

**Til:** Helse- og omsorgsdepartementet  
Postboks 8011 Dep  
0030 Oslo

**Kopi** Nasjonal IKT programkontor

**Fra:** Nasjonal IKT Fagforum Arkitektur

**Dato:** 16.09.10

## Høringsuttalelse - Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

<b>OPPSUMMERING</b> .....	<b>1</b>
<b>HOVEDKONKLUSJONER – ARKITEKTURMESSIGE KONSEKVENSER</b> .....	<b>2</b>
<b>FORSKRIFTENS OG PÅVIRKNING PÅ SPESIALISTHELSETJENESTENS ARKITEKTUR</b> .....	<b>3</b>
KAPITTEL 1 INNLEDENDE BESTEMMELSER .....	3
KAPITTEL II GENERELLE KRAV TIL INFORMASJONSSIKKERHET .....	4
KAPITTEL III KRAV OM SYSTEM FOR UTSTEDELSE AV AUTORISASJONER OG KRAV TIL AUTENTISERING .....	6
KAPITTEL IV TILGANG TIL HELSEOPPLYSNINGER I BEHANDLINGSRETTET HELSEREGISTER .....	9
KAPITTEL V TILLEGGSBESTEMMELSER FOR DIREKTE TILGANG TIL HELSEOPPLYSNINGER I BEHANDLINGSRETTET HELSEREGISTER PÅ TVERS AV VIRKSOMHETER .....	10
KAPITTEL VI SPERRING AV HELSEOPPLYSNINGER .....	14
KAPITTEL VII KRAV OM LOGGING OG DOKUMENTASJON AV TILGANG .....	15
KAPITTEL VIII AVSLUTTENDE BESTEMMELSER .....	17

### Oppsummering

Nasjonal IKT ved Fagforum Arkitektur har gjennomgått forskriften og vurdert denne opp mot dagens system og løsningsportefølje i de regionale helseforetakene, og den omforente arkitekturen slik den er nedfelt i styringsdokumentet "Tjenesteorientert arkitektur i spesialisthelsetjenesten". Generelt er vurderingen at forskriften er relativt godt i overensstemmelse med tjenesteorientering og de målbilder som tjenesteorienteringen skal understøtte.

Konsekvensene av forskriften for dagens arkitektur og systemportefølje er derimot stor, og en fullstendig realisering av kravene i forskriften vil medføre svært store endringer i arbeidsprosesser, system og løsningsporteføljer i alle regionale helseforetak. Dette skyldes både at forskriftens formål og omfang dekker en mye større løsningsportefølje enn det som tradisjonelt er ansett å være "journalssystemet", og at dagens løsninger og forvaltningen av disse har store mangler i forhold struktur og teknisk støtte for innholdsstruktur (strukturert journal), bruk av eksterne systemer for autentisering, autorisasjon, tilgangsstyring og logganalyse samt at det er stor variasjon i modenhet, evne og kapasitet blant leverandørene i forholdt til å realisere nye og omfattende krav.

Dagens dominerende EPJ leverandører i spesialisthelsetjenesten har ikke tilstrekkelig systemstøtte for strukturert journalføring, og det vil innebære store organisatoriske, prosjektmessige og utviklingsmessige endringer for å realisere strukturerte journalssystemer.

Ved innføring av andre nye IKT systemer som RIS/PACS, laboratoriestøttesystemer med flere, vil det være mulig å stille krav i anskaffelsene knyttet til oppfyllelse av forskriftens krav. Det er imidlertid en

trend i forhold til anskaffelse av nye kliniske støttesystemer at det i større grad er internasjonale leverandører som er konkurransedyktige, og det er ikke kjent for oss i hvilken grad forskriftens krav oppfylles av internasjonale leverandører, eller om det vil kreves lokalisering og utvikling.

For å kunne realisere tilgang på tvers ser vi at det er nødvendig med sentrale, nasjonale sambruks- og gjenbrukskomponenter for å sikre autentisering, logging og avtaleforvaltning mellom samarbeidsparter. Dette vil sette større krav til utvikling, forvaltning og tjenestestyring av nasjonale tjenester gjennom hele leveransejeden enn hva som er tilfelle i dag.

Innføring og realisering av forskriften og dens krav vil derfor realistisk sett kreve 5-10 år for å sette foretakene i stand til å drive sin virksomhet i tråd med lov og forskrift. Dette forutsetter at endringsarbeidet tilføres tilstrekkelig midler, og organisering av endringsarbeidet blir tilstrekkelig (sentralt) styrt og forankret ut i helseforetakene gjennom de regionale eierne.

## Hovedkonklusjoner – arkitekturmessige konsekvenser

Paragraf	Vurdering og konsekvenser
§1 og §2	<p>Formål og virkeområde (§1 og §2) tydeliggjør at forskriften regulerer mer enn tilgang til helseopplysninger i behandlingsrettede helseregistre på tvers av virksomheter. Kun fire av forskriftens totalt 36 paragrafer regulerer tilgang på tvers av virksomheter spesielt, de andre gjelder for alle behandlingsrettede helseregistre, dvs. <i>"alle IKT systemer som inneholder personidentifiserbar informasjon om pasienter og som benyttes for å yte helsehjelp eller administrere slik hjelp"</i></p> <p>Dette betyr at store deler av forskriften er en klargjøring og konkretisering av krav til sikkerhet i helserettede behandlingsregistre. Ivaretagelse av dette formålet krever god informasjonssikkerhet og gjelder "helseopplysninger i behandlingsrettede helseregistre" som innebærer at IKT systemer ut over de tradisjonelle "EPJ systemene" faller inn under forskriftens virkeområde.</p> <p>For tilgang på tvers av virksomheter synes det som forskriften regulerer online tilgang (direkte (lese-) tilgang til helseopplysninger på tvers av virksomheter) mellom to virksomheter der hvor disse samarbeider tett om pasienten og tilgangen inngår som en del av planlagte tjenester.</p> <p>En virksomhet kan inngå avtaler med flere virksomheter som gjennomfører slike planlagte tjenester, og bilaterale avtaler og sikkerhetsvurderinger må gjennomføres i hvert tilfelle.</p> <p><b><i>Samlet sett gir dette konsekvenser for arkitektur og teknisk løsningsdesign i de fleste fagsystemer i spesialisthelsetjenesten, og innebærer endring og tilpasning av mange systemer. I tillegg kommer at det mangler vesentlige komponenter for å oppfylle sikkerhetskravene ved online tilgang mellom juridiske enheter og de berørte fagsystemer. Samlet sett setter forskriften betydelige krav på alle berørte foretak i spesialisthelsetjenesten, som det vil være svært vanskelig å oppfylle uten en vesentlig større satsning på å bygge opp nasjonal praksis og tjenester som alle kan benytte. (Centre of excellence tankegang)</i></b></p>
§10, §14, §19	Det kreves en <b>strukturet journal</b> for å oppfylle flere av kravene i forskriften

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

	og dette er det få eller ingen systemer og leverandører til spesialisthelsetjenesten som leverer i dag. Endring og utskiftning av systemer vil kreve store investeringer og ressurser og berøre arbeidsprosessene i helseforetakene direkte. Dette er sannsynligvis den største utfordringen i forhold til å kunne etterleve forskriften.
§14, §15, §15 m.flere	<b>Krav til autentisering og autorisasjon</b> er spesifisert omfattende og vil kreve en helhetlig tilnærming til identitets- og tilgangstyring, samt en autorisasjonsmodell og autorisasjonssystemer og tjenester som ligger utenfor dagens journalsystemer.
	<b>Krav til logging, rapportering og tjenester</b> omkring sikkerhets-”governance” vil øke som følge av kravene i forskriften, og vil kreve utvikling av nye løsninger og tjenester i foretakene.
§24	<b>Avtaleregime</b> og tillitskjedene som skal til for å etablere tilgang på tvers i henhold til forskriften vil kreve betydelig arbeid på de organisatoriske og forvaltningsmessige nivåene. Dette er en betydelig forretningsmessig og organisatorisk problemstilling som kommer i tillegg til tekniske utfordringer.

## Forskriftens og påvirkning på spesialisthelsetjenestens arkitektur

### Kapittel 1 Innledende bestemmelser

§ 1 Forskriftens formål	Vurdering av konsekvenser
<p>Departementet foreslår å bruke begrepet ”<b>god informasjonssikkerhet</b>” i formålsparagrafen for å understreke at man er avhengig av pasientens tillit til at konfidensialitet, integritet, kvalitet og tilgjengelighet er ”mer enn tilstrekkelig”.</p> <p><b>Sporbarhet</b> er nødvendig for at man i ettertid kan måle/vurdere om informasjonssikkerheten har vært/er god. Det skal fremgå hvem som har registrert opplysningene, og dette kan gjøres ved hjelp av <b>digital signatur</b> eller tilsvarende sikker dokumentasjon.</p>	<p>Sporbarhet på tvers av systemer og virksomheter.</p> <p>Mer bruk av digitale signaturer.</p> <p>Sikker identifisering av ansatte i og på tvers av virksomheter</p> <p>Sikker identifisering av pasienter i og på tvers av virksomheter</p>
§ 2 Forskriftens virkeområde	Vurdering av konsekvenser
<p>Forskriften skal gjelde for behandling av helseopplysninger i behandlingsrettede helseregistre.</p> <p>Begrepet behandlingsrettet helseregister sikter til alle <b>registre som inneholder personidentifiserbar informasjon</b> om pasienter og som benyttes for å <b>yte helsehjelp</b> eller <b>administrere</b> slik hjelp.</p>	<p>Vil gjelde alle fagsystemer i helseforetakene, inklusive flere administrative.</p> <p>Unntak; systemer for forskning/kvalitetsregistre uten pasientidentifiserbar informasjon (anonymisert/pseudonymisert info)</p>

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

§ 3 Definisjoner	Vurdering av konsekvenser
<p>Departementet opprettholder forslaget fra høringsnotatet om at forskriften skal definere begrepene <b>autorisasjon</b> og <b>autentisering</b>. I tillegg foreslår departementet at det tas inn definisjoner av begrepene, ”<b>tilgang til helseopplysninger</b>”, ”<b>direkte tilgang til helseopplysninger</b>” og ”<b>sperrede helseopplysninger</b>”</p> <p>Departementet mener at beslutningsstyrt tilgang bør være et krav i forskriften, uavhengig av definisjonen av tilgang til opplysninger.</p> <p>I forskriften menes med</p> <ol style="list-style-type: none"> <li>1. <b>autentisering</b>: Prosess som gjennomføres for å bekrefte en påstått identitet.</li> <li>2. <b>autorisasjon</b>: En person i en bestemt rolle gis bestemte rettigheter til lesing, registrering, redigering, retting, sletting, sperring eller annen behandling av helseopplysninger.</li> <li>3. <b>tilgang til helseopplysninger</b>: Helseopplysninger om en eller flere bestemte pasienter er eller gjøres tilgjengelig for autorisert personell, jf. punkt 2.</li> <li>4. <b>direkte tilgang til helseopplysninger</b>: Helsepersonell kan logge seg rett inn på et behandlingsrettet helseregistersystem og fra dette systemet logge seg rett inn på andre behandlingsrettede helseregistersystemer, internt i virksomheten eller i ekstern virksomhet. Pålogging kan skje fra den interne virksomhetens helseregistersystem eller fra den eksterne virksomhetens system.</li> <li>5. <b>sperrede helseopplysninger</b>: Helseopplysninger som pasienten etter helsepersonelloven §§ 25 eller 45 har motsatt seg eller motsetter seg at andre gis tilgang til.</li> </ol>	<p>Krav til identifikasjon, autentisering og autorisasjon i alle <i>behandlingsrettede helseregistre</i> vil sette krav til en helhetlig tilnærming til brukerforvaltning, identitets- og tilgangsstyring. Dette gjelder både internt i et helseforetak og mellom helseforetak, og vil trolig medføre egne systemer og løsninger utenfor fagsystemene.</p> <p>Identifisering, tilgangsstyring og forvaltning (IAM) blir for omfattende og viktig til at hver enkelt fagsystemleverandør kan få løse dette.</p> <p>Det ligger også implisitt i <i>tilgang til helseopplysninger</i> at tilgangsstyringen skal være ”beslutningsstyrt” og beslutningen må kunne dokumenteres og spores. Er beslutningsstyrt tilgang godt nok forstått og definert til å benyttes i alle behandlingsrettede helseregistre, og er det behov for å knytte denne dokumentasjonen til et eget styringssystem?</p> <p>I <i>sperrede helseopplysninger</i> ligger det at en pasient kan sperre hele eller deler av journalinformasjonen og dette vil kreve klassifisering og struktur av type opplysninger i journal.</p>

## Kapittel II Generelle krav til informasjonssikkerhet

§ 4 Krav om forsvarlige systemer	Vurdering av konsekvenser
<p>Videre fulgte det av forskriften at <b>personopplysningsforskriften</b> kapittel 2 om informasjonssikkerhet vil gjelde som <b>utfyllende bestemmelser til forskriften</b>.</p> <p>Departementet mener det er viktig at forskriften inneholder et eget kapittel med generelle krav til informasjonssikkerhet for behandling av helseopplysninger, selv om noen av bestemmelsene kan sies å følge av personopplysningsforskriften.</p>	<p>Det at forskriften vil inneholde mer konkrete krav som blir rettslig bindende for helseforetakene og deres ledelse, bør medføre større behov for logging, audit og kontrollsystemer for å sikre etterlevelse.</p> <p>En (nasjonal?) IAM strategi med tilhørende kompetansebygging, forvaltningsregime og ”governance” blir</p>

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

<p>Det er etter departementets vurdering ikke tilstrekkelig at ovennevnte krav tas inn som merknader til personopplysningsforskriften eller er omhandlet i Norm for informasjonssikkerhet, blant annet fordi <b>merknadene og normen ikke er direkte rettslig bindende</b>.</p> <p>Det er ikke nok å ha et overordnet regelverk og forutsette at det etterleves nedover i virksomheten. Den <b>databehandlingsansvarlige må kunne dokumentere at forskriftens krav er implementert på alle nivåer i virksomheten</b>.</p>	<p>kritisk for helseforetakene.</p> <p>Opplæring av ansatte gjennom eLæring ved ansettelse, sikkerhetstesting og regelmessig godkjenning kan være et relevant tiltak og bør kunne etableres som nasjonal standard og tjeneste. eLæringssystemet kan kobles til identitetsforvaltning for knytte dokumentert opplæring til den enkelte ansatte.</p>
---	--

§ 5 Krav til planlegging, organisering og rutiner (utdrag)	Vurdering av konsekvenser
<p>Virksomhet som tar i bruk behandlingsrettede helseregistre, skal utarbeide en overordnet strategi og målsetting for informasjonssikkerheten i virksomheten. Det skal utarbeides informasjonssikkerhetsplaner og styrende dokumenter for behandlingen av helseopplysninger for alle nivåer i virksomheten.</p> <p><b>Alle nivåer i virksomheten skal ha skriftlige rutiner for behandling av helseopplysninger.</b> Rutinene skal ha utgangspunkt i den overordnede planen, jf. første ledd.</p>	<p>Ingen spesielle</p>

§ 6 Krav om internkontroll	Vurdering av konsekvenser
<p>Databehandlingsansvarlig skal etablere internkontroll i samsvar med helseregisterloven § 17. De systematiske tiltakene skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang det er nødvendig for å etterleve kravene i helseregisterloven og i denne forskriften.</p> <p>Kravet til internkontroll innebærer at den databehandlingsansvarlige blant annet skal ha kjennskap til gjeldende regler om behandling av helseopplysninger, tilstrekkelig og oppdatert dokumentasjon for gjennomføring av reglene samt ha denne dokumentasjonen tilgjengelig for de den måtte angå.</p> <p><b>Den databehandlingsansvarlige skal ha rutiner for oppfyllelse av sine plikter og de registrertes rettigheter etter det til enhver tid gjeldende regelverk, herunder ha rutiner for</b></p> <ul style="list-style-type: none"> <li>- administrasjon og kontroll av autorisasjoner etter kapittel III,</li> <li>- administrasjon, kontroll og oppfølging av logg etter kapittel VI,</li> <li>- innhenting av <b>samtykke</b> etter § 29,</li> <li>- oppfyllelse av <b>henvendelser fra den registrerte om innsyn i logg</b> etter § 36 og</li> </ul>	<p>Autorisasjoner skal være tidsbegrenset og kan ha en varighet på 1-2 år for ansatte med faste gjøremål i en stabil virksomhet. Endringer i ansettelsesforhold eller organisasjon skal medføre revurdering av tildelte autorisasjoner. Dette fordrer en mer aktiv bruk av FRESH enn det som er tilfellet i dag og "FRESH tjenesten" må videreutvikles i en nasjonal sammenheng.</p>

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

<p>- <b>avdekking, oppretting og forebygging av overtredelser</b> av forskriften.</p> <p>Databehandlere som behandler helseopplysninger på oppdrag fra den databehandlingsansvarlige, skal behandle opplysningene i samsvar med rutiner den databehandlingsansvarlige har oppstilt.</p>	
---	--

§ 7 Sikkerhetsledelse	Vurdering av konsekvenser
<p>Den som har den daglige ledelse av virksomheten som den databehandlingsansvarlige driver, har ansvaret for at informasjonssikkerheten i virksomheten er god og at bestemmelsene i helseregisterloven og denne forskriften følges.</p>	Ingen spesielle

§ 8 Forholdet til personopplysningsforskriften	Vurdering av konsekvenser
<p>Bestemmelsene i personopplysningsforskriften om informasjonssikkerhet gjelder som utfyllende bestemmelser til denne forskriften.</p>	Ingen spesielle

### **Kapittel III Krav om system for utstedelse av autorisasjoner og krav til autentisering**

§ 9 Krav om system for administrering av autorisasjoner	Vurdering av konsekvenser
<p>Den databehandlingsansvarlige skal <b>etablere nødvendige organisatoriske og tekniske tiltak for tildeling, administrasjon og kontroll av autorisasjoner</b>. Autorisasjonen skal bidra til å sikre at informasjonssikkerheten, herunder bestemmelsene om taushetsplikt og pasientens rett til konfidensialitet, blir ivaretatt.</p> <p>Den enkelte autorisasjon skal bygge på konkrete risikovurderinger for urettmessig og uriktig behandling av helseopplysninger.</p>	

§ 10 Krav til tilgangsstyringen – forholdet til taushetsplikt	Vurdering av konsekvenser
<p>Den databehandlingsansvarlige skal sørge for at <b>virksomhetens tilgangsstyring sikrer og begrenser tilgangen til de helseopplysninger som er relevante og nødvendige for formålet med tilgangen</b>. Tilgangen skal vurderes og konfigureres med hensyn til:</p> <ul style="list-style-type: none"> <li>- <b>antall registrerte</b> det gis tilgang til</li> <li>- <b>mengde informasjon</b> om den enkelte det gis tilgang til og</li> </ul>	<p>Antall registrerte omhandler antall pasienter den autoriserte skal få tilgang til.</p> <p>Mengde informasjon omhandler hvor mye av pasientens journal den autoriserte skal få tilgang til.</p> <p>I sin ytterste konsekvens kan denne type begrensning føre til at en</p>

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre



<p>- <b>varighet</b> av tilgangen.</p> <p>Enhver autorisasjon skal være tidsbegrenset og bare omfatte slik behandling av helseopplysninger som er relevant og nødvendig for å nå det angitte formålet med tilgangen. Den enkelte tjenesteyters behov for den aktuelle autorisasjonen i tjenesten skal vurderes og oppdateres jevnlig.</p> <p>Virksomheten skal dokumentere vurderingene etter andre ledd. Dokumentasjonen skal inngå i virksomhetens internkontrollsystem.</p>	<p>behandler ikke kan behandle en gitt pasient siden han har for mange pasienter i ft begrensningen, noe som kan gå på bekostning av pasienters liv og helse.</p> <p>Hvis begrensningen opprettholdes i forskriften, kreves det kategorisering og struktur i journalen for å kunne oppfylles.</p> <p>Varighet – autorisasjoner skal være tidsbegrenset og kan ha en varighet på 1-2 år for ansatte med faste gjøremål i en stabil virksomhet. Endringer i ansettelsesforhold eller organisasjon skal medføre revurdering av tildelte autorisasjoner. Dette fordrer en mer aktiv bruk av FRESH.</p>
--	--

§ 11 Vilkår for utstedelse av autorisasjon	Vurdering av konsekvenser
<p>Autorisasjon kan bare gis i den grad det er nødvendig for tjenesteyters arbeid, er begrunnet i tjenstlige behov og tilfredsstillende bestemmelser om taushetsplikt. <b>Grunnlaget for tilgangen skal dokumenteres.</b></p> <p>Ingen kan autoriseres for tilgang til helseopplysninger i videre omfang enn det som følger av reglene om taushetsplikt i helsepersonelloven.</p>	<p>Autorisasjon og dokumentasjon av grunnlag for autorisasjon er i dag fragmentert i flere fagsystemer og registre.</p> <p>En autorisasjonsløsning og forvaltning som er overgripende for de (mange) fagsystemene vil være nødvendig.</p>

§ 12 Krav om opplæring	Vurdering av konsekvenser
<p>Den databehandlingsansvarlige skal sørge for at enhver som gis autorisasjon, får nødvendig opplæring og informasjon om hvordan autorisasjonen skal brukes, og om dens begrensninger og muligheter. Opplæringen skal som hovedregel gis før autorisasjon utstedes, eller i spesielle tilfelle så snart som mulig etter at autorisasjonen er utstedt. Opplæringen skal gjentas slik at kunnskapen holdes ved like.</p>	<p>Opplæring av ansatte gjennom eLæring ved ansettelse, sikkerhetstesting og regelmessig godkjenning kan være et relevant tiltak og bør kunne etableres som nasjonal standard og tjeneste. eLærings systemet kan kobles til identitetsforvaltning for knytte dokumentert opplæring til den enkelte ansatte.</p>

§ 13 Krav om autentisering	Vurdering av konsekvenser
<p>Enhver som gis autorisasjon, skal entydig identifiseres som en bestemt tjenesteyter i en bestemt rolle</p>	<p><i>"Autentisering = prosess som gjennomføres for å bekrefte en påstått identitet."</i></p> <p>En (nasjonal?) IAM strategi med tilhørende kompetansebygging, forvaltningsregime og "governance" blir kritisk for helseforetakene for å oppfylle</p>

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

	<p>kravene om entydig identifisering inn i alle berørte systemer og registre.</p> <p>Tjenesteyter og rollebegrepene er upresise og spesielt rollemodell og -begreper er kompliserte og det finnes ingen omforent standard eller løsning i virksomhetene i dag.</p>
--	--

§ 14 Autorisasjon for ytelse av helsehjelp (utdrag)	Vurdering av konsekvenser
<p>Autorisasjon kan gis til helsepersonell som har behov for det for å kunne yte forsvarlig helsehjelp til pasient. <b>Autorisasjonen skal gis det innhold som er nødvendig</b> for at helsepersonellet skal kunne ivareta sine oppgaver og sitt ansvar ovenfor pasienten på en forsvarlig måte.</p> <p><b>Direkte tilgang til helseopplysninger i ekstern virksomhet</b>, jf. forskriften kapittel V, <b>krever at det i eget system er en eksplisitt mulighet til å autorisere en bruker for rett til å forespørre informasjon i ekstern virksomhet.</b></p>	<p>Kravene om et eget system for eksplisitt å autorisere en brukers rett til å forespørre informasjon i ekstern virksomhet, indikerer en SAML/federeringsløsning utviklet med tjenester som er tilpasset spesifikke krav i forskriften.</p> <p>Disse kravene er knyttet til teknisk håndheving av avtaler mellom virksomheter, autorisasjon, håndtering av samtykke, logging og bruk av tilgang, samt utlevering av tilgangsløgg til pasient.</p>

§ 15 Autorisasjon for administrering av helsehjelp	Vurdering av konsekvenser
<p>Autorisasjon kan gis til personell i pasientadministrasjonen som har behov for det for å kunne administrere helsehjelp til pasient, jf. helsepersonelloven § 26 andre ledd</p>	<p>Ingen spesielle</p>

§ 16 Autorisasjon for ytelse av nødvendige støttefunksjoner	Vurdering av konsekvenser
<p>Personell som skal bistå med elektronisk bearbeiding av opplysninger, eller som bistår med service og vedlikehold av utstyr, jf. helsepersonelloven § 25 andre ledd, kan bare gis autorisasjon i den grad det er nødvendig for å ivareta den aktuelle oppgaven.</p>	<p>Fra merknadene: I praksis må derfor slikt personell i noen tilfeller ha ganske <b>vide</b>, men <b>svært tidsbegrenset</b> autorisasjoner, når det gjelder hvilke journalopplysninger vedkommende kan få tilgang til. Det er <b>spesielt viktig at disse autorisasjonene blir registrert og fulgt opp med kontroll av hvordan autorisasjonen blir benyttet</b>, jf. forskriften § 33.</p> <p>Krav til IAM strategi og implementering av denne bør settes opp med spesielle krav til servicepersonell/støttefunksjoner.</p>

§ 17 Krav om register over og kontroll av autorisasjoner	Vurdering av konsekvenser
<p>Den databehandlingsansvarlige skal <b>føre et register over utstedte autorisasjoner (autorisasjonsregister)</b>. Registeret skal inneholde informasjon om hvem som er</p>	<p>Dette registeret og forvaltningsrutiner omkring dette bør bygges på og videreutvikles omkring FRESH og</p>

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre



tildelt autorisasjon, til hvilken rolle autorisasjonen er tildelt, formålet med den, tidspunktet for når den ble gitt, varighet og om et eventuelt tilbakekall av autorisasjonen.	masterdata fra (lønn og) personalsystemet.
---	--

## Kapittel IV Tilgang til helseopplysninger i behandlingsrettet helseregister

§ 18 Krav om autentisering og bruk av autorisasjonen	Vurdering av konsekvenser
<p>Enhver som gis elektronisk tilgang til helseopplysninger skal autentisere seg som en bestemt person i en bestemt rolle.</p> <p>Ingen kan gjøre bruk av en tildelt autorisasjon i videre omfang enn det som følger av reglene om taushetsplikt.</p>	<p>Formålet med paragrafen er å kunne spore på individ for å kunne gjennomføre kontroller på hvorvidt en autorisert bruker retten til tilgang videre enn nødvendig..</p>

§ 19 Tilgang til helseopplysninger for ytelse av helsehjelp	Vurdering av konsekvenser
<p>Helsepersonell som yter helsehjelp til pasient, har <b>bare tilgang til helseopplysninger som er nødvendige og relevante for å kunne yte helsehjelpen</b>. Tilgangen skal følge av en konkret beslutning om å yte helsehjelp til pasienten. Dette samme gjelder for helsepersonells medhjelpere, elever og studenter, jf. § 14 tredje og fjerde ledd.</p> <p>Helsepersonell som på selvstendig grunnlag kan treffe beslutning om helsehjelp, kan gis elektronisk tilgang til nødvendige og relevante helseopplysninger om de pasienter vedkommende tjenesteyter har rett og plikt til å treffe slik beslutning om. <b>Det skal fremgå av journalen hvem som har truffet beslutningen.</b></p> <p>Tilgangen til helseopplysninger etter denne bestemmelsen <b>varer så lenge det er nødvendig for helsehjelpen.</b></p> <p>Tilgangen til helseopplysningene gjelder bare dersom pasienten ikke har motsatt seg eller motsetter seg at tilgang til de aktuelle opplysninger gis, så fremt tungtveiende grunner ikke tilsier noe annet, jf. pasientrettighetsloven 5-3.</p>	<p>Igjen er det den helhetlige løsningen og kontrollen med:</p> <ol style="list-style-type: none"> <li>1. identifisering av helsepersonell (autentisering)</li> <li>2. beslutning om å yte helsehjelp – dokumentert</li> <li>3. autorisasjon for tilgang til opplysninger (i flere systemer)</li> <li>4. Hvem som autoriserer skal logges (har truffet beslutningen)</li> <li>5. Rollebasert tilgang (flere systemer)</li> <li>6. Tidsbegrenset tilgang (så lenge behandlingen varer)</li> </ol> <p>Denne paragrafen har omfattende merknader og stiller store krav til helserettede behandlingsregistre og registreringsdisiplin i forhold til at <i>"noen helseopplysninger fremstår som mer sensitive enn andre"</i>.</p> <p>Utdrag fra merknadene: Bestemmelsen innebærer at <b>dersom det ikke er tatt noen beslutning</b> om at en bestemt pasient skal gis helsehjelp, vil helsepersonell <b>ikke ha lovlig tilgang til registrerte opplysninger</b> om vedkommende</p>

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

	<p>pasient i henhold til denne bestemmelsen.</p> <p>Bestemmelsen <b>forskriftsfester såkalt beslutningsstyrt tilgang</b>: Når det treffes en beslutning om å yte helsehjelp til pasient og denne beslutningen registreres, <b>innebærer det samtidig en registrering av hvor denne helsehjelpen skal tilbys og herunder hvilke helsepersonell man forventer vil bli delaktig i ytelse av helsehjelpen.</b></p> <p><b>Hvor mange tjenesteytere som vil få tilgang</b> til helseopplysninger ved beslutningsstyrt tilgang vil blant annet bero på hvordan tilgangsstyringen konfigureres.</p>
--	---

§ 20 Tilgang til helseopplysninger for administrering av helsehjelp	Vurdering av konsekvenser
<p>Personell som administrerer helsehjelp, har bare tilgang til de pasientadministrative helseopplysninger som er nødvendige og relevante for å kunne administrere hjelpen, jf. helsepersonelloven § 26 andre ledd.</p> <p>§ 19 andre, tredje og fjerde ledd gjelder tilsvarende for personell i pasientadministrasjonen.</p>	<p>Første ledd gir personell som administrerer helsehjelp til pasient elektronisk tilgang til de pasientadministrative opplysninger som er nødvendige og relevante for å kunne administrere helsehjelpen.</p> <p>Dette setter krav til å kunne skille på type informasjon i systemene – krever bl.a. strukturert og klassifisert journal.</p>

§ 21 Tilgang til helseopplysninger for personell med støttefunksjoner	Vurdering av konsekvenser
<p>Personell som skal bistå med elektronisk bearbeiding av opplysninger, eller som bistår med service og vedlikehold av utstyr, jf. helsepersonelloven § 25 andre ledd, har bare tilgang til de helseopplysninger som er nødvendig for å kunne ivareta den aktuelle oppgaven.</p>	<p>Se under §16</p>

## ***Kapittel V Tilleggsbestemmelser for direkte tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter***

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

§ 22 Avtale om direkte lesetilgang til helseopplysninger på tvers av virksomheter	Vurdering av konsekvenser
<p>Helsepersonell som ikke står under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet kan, dersom det på forhånd er inngått en avtale om det, gis direkte lesetilgang til helseopplysninger i behandlingsrettet register virksomheten er ansvarlig for. Avtale om lesetilgang kan bare inngås for tilfeller der formålet med tilgangen er ytelse av helsehjelp til pasient, og kan bare omfatte strukturerte helseopplysninger som er relevante og nødvendige for å nå formålet med behandlingen av dem. Det kan bare gis tilgang til opplysninger som det på forhånd er vurdert kan deles med annet helsepersonell som skal yte eller yter helsehjelp til pasienten. 72</p> <p>Det skal fremgå av avtalen hvilke formål (type helsehjelp) avtalen gjelder og hvilke forutsetninger som ligger til grunn for avtalen, herunder også hvilke tekniske løsninger som skal benyttes ved slik tilgang.</p> <p>Avtale som nevnt i første og andre ledd, inngås mellom den virksomhet som har databehandlingsansvaret for behandlingen av opplysningene og den virksomhet som gis lesetilgang til opplysningene.</p>	<p><a href="#">Minstekrav til EPJ-systemer.</a></p> <p>Utdrag fra merknadene: Bestemmelsen fastslår at avtalen bare kan omfatte <b>strukturerte helseopplysninger som på forhånd er vurdert å kunne deles</b> med annet helsepersonell.</p> <p>For at dette skal kunne etterleves er det flere forutsetninger som må på plass – blant annet:</p> <ul style="list-style-type: none"> <li>- Journalsystemene må kunne klassifisere og merke delbar informasjon (strukturert og markert)</li> <li>- Avtalen mellom foretak er tett knyttet til teknisk løsning</li> <li>- Logging av forespørsler må kunne gjøres per ansatt og per registrert pasient</li> </ul>

§ 23 Avtale om skrive-tilgang på tvers av virksomheter	Vurdering av konsekvenser
<p>Dersom det er nødvendig for å utføre formålet med lesetilgang i medhold av § 22, kan det for særskilte områder avtales at helsepersonell som i en bestemt rolle gis slik tilgang, skal kunne registrere bestemte anmerkninger i det behandlingsrettede helseregister det er gitt tilgang til. Dette gjelder bare i de tilfeller der anmerkningen er nødvendig med tanke på helsehjelpen pasienten skal tilbys. Anmerkningen skal kunne føres tilbake til navngitt person.</p>	<p>Krav til autorisasjon og logging i journalsystemet i virksomheten det skrives tilbake til blir en utfordring og setter store krav til IAM løsning og journalsystem.</p> <p>Tilgang på tvers av virksomheter vil kreve en ID Federeringsløsning, og journalen må kunne logge hvilken virksomhet og ansatt/identitet som har gjort endringen.</p>

§ 24 Forutsetninger for å kunne inngå avtale om direkte tilgang til helseopplysninger på tvers av virksomheter	Vurdering av konsekvenser
<p>Avtale som nevnt i §§ 22 og 23 kan bare inngås dersom begge virksomheter har tekniske løsninger som kan avgrense tilgangen til å omfatte strukturert og</p>	<p>Fra merknadene: <i>Det kreves at journalføringen <b>kan struktureres og er strukturert på en slik måte at det er mulig</b></i></p>

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

<p>forhåndsvurdert klinisk informasjon om en navngitt person relatert til forespørselen.</p> <p>Avtale som nevnt kan videre bare inngås dersom gjennomføring av den ikke svekker informasjonssikkerheten ved behandling av helseopplysninger ved noen av virksomhetene. Begge parter i avtalen må være kjent med den andre partens sikkerhetsmål og sikkerhetsstrategi</p>	<p><b>å bare gi tilgang til et avgrenset sett av klinisk informasjon - som før tilgang gis er vurdert at kan deles med annet helsepersonell i ekstern virksomhet ved direkte tilgang.</b></p> <p>Dette setter krav til strukturerte journaler som i dag ikke eksisterer i spesialisthelsetjenesten. Utvikling av dagens løsninger eller skifte av slike løsninger er tunge endringsprosjekter og vil ikke kunne gjennomføres innen 1-2 år.</p> <p><i>En forutsetning for å inngå avtale, er at begge parter i avtalen er kjent med hverandres sikkerhetsmål og sikkerhetsstrategi. Dette medfører en praktisk utfordring så lenge det ikke finnes et omforent sikkerhetsnivå og en form for sertifisering av virksomhetenes sikkerhet som sikrer nødvendig tillitsforhold.</i></p> <p><b>Det er først og fremst der meldingsutveksling ikke er godt nok, at avtale om tilgang på tvers av virksomhetsgrenser bør inngås.</b></p> <p>Med de samlede kravene som er oppstilt vil det være svært langt frem før direkte tilgang på tvers kan benyttes som hovedregel, og bare unntaksvis vil direkte tilgang på tvers anvendes. Konsekvensene er fortsatt duplisering av data og et fortsatt regime hvor det ikke er mulig å ha oversikt over pasientens samlede og sist oppdaterte opplysninger.</p>
--	--

§ 25 Krav til autentisering	Vurdering av konsekvenser
<p>Enhver som gis tilgang til helseopplysninger i et behandlingsrettet helseregister ved en ekstern virksomhet, skal autentisere seg ved bruk av kvalifisert sertifikat.</p>	<p>Fra merknadene: <i>Bestemmelsen fastslår at enhver som gis tilgang til helseopplysninger i et behandlingsrettet helseregister i ekstern virksomhet, §§ 22 og 23, skal autentisere seg ved bruk av kvalifisert sertifikat.</i></p> <p>Bruk av kvalifisert sertifikat (personlig) innføres i.f.m eResept slik at basis infrastruktur vil bli tilgjengelig for leger med forskrivningsrett. Utvikling av federert identitetsløsning og integrasjon</p>

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

	<p>med PKI løsning vil måtte gjennomføres.</p> <p>Mulig (tidsbegrenset) unntak er når de samarbeidende virksomhetene har journalsystemet i samme løsning.</p>
--	---

§ 26 Krav til forespørselen m.m.	Vurdering av konsekvenser
<p>En forespørsel om og direkte tilgang til helseopplysninger i annen virksomhet skal skje via autorisasjons- og autentiseringsmekanismer i regi av egen virksomhet. Forespørselen og tilgangen til helseopplysninger kan bare omfatte en <b>person</b> om gangen. Forespørselen samt <b>beslutningen om å etterkomme den, eller ikke</b>, skal registreres. Ved behov for gjentatt tilgang til helseopplysninger om samme pasient skal det gjøres en ny forespørsel.</p>	<p>Det er uklart om bruk av <b>person</b> gjelder den ansatte/tjenesteyter eller pasient i denne formuleringen. (må avklares i høringsrunden)</p> <p>Det er også uklarerheter om hva som ligger i beslutningen om å etterkomme forespørsel eller ikke krever manuell godkjenning for hver forespørsel – dersom det kreves en manuell/aktiv godkjenning for hver forespørsel vil det kraftig begrense anvendelse av tilgang på tvers. En føderert identitetsløsning vil kunne automatisere registrering og logging.</p> <p>Fra merknadene: <i>Det følger av bestemmelsen at dersom helsepersonellet som har ekstern lesetilgang <b>ikke lenger yter eller skal yte helsehjelp til pasienten</b>, pasienten er for eksempel utskrevet eller flyttet, skal det heller <b>ikke lenger være mulig for vedkommende helsepersonell å forespørre om tilgang til helseopplysninger i den eksterne virksomheten.</b></i></p> <p>En løsning som støtter tilgang på tvers av virksomheter må inneha sjekk mot det pasientadministrative systemet for å avgjøre om det fortsatt ytes helsehjelp til pasienten.</p>

§ 27 Krav om samtykke	Vurdering av konsekvenser
<p>Direkte tilgang til helseopplysninger på tvers av virksomheter kan bare gis etter uttrykkelig, informert og frivillig samtykke fra den registrerte. Samtykket skal dokumenteres.</p>	<p>Samtykke skal kunne registreres i journalsystemet både i den virksomheten som ber om tilgang og den virksomheten som gir tilgang. Krav om at samtykke når</p>

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

	som helst kan trekkes tilbake (og at dette da skal registreres i flere systemer) vil sette krav som høyst sannsynlig best vil kunne løses med en nasjonal samtykkeløsning. (Altinn har etablert en slik)
--	--

§ 28 Unntak fra krav om at samtykke skal være uttrykkelig	Vurdering av konsekvenser
Kravet om at samtykket skal være uttrykkelig kan fravikes dersom pasienten på grunn av sin fysiske eller psykiske tilstand ikke er i stand til å gi et slikt samtykke, og det må antas at pasienten ville ha gitt uttrykkelig samtykke dersom han eller hun hadde vært i stand til det. Det skal fremgå av det aktuelle registeret at uttrykkelig samtykke ikke er gitt, og begrunnelsen for det.	Krav om at beslutninger om unntak fra samtykke skal dokumenteres vil også kreve løsning som under § 27

## Kapittel VI Sperring av helseopplysninger

§ 29 Sperring av helseopplysninger	Vurdering av konsekvenser
<p>Dersom den registrerte har motsatt seg eller motsetter seg at andre får tilgang til helseopplysninger, jf. helsepersonelloven §§ 25 og 45, skal opplysningene sperres.</p> <p>Den registrerte kan bestemme om sperringen kun skal gjelde bestemte personer, om de sperrede opplysningene bare skal være tilgjengelige for den eller de den registrerte selv bestemmer, eller om de bare skal være tilgjengelig etter samtykke.</p> <p>Dersom de opplysninger den registrerte krever sperret antas å være påtrengende nødvendig for å yte forsvarlig helsehjelp i en akutt situasjon, skal det fremgå av journalen at det er registrert opplysninger som er sperret.</p>	<p>Fra merknadene: <i>Bestemmelsen åpner for at den registrerte kan bestemme om sperringen kun skal gjelde bestemte personer, om de sperrede opplysningene bare skal være tilgjengelige for den eller de den registrerte selv bestemmer, eller om de bare skal være tilgjengelig etter samtykke.</i></p> <p>Har journalsystemene støtte for en slik tredeling av sperremekanismer?          a)eksplisitt sperre, b)implisitt sperre og c)generell sperre.</p> <p>Det er også krav om at man kan sperre mot innsyn i deler av journalen – krever kategorisering og struktur.</p>

§ 30 Tilgang til sperrede opplysninger	Vurdering av konsekvenser
Tilgang til sperrede opplysninger kan skje dersom tungtveiende grunner taler for det, jf. pasientrettighetsloven § 5-3.	Ingen spesielle



## Kapittel VII Krav om logging og dokumentasjon av tilgang

§ 31 Krav om dokumentasjon av tilgang	Vurdering av konsekvenser
<p>Alle tilfeller av tilgang til opplysninger i et behandlingsrettet helseregister skal automatisk dokumenteres i registeret. Dokumentasjonen skal inneholde informasjon om:</p> <p>a) navn, rolle og organisatorisk tilhørighet til den som har fått tilgang</p> <p>b) grunnlaget for tilgangen</p> <p>c) det tidsrom vedkommende har hatt tilgang til opplysningene.</p>	<p>Fra merknadene: <i>Bestemmelsen krever at det i behandlingsrettede helseregistre skal finnes dokumentasjon av <b>hvem som har hatt tilgang til opplysningene i registrene</b>, i hvilket tidsrom den enkelte har hatt tilgang, og hva som er <b>grunnlaget for tilgangen</b>. Det er ikke nok bare å skrive helsehjelp. Type helsehjelp må angis.</i></p> <p>Her er det litt uklart om det menes de som har hatt tilgang (en rolle er i praksis en gruppe brukere = kan være mange) eller om det er de som faktisk har gjort oppslag eller endringer i helseregisteret.</p> <p>Ut fra krav om dokumentasjon til pasient er det antagelig det siste:</p> <p><i>Ettersom dokumentasjonen vil være betydelig mer oversiktlig enn registreringer i hendelsesregistrene, kan det antas at den vil være et godt hjelpemiddel for pasienter som ønsker å få <b>klarlagt om noen uberettiget har tilegnet seg opplysninger i journalen</b>. Dokumentasjonen etter denne bestemmelsen er en del av "pasientens journal" 64</i></p> <p>og berøres ikke av at korresponderende bestemmelser i hendelsesregisteret, jf. forskriften § 32, blir slettet etter 2 år.</p>

§ 32 Krav om hendelsesregistrering/logg	Vurdering av konsekvenser
<p>For å avdekke uautorisert tilgang til opplysninger i behandlingsrettede helseregistre, eller forsøk på slik tilgang, skal den databehandlingsansvarlige sørge for at det lagres hendelsesregistre over uautoriserte forsøk på pålogging til systemer som benyttes til å behandle helseopplysninger og over autoriserte pålogginger til slike systemer.</p> <p>Videre skal hvert enkelt tilfelle av tilgang til helseopplysninger fra et behandlingsrettet helseregister registreres i et hendelsesregister med dokumentasjon</p>	<p>Fra merknadene: <i>Første ledd krever at det lagres hendelsesregistre over uautoriserte forsøk på pålogging til systemer som inneholder helseopplysninger og over autoriserte pålogginger til slike systemer. For å oppfylle dette formålet må virksomheten ha flere hendelsesregistre, jf. flertallsformen. Hendelsesregistrene etter denne paragrafen er ikke en del av den enkelte pasients</i></p>

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

<p>av:</p> <p>a) entydig identifikasjon av den som har fått tilgang          b) stedet hvor vedkommende har vært pålogget fra          c) referanse til de opplysninger det er gitt tilgang til          d) hvilke systemer vedkommende har benyttet mens han eller hun var pålogget          e) det tidsrom vedkommende har hatt tilgang til opplysningene.</p> <p>Hendelsesregistrering som nevnt skal skje uavhengig av om opplysningene ble gitt tilgang til for å leses på skjerm, skrives ut eller for å være gjenstand for andre former for behandling.</p> <p>Hendelsesregistre som skal kunne sammenstilles med virksomhetens autorisasjonsregister, jf. § 17, og med register eller liste over tilstedeværelse av personell.</p> <p>Dokumentasjonen som registreres kan slettes etter 2 år.</p>	<p><i>journal/behandlingsrettede helseregister.</i></p> <p><i>Andre ledd stiller krav om hvilken informasjon som skal registreres i et hendelsesregister. Stikkordsmessig kan dette oppregnes i: <b>hvem – hvorfra – hvorfor - hva og når</b></i></p> <p>Det er noen uklarheter (spesielt i punkt b), men det stilles relativt mange, detaljerte og utfordrende krav til systemstøtte for logging og behandling av logger.</p> <p>For at effektiv logging skal kunne realiseres må krav til loggdata være entydige og konkrete ovenfor (journal) leverandørene.</p> <p>Innsamling og behandling av logger bør gjøres av spesialiserte systemer (og kompetanse) hvor formål og kravspesifikasjon er gjennomarbeidet før implementering.</p>
---	--

§ 33 Oppfølging og kontroll av elektronisk tilgang	Vurdering av konsekvenser
<p>Den databehandlingsansvarlige skal jevnlig kontrollere hvem som har hatt elektronisk tilgang til helseopplysninger i et behandlingsrettet helseregister. Dersom gjennomgang av kontrollen viser at det har skjedd en urettmessig tilegnelse av helseopplysninger, skal Datatilsynet informeres, jf. personopplysningsforskriften § 2-6. Videre skal pasienten opplysningene er knyttet til informeres.</p>	<p>Dette gjennomføres i svært liten grad i dag, og krever en helt annen systemstøtte og kvalitet på forvaltningsregime for å kunne gjennomføres effektivt. For å kunne foreta jevnlig kontroll kreves enten en stor manuell innsats/ressursbruk eller automatiserte kontroller. Selv om det sistnevnte er utredet i noen sammenhenger, er det mange utfordringer knyttet til at automatisk kontroll kan gi for mange positive treff, dvs. at helsepersonell/ansatte blir feilaktig beskyldt for snoking, eller at for få tilfeller blir avdekket, noe som gir et falskt bilde av at kontrollen er god.</p>

§ 34 Innsynsrett i logg og annen dokumentasjon av tilgang	Vurdering av konsekvenser
Den registrerte har rett til innsyn i dokumentasjon som gir	Utskrift av tilgangslogger til pasienten er

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

<p>informasjon om behandling av helseopplysninger som kan knyttes til vedkommende. For å gjøre tilgangsløkken forståelig for den registrerte skal det ved innsyn eller utskrift foretas sammenstilling med virksomhetens autorisasjonsregister og det behandlingsrettede helseregister tilgangsløkken gjelder. Sammenstillingen skal som et minimum inneholde følgende opplysninger:</p> <p>a) navn, rolle og organisatorisk tilhørighet til den som <b>har hatt tilgang</b></p> <p>b) tidspunkt for den enkelte tilgang</p> <p>c) hvilken <b>type opplysninger</b> det ble gitt tilgang til ved <b>det enkelte tilfelle</b></p> <p>d) registreringsdato for den enkelte opplysning det er gitt tilgang til ved det enkelte tilfelle.</p> <p>Den registrerte har krav på en kortfattet forklaring av tekniske uttrykk og lignende dersom vedkommende ber om det. Den registrerte har også rett til å få utskrift av dokumentasjonen. Ved utskrift skal det kunne foretas sortering i henhold til den registrertes ønske.</p> <p>Forespørsel om innsyn og rett til utskrift av dokumentasjon som nevnt skal besvares uten ugrunnet opphold og senest innen 30 dager etter henvendelsen kom inn.</p> <p>Det kan ikke tas vederlag for utskrift av dokumentasjon etter denne bestemmelsen med mindre særlige forhold tilsier det.</p>	<p>en effektiv og allmennpreventiv måte å bedre sikkerhetsbevissthet hos ansatte og tilliten hos pasienten (forutsatt god og riktig dokumentasjon).</p> <p>Det er tre utfordringer i de formuleringene som er brukt:</p> <ol style="list-style-type: none"> <li>1. har <b>hatt tilgang</b>, eller <b>har brukt tilgangen</b>?</li> <li>2. type opplysninger krever klassifisering og struktur i journalen</li> <li>3. det enkelte tilfelles – per oppslag eller så lenge helsehjelpen ytes?</li> </ol>
--	--

## Kapittel VIII Avsluttende bestemmelser

§ 35 Straff	Vurdering av konsekvenser
<p>Den som forsettlig eller grovt uaktsomt overtrer bestemmelsene i forskriften straffes med bøter eller fengsel inntil ett år eller begge deler.</p>	<p>Liten direkte betydning for virksomhetsarkitektur, men <b>foretaksledelsen ansvarliggjøres</b> og kan få inntil ett års fengsel eller bøter ved grov uaktsomhet eller forsettlighet.</p>
§ 36 Ikrafttredelse	Vurdering av konsekvenser
<p>Forskriften trer i kraft fra det tidspunkt departementet bestemmer. En beslutning om ikrafttredelse kan omfatte hele eller deler av helsetjenesten. Departementet kan også beslutte at de enkelte bestemmelser i forskriften skal tre i kraft til forskjellig tid. Alle bestemmelsene i forskriften kapittel V må settes i kraft samtidig.</p>	<p>Slik forskriften er oppstilt vil det antagelig ta minst ett år før spesialisthelsetjenesten har oversikt over alle konsekvensene og kan ha en innføringsplan som er noenlunde realistisk.</p>

Høringsuttalelse -

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre