kraft, men kan likevel være aktuell.

I saken konkluderte Helsetilsynet med at et helseforetak hadde brutt spesialisthelsetjenesteloven § 2-2, og to leger ble gitt advarsler, den ene i medhold av både

hpl. §§ 21 og 21a, og den andre i medhold av hpl. § 21. Datatilsynet konkluderte i samme sak gjennom en tilsynsrapport at det forelå brudd på pjl. § 22 jf. § 19. Saken gjaldt et par som var til konsultasjon ved et helseforetak. På forhånd hadde klager levert inn en prøve, og resultatet ble nedtegnet i en felles journal. Resultatet ble også sendt til fastlege. I løpet av konsultasjonen og etter øvrig korrespondanse mellom klager og klinikken, reagerte legen på klagers reaksjonsmønster. Avdelingsoverlege og overlege besluttet derfor å sette behandlingen på vent frem til de hadde innhentet ytterligere informasjon om bakgrunnen til klager. I medhold av bioteknologiloven § 2-6 ble det hentet ut sensitive opplysninger, i form av epikriser om klagers tidligere sykdomsforløp. På bakgrunn av denne informasjonen ble det bestemt at klinikken ikke kunne fortsette å tilby paret behandling og underrettelse om dette ble sendt til fastlege.

Klager oppdaget at vurderingene som lå til grunn for avslutningen av behandlingen, var nedtegnet i felles journal og klagde klinikken inn for Fylkesmannen og Datatilsynet.

Helsetilsynet konkluderte med at formålet med legens oppslag var psykososial vurdering som krever pasientens samtykke. Helseforetakets prosedyrer for tilgangsstyring tok ikke høyde for at slike oppslag krever samtykke fra pasienten. Til tross for at slike avvik som regel vurderes som systemfeil, gav Helsetilsynet i denne saken en advarsel til legene som gjorde oppslaget.

Denne saken er et eksempel som kan illustrere noe av problematikken rundt regelverket for tilgangsstyring: Helseforetakets har ansvaret for forsvarlige prosedyrer for tilgangsstyringen på systemnivå. Prosedyrene var i dette tilfellet ikke tilstrekkelige, og det fikk personlige konsekvenser for helsepersonell i form av advarsel fra Helsetilsynet.

4.1 Konsekvenser av GDPR

Konsekvensene av GDPR utgjør kanskje ikke en så stor realitetsforskjell som man får inntrykk av. Helselovgivningen knyttet til informasjonssikkerhet og tilgangsstyring ivaretok også tidligere de samme prinsippene, med innføringen av GDPR er det tidligere lovverket i stor grad videreført, men med ytterligere detaljering av kravene. Samtidig har regelverket stor kompleksitet med en vid ordlyd som gir rom for tolkning og som det kan være vanskelig å sette seg inn i for helsepersonell. Konsekvensen kan derfor bli at ansvaret for vurderingene i for stor grad blir overlatt til helseforetakenes jurister, informasjonssikkerhetsledere og

personvernombud.[93] I april 2019 sendte Helse og omsorgsdepartementet ut Rundskriv I-3/2019 om informasjonshåndtering i spesialisthelsetjenesten for å klargjøre regelverket. Samlet sett synes den største utfordringen å ligge i gapet mellom de kravene lovverket setter, og begrensede tekniske muligheter for informasjonssikkerhet og tilgangsstyring i «gårsdagens» IKT-systemer i helseforetakene. Videre bygger helseforetakene sine prosedyrer på Normen som arbeidsverktøy og lovteksten og GDPR blir derfor fjernt for helsepersonell i hverdagen.

4.2 Konsekvenser av ny pasientjournalforskrift

Den nye pasientjournalforskriften inneholder mer konkrete forslag/krav til hva helseforetakene kan gjøre for å forbedre tilgangsstyringen. Det gir en tydeligere sammenheng i regelverket at man nå kan bruke pasientjournalforskriften, fremfor å se hen til personopplysningsforskriften, som nå er av en mer administrativ karakter. Mange av kravene som følger av den nye pasientjournalforskriften er dessuten i samsvar med Normen, slik at disse punktene i Normen kan tillegges større vekt i vurderingen, om den benyttes sammen med forskriften.

[93] Personvernombudet er utpekt av en dataansvarlig, jf. poppyl § 19, jf. GDPR art. 37. Personvernombudets oppgave er å hjelpe dataansvarlig å følge personopplysningsloven og GDPR, med tilhørende forskrifter, se https://www.datatilsynet.no/regelverk-og-verktoy/verktoy/ordbok-a-til-a/#P, sist sjekket 09.05.19. Personvernombudets plikter og oppgaver er nærmere beskrevet i poppyl. § 18 og GDPR art. 38 og 39.

5 Konklusjon

Konklusjonen er etter en helhetlig vurdering av det foreliggende rettskildebilde, praksis og IKT-situasjonen i helseforetakene, at kravet til tilgangsstyring av EPJ enda ikke kan anses å tilstrekkelig ivareta både pasientens personvern og helsepersonells tjenstlige behov for tilgang til EPJ.

6 Forbedringstiltak

6.1 Normen

Som nevnt i punkt 3.1. er det i stor grad opp til helseforetakene å finne ut hvordan de skal oppfylle kravene regelverket stiller til tilgangsstyring. Normen er et hjelpemiddel og arbeidsverktøy for helseforetakene. Bruken av Normen er ikke uproblematisk og som rettskilde vil den ha begrenset rettskildemessig vekt. Et spørsmål som kan stilles er om også Normen bør innføres som en forskrift, slik at den kan tillegges tyngre rettskildemessig vekt.

I sakene fra både Datatilsynet og Statens helsetilsyn at tilsynsmyndighetene forholder seg til lovverket, mens helseforetakene forholder seg til normen. Det kan være problematisk, og det vil kanskje ha bidratt til en mer lik fortolkning av regelverket dersom Normen var fastsatt i forskrift.

På den andre siden møtes styringsgruppen hvert halvår, og det gir anledning til en dynamisk norm, som raskt kan endres slik at den møter behovene etter hvert som de foreligger. Dette gjør Normen godt rustet for å følge med på den teknologiske utviklingen. Det er ikke anledning til en like dynamisk atferdsnorm, dersom den skulle være en forskrift. Det poengteres dessuten i rundskriv fra HOD at «regelverket ikke skal være til hinder for innovasjon og bruk av ny teknologi som kan gi pasientene bedre helsehjelp».[94] Norm i forskrift ville derfor være i strid med en av de sentrale målsettingene med informasjonshåndtering i helseforetak.

Det vil også være slik at når EDPB kommer med retningslinjer for hvordan atferdsnormer skal utformes, vil det være naturlig å tro at det legges til rette for at Normen blir godkjent, eller at det utarbeides en ny atferdsnorm som kan ilegges rettskildemessig vekt, jf. GDPR art. 40 nr. 1. Det vil på bakgrunn av den ovennevnte argumentasjonen ikke være hensiktsmessig å innføre Norm i forskrift.

[94] Helse- og omsorgsdepartementet: Rundskriv I-3/2019 s.

6.2 Tydeligere regelverk

Det foreligger en rekke rettskilder knyttet til kravet til tilgangsstyring, og et komplisert rettskildebilde å forholde seg til. Det er nødvendigvis ikke manglende rettskilder, men disse kildene sier for lite om hvordan innholdet av reglene om tilgangsstyring skal forstås. De er ofte av liten veiledende karakter, og målet for hva man skal oppnå med tilgangsstyring er mye tydeligere kommunisert, enn fremgangsmåten og veien dit. Derfor blir det i stor grad opp til hvert enkelt helseforetak å finne ut hvordan de skal gå frem for å sikre informasjonssikkerheten i EPJ. I rundskriv fra Helse- og omsorgsdepartementet (HOD) uttaler departementet at de erfarer at det kan være uklarheter og ulike oppfatninger knyttet til forståelse og praktisering av reglene om taushetsplikt, personvern og informasjonssikkerhet.[95]

En konsekvens av et regelverk der det i stor grad er opp til den enkelte virksomhet å fortolke innholdet av reglene rundt tilgangsstyring, er at det skaper usikkerhet. HOD uttaler i den sammenheng at dersom jurister ved et helseforetak opplever at det er usikkerhet rundt tolkningen av helselovgivningen og juridisk litteratur eller andre kilder ikke gir svar, kan det være naturlig å rette en henvendelse til eget regionalt foretak, eventuelt til Helsedirektoratet eller Direktorat for e-helse.[96] Det kan stilles spørsmål til om rundskrivet egentlig bidrar til å rette opp i uklarheter, men heller forteller virksomhetene hvordan de eventuelt kan finne det ut. At det i så stor grad legges opp til at et hvert helseforetak må foreta en egen tolkning, svekker også hensynet til likhet og kan gi uønsket variasjon. Det som kan være brudd på regelverket et sted, kan gå under radaren et annet sted.

På en side er det positivt at HOD tydelig kommuniserer hvilke oppgaver de ulike instansene har med tanke på regelverket.

Et alternativ kunne være å utforme et skriv der det gjøres rede for hvordan reglene faktisk skal forstås. En mulighet kan være at dette gjennomføres i en felles atferdsnorm som også vil ha et mer dynamisk preg. En felles atferdsnorm vil være et omfattende arbeid, men det vil bidra til å forenkle og forbedre tilgangsstyringen i helseforetakene. Det skaper også gjennomgående gode rutiner i helseforetakene om de samme reglene gjelder overalt/skaper en god kultur for

[95] Helse- og omsorgsdepartementet: Rundskriv I-3/2019 s. 1

[96] Helse- og omsorgsdepartementet: Rundskriv I-3/2019 s. 6

hvordan håndtering av helseopplysninger skal foregå. Dette vil både styrke personvernet til pasientene og rettsvernet til helsepersonell.

Litteraturliste

Lover

1814 Kongeriket Norges Grunnlov – lov 17. mai 1814 (Grunnloven)

1967 Lov om behandlingsmåten i forvaltningssaker – lov 10. februar 1967 (forvaltningsloven)

1984 Lov om statlig tilsyn med helse- og omsorgstjenesten m.m. – lov 30. mars 1984 nr. 15 (helsetilsynsloven)

1992 Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske samarbeidsområdet (EØS) m.v. – lov 27. november 1992 nr. 109 (EØS-loven)

1999 Lov om helsepersonell m.v. – lov 2. juli 1999 nr. 64 (helsepersonelloven)

2014 Lov om behandling av helseopplysninger ved ytelse av helsehjelp – lov 20. juni 2014 nr. 42 (pasientjournalloven)

2018 Lov om behandling av personopplysninger – lov 15. juni 2018 nr. 38 (personopplysningsloven)

Forordninger

EØS-avtalen vedlegg XI nr 5e (forordning (EU) 2016/679) – personvernforordningen (GDPR)

Forarbeider

Offentlige utredninger

NOU 2019:5, 14.mars Ny forvaltningslov Lov om saksbehandlingen i offentlig forvaltning (forvaltningsloven)

Proposisjoner

Ot.prop. nr. 13 (1998-1999)	Om lov om helsepersonell m.v. (helsepersonelloven)
Ot.prop. nr. 14 (2000-2001)	Om lov om endringer i lov 2. juli 1999 nr. 64 om helsepersonell m v (helsepersonelloven) og enkelte andre lover
Ot.prop. nr. 25 (2007-2008)	Om lov om endringer i helsepersonelloven og helseregisterloven (krav til helsepersonells attester, erklæringer o.l., administrative reaksjoner og forbud mot urettmessig tilegnelse av helseopplysninger)
Prop. 91 L (2010-2011)	Om lov om kommunale helse- og omsorgstjenesteloven (helse- og omsorgstjenesteloven)
Prop. 72 L (2013-3014)	Om pasientjournalloven og helseregisterloven m.v. (helsepersonelloven)
Prop. 56 L (2017-2018)	Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen

Stortingsmeldinger

Meld. St. 11 (2012-2013)	Personvern – utsikter og utfordringer

Forskrifter

FOR nr. 1385 (2000)	Forskrift om pasientjournal. (Oppheves ved ikrafttredelse av ny forskrift om pasientjournal 1. juli 2019.).
FOR nr. 853 (2015)	Forskrift om IKT-standarder i helse- og omsorgstjenesten
FOR nr. 876 (2018)	Forskrift om behandling av personopplysninger
FOR nr. 168 (2019)	Forskrift om pasientjournal. (Ikrafttredelse 1. juli 2019.)

Rettspraksis

Høyesterett

Rt. 1997 s. 529

Rt. 2006 s. 529

Rt. 2013 s. 1442

HR-2018-2452-A

Den europeiske menneskerettsdomstol

EMD sak 20511/3 I mot Finland, avsagt 17. juli 2008

Litteratur

Engelschiøn og Vigerbust (2015)	Engelschiøn, Sverre og Elisabeth Vigerbust, *Pasientjournalloven og helseregisterloven*, 1. utgave, Oslo: Universitetsforlaget (2015)
Befring, Anne Kjersti mfl. (2016)	Befring, Anne Kjersti, Morten Kjelland og Aslak Syse mfl. medforfattere, *Sentrale helserettslige emner*, 1. utgave, Oslo: Gyldendal Norsk Forlag (2016)
Wessel-Aas og Ødegaard (2018)	Wessel-Aas, Jon og Magnus Ødegaard, *Publisering og behandling av personopplysninger*, 1. utgave, Oslo: Gyldendal Norsk Forlag (2018)
Befring og Ohnstad (2019)	Skar, Randi og Bente Ohnstad, *Helsepersonelloven Kommentarutgave*, 1. utgave, Bergen: Fagbokforlaget (2019

Forvaltningspraksis

Rundskriv

Helse- og omsorgsdepartementet: Rundskriv I-3/2019

Saker fra tilsynsmyndigheter

Personvernnemnda sak PVN-2015-07 (Tromsø kommune)

Statens helsetilsyn sak 2015/1502 dokument 3 og sak 2017/1783 dokument 13

Statens helsetilsyn sak 2016/1808 dokument 55, 14. juni 2017

Statens helsetilsyn sak 2016/1808 dokument 74, 11. juli 2017
Datatilsynet sak 16/01531 dokument 52, 24.10.17

Datatilsynet sak 17/00243 dokument 28, 22. februar 2018

Andre kilder

Artikkel 29-gruppen, Opinion 1/2010 on the concept of «controller» and "processor», Adopted on 16 february 2010.

Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen), Direktoratet for e-helse.

Direktorat for e-helse: https://ehelse.no/standarder-kodeverk-og-referansekatalog/elektronisk-pasientjournal-epj#informasjonskategorier-og-styring-av-tilgang-til-journalopplysninger

Difi: https://internkontroll-infosikkerhet.difi.no/ledelsens-gjennomgang/hvorfor-internkontroll-pa-informasjonssikkerhetsomradet

Datatilsynet: https://www.datatilsynet.no/regelverk-og-verktoy/verktoy/ordbok-a-til-a/#D

Datatilsynet: https://www.datatilsynet.no/aktuelt/2017/ni-helseforetak-er-varslet-om-gebyr/

Håndboka OUS: https://ehandboken.ous-hf.no/

Aftenposten: https://www.aftenposten.no/meninger/debatt/i/21O7yl/Sykehuset-ivaretar-bade-pasientsikkerhet-og-personvern--Solvi-Andersen

Aftenposten: https://www.aftenposten.no/meninger/debatt/i/m6mEdp/Den-vanskelige-rollen-som-personvernombud--Cecilie-Ronnevik-og-Thomas-Olsen

Østlandsposten: https://www.op.no/nyheter/larvik-kommune/helse/bekymret-for-taushetsplikten-na-stoppes-all-elektronisk-oversendelse-av-helseopplysninger-i-larvik/s/5-36-754560