HELSE VEST

Besøksadresse:
Nådlandskroken 11,
4034 Stavanger

Postadresse:
Postboks 303, Forus
4066 Stavanger
Org.nr. 983 658 725

Tlf.: 51 96 38 00
Faks: 51 96 38 01
helse@helse-vest.no
www.helse-vest.no

Helse- og omsorgsdepartementet

Postboks 8011 Dep
0030 Oslo

Vår ref.:	Deres ref.:	Saksbehandler:	Dato:
2010/248 - 3952/2010		Åsmund Norheim, 51 96 38 08	19.09.2010

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

Helse Vest RHF viset til departementets brev av 3. juni 2010, ref 201001921-/ASD, og takker for anledningen til å gjennomgå høringsnotatet *Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre.* Vi setter stor pris på at Helse- og omsorgsdepartementet med dette forskriftsforslaget setter fokus på et viktig, men vanskelig område.

Helse Vest RHF har forelagt høringsnotatet for helseforetakene i vår region og vårt IKT-selskap, Helse Vest IKT AS. Tre av foretakene har gitt skriftlige tilbakemeldinger som danner grunnlag for Helse Vest sin uttalelse. I tillegg har Helse Vest deltatt i et samarbeid på tvers av RHFene, for på den måten å søke å oppsummere sentrale momenter i de respektive RHF-uttalelsene som man er omforent om.

Helse Vest sin uttalelse vil bestå av en oppsummering av disse sentrale momentene. I tillegg har vi valgt å vedlegge uavkortet de skriftlige uttalelsene som foreligger fra henholdsvis Helse Bergen HF, Helse Stavanger HF og Helse Fonna HF. Når det gjelder uttalelsen fra Helse Bergen, har både Helse Vest RHF og Helse Vest IKT hatt anledning til å kommentere denne i forkant. Helse Vest slutter seg fullt ut til uttalelsen slik den nå foreligger, og vi ber om at den blir behandlet som Helse Vest sin uttalelse sammen med dette oversendelsesbrevet.

Forslaget til forskrift søker å tydeliggjøre rettigheter og begrensninger for pasienter og helsepersonell i forhold til opplysninger i, og tilgang til, elektroniske pasientjournaler. Det er utvilsomt behov for en forskrift for å klargjøre disse områdene. Selv om Helse Vest RHF, i likhet med de øvrige RHFene, støtter intensjonen med forskriftsforslaget, har vi en del kommentarer, samt enkelte forslag til endringer og presiseringer. Disse kommentarene og forslagene er knyttet til form, begrepsbruk og definisjoner, ivaretakelse av pasientsikkerhet og behovet for å kunne utføre helsetjenester, og praktiske implikasjoner. I tillegg er det knyttet kommentarer til noen enkeltparagrafer, disse kommentarene utdypes i underliggende høringsuttalelse. Helseforetakene vil påpeke at forskriften vil kunne ha store implikasjoner for mange pasienter, samt ha praktiske implikasjoner for helsepersonells hverdag i sektoren. En felles og entydig anbefaling fra helseforetakene er derfor at man svært nøye må se på de praktiske implikasjoner av alle sider ved forskriften før den vedtas. Spesielt bør det avdekkes om praktiske implikasjoner av forskriften kan sette liv og helse i fare. Forskriftsarbeidet trenger å suppleres med en tydelig og praktisk rettet konsekvensvurdering.

Form, begrepsbruk og definisjoner

Helseforetakene etterlyser en konsistent og tydelig plassering av denne forskriften i forhold til gjeldende regelverk. I dagens utkast er det eksempelvis uklart i hvilken grad forskriften er underlagt, sideordnet, overordnet, utdypende, supplerende eller erstattende til annet regelverk. Uklarhet av denne karakter vil

være krevende å håndtere dersom forskriften iverksettes. Forskriften er i dag svært detaljert på en rekke områder som alt er dekket annet sted i lovverket. Samtidig opplyses det i § 8 om at bestemmelsene i personopplysningsforskriften om informasjonssikkerhet gjelder som utfyllende bestemmelser til forelagt forskrift.

Vi oppfatter forslaget til forskrift som tidvis overordnet, tidvis svært detaljert. Eksempelvis behandles krav om logging og dokumentasjon av tilgang meget detaljert i forskriftens kapittel VII. Helseforetakenes oppfatning er at det ikke bør settes krav til logging utover det som er praktisk gjennomførbart.

I tillegg vil vi påpeke at ord- og begrepsbruk til tider er noe uensartet, eksempelvis brukes ordene god, god nok, forsvarlig og tilfredsstillende om hverandre for å beskrive kvaliteten på informasjonssikkerhet. Begrepet "strukturert" slik det benyttes i § 22 bør defineres tydelig. Uensartet ord- og begrepsbruk kan skape uklarhet.

Ivaretakelse av pasientsikkerhet og behovet for å kunne utføre helsetjenester

Utviklingen i helsesektoren går mot økt samhandling, og en kombinasjon med økt spesialisering og økt tilgjengeliggjøring av spisskompetanse til en større andel av pasientmassen. Disse utviklingstrekkene belyses i samhandlingsreformen. Det er videre et sterkt fokus på effektiv og forsvarlig pasientbehandling. Det er viktig at forskriften legger til rette for en fortsettelse av denne utviklingen. I sin nåværende form oppleves forskriftsforslaget til en viss grad å legge begrensninger på dette. Dersom regelveket ikke balanserer hensynet til tilgjengelige helseopplysninger og ivaretakelse av konfidensialitet vil det ikke optimalt bidra til lovgivers intensjon om forsvarlig og effektiv pasientbehandling samtidig som taushetsplikten ikke svekkes.

Et spesifikt behov det pekes på fra spesialisthelsetjenesten er helsepersonells behov for, i etterkant av behandling, å gå tilbake til tidligere egne pasienters journal for å kunne kvalitetssikre, sammenligne og lære av erfaringer. Uten dette vil helsepersonell ha mindre mulighet for elementær kvalitetssikring og kompetanseheving. Feil og mangler vil da i de fleste tilfeller kun kunne avdekkes ved alvorlige brudd som tilsynssaker, klagesaker etc. På denne bakgrunn finner vi ikke at § 14 i tilstrekkelig grad uttrykker dette behov og avgrensning klart nok.

Praktiske implikasjoner av forslag til forskrift

Underliggende høringsuttalelse fra Helse Bergen gjennomgår de ulike paragrafer i fremlagt forskriftsforslag i større detalj. Helseforetakene ønsker i tillegg å peke på enkelte deler av forskriften som kan innebære uheldige praktiske implikasjoner og muligens en vanskeliggjøring av helsetjenestens daglige arbeid. Dette er momenter som har blitt diskutert på tvers av RHFene og som det hersker bred enighet rundt.

Helseforetakene reagerer på at alle deler av forskriften skal gjelde alle behandlingsrettede registre. Helseforetakene har en lang rekke systemer som inneholder personidentifiserbar informasjon om pasienter og som benyttes for å yte helsehjelp eller administrere slik hjelp, og det er viktig å påpeke at omfanget, rekkevidden og kompleksiteten av disse systemene varierer sterkt. Å sette samme krav til alle disse svært ulike systemene vil være uheldig. Dette synet vil bli utdypet i underliggende høringsuttalelse. Systemsikkerhet må isteden relateres til risikovurderinger og til akseptabelt risikonivå i tråd med personopplysningsloven og personopplysningsforskriften.

I merknaden til § 9 settes det krav til helsefaglig kompetanse for helsepersonell som gis myndighet til å treffe beslutning om innholdet i en autorisasjon. Helseforetakene mener at ledere må ha myndighet til å tildele autorisasjon til sine ansatte når det gjelder tilgang til systemene.

I høringsbrevet bes det særskilt om eventuelle merknader til deler av § 10. Helseforetakene oppfatter ikke kriteriene (a-c) for å vurdere tilgang som praktisk egnede. Vi foreslår i utgangspunktet å stryke disse. Dersom denne typen kriterier allikevel inkluderes foreslår vi å endre fokuset noe; "antall registrerte det gis tilgang til" bør isteden dreie seg om pasient/pasientgruppe, "mengde informasjon" bør endres til "type informasjon" og "varighet av tilgangen" bør knyttes opp mot rolle, og være hendelsesbasert

fremfor tidsbasert. Videre settes det i § 11 krav til at grunnlaget for tilgang skal dokumenteres. Det vil være svært vanskelig å etterkomme og vedlikeholde et slikt krav i praksis, og det foreslås derfor isteden å sette krav til at det er grunnlaget for autorisasjonen som skal dokumenteres, ikke tilgangen i seg selv.

Konklusjon

Høringsbrevet spesifiserer at departementet, i arbeidet med forskriften, har lagt stor vekt på å få frem et regelverk som er godt balansert mellom hensynet til rask tilgang til relevante pasientopplysninger når det er nødvendig for å yte helsehjelp til pasienten, og hensynet til pasientens rett til vern om opplysningene. Departementet ber om høringsinstansenes synspunkter på om forskriften har en slik balanse. Helseforetakene er av den oppfatning at en slik balanse i enda større grad kan oppnås dersom det i større grad fokuseres på å gjøre forskriften praktisk mer hensiktsmessig, redusere uklarheter og dermed tolkningsmuligheter, og finne et bedre samsvar mellom krav og formål.

Med hilsen

Ivar Eriksen
Eierdirektør

Vedlegg: Brev fra Helse Bergen HF datert 10.09. 2010
Brev fra Helse Stavanger HF datert 26.08. 2010
Brev fra Helse Fonna HF datert 25.08. 2010

Kopi: Helseforetakene og Helse Vest IKT

HELSE BERGEN
Haukeland universitetssjukehus

Helse Bergen HF
Forsknings- og utviklingsavdelingen

Helse Vest RHF
Postboks 303 Forus
4066 Stavanger

Dykkar ref:	Vår ref:	Saksbehandlar	Bergen,
2010/248 - 2953/2010	2010/2472	Eline Monstad, tlf. 55976539	10.09.2010

Høyring av forslag til forskrift om informasjonssikkerheit, tilgangsstyring og tilgang til helseopplysinga i behandlingsretta helseregister

Vedlagt sender vi over merknader til høyringa av den nye forskrifta. Vi reknar med at Helse Vest RHF vidaresender våre merknader til Helse- og omsorgsdepartementet.

Med vennleg helsing

Alf Henrik Andreassen
Fagdirektør
sign

Eline Monstad
Eline Monstad
IT-sikkerheitsleiar/personvernombod

Kopi: Interne bidragsytarar

Besøksadresse: Jonas Liesv 65, 5021 Bergen
Postadresse: Helse Bergen HF, 5021 Bergen
Telefon: 05300 – Telefaks: 55974785 – E-post: postmottak@helse-bergen.no – Org. nr.: 983974724

Kommentar til høring av helseregisterforskrift fra Helse Bergen HF 10.09.2010

Helse Bergen HF er enig i at det er behov for en forskrift til helseregisterloven for å klargjøre krav til informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede registre. Det er likevel nødvendig å finne frem til et bedre samsvar mellom krav og formål, redusere uklarheter og dermed tolkningsmuligheter, samt å sørge for at forskriften blir mer praktikabel. Dette vil etter vår vurdering gi bedre balanse mellom personvern og pasientsikkerhet.

Helse Bergen har innvending til at alt i forskriften skal gjelde alle behandlingsrettede registre. Forskriften tydeliggjør hva som inngår i et behandlingsrettet register og at det gjelder *alle* systemer som inneholder personidentifiserbar informasjon om pasienter og som benyttes for å yte helsehjelp eller administrere slik hjelp. Helseforetak har mange slike systemer, en god del virksomhetsomfattende større systemer - og en rekke avdelingsvise mindre systemer. Noen systemer har også flere formål. Det blir en stor utfordring, i praksis umulig, å skulle sette samme krav til alle disse svært ulike systemene. Et system med få pasienter, lite omfang av sensitiv informasjon og med en begrenset mengde brukere som har tilgang, trenger ikke samme grad av beskyttelse som et stort, virksomhetsomfattende system for å oppnå tilfredsstillende (eller forsvarlig/god/god nok) sikkerhet. Det blir feil å etablere regler som ikke er praktisk mulig å oppfylle, når systemene egentlig er sikre nok og dekker et viktig behov i forhold til pasientsikkerhet. Sikkerhet til systemer må relateres til risikovurderinger og til akseptabelt risikonivå i tråd med Personopplysningsloven og Personopplysningsforskriften, ikke til et endelig sett av detaljerte bestemmelser. Dette blir ytterligere kommentert nedenfor.

Forskriften er svært detaljert på en rekke områder som alt er dekket annet sted i lovverket. Det kan være praktisk at mest mulig samles i forskriften for oversiktens del, men det kan skape uklarheter og dermed tolkningskonflikter hvis innholdet mellom de forskjellige lovene/forskriftene ikke oppfattes som identisk. En del ord/uttrykk er brukt om hverandre i forskriftene. Eksempel: God, god nok, forsvarlig og tilfredsstillende informasjonssikkerhet. Er god sikkerhet bedre enn tilfredsstillende sikkerhet eller forsvarlig sikkerhet? Og er ikke tilfredsstillende eller forsvarlig sikkerhet god/god nok?

HOD viser i merknaden til forskriften til at all kommunikasjon ikke trenger å skje ved direkte tilgang, men at elektronisk meldingsformidling fortsatt vil være en viktig samhandlingsform, og i mange tilfeller den mest hensiktsmessige. Det er korrekt at meldingsformidling kan være formålstjenlig i mange tilfeller, men slett ikke i alle. For det første er det avhengig av at rett informasjon finnes samlet og er i egnet form for meldingsformidling. Eksempler kan være epikriser, operasjonsbeskrivelser eller andre bestemte dokumenter. Er det behov for å lete etter riktig informasjon for å kunne gi pasienten riktig behandling, så vil direkte tilgang være en langt mer egnet måte. For det andre, så er det informasjonsmengder som ikke egner seg for meldingsformidling. Eksempler kan være røntgenbilder, video, ultralyd m.m., som i noen tilfeller ikke vil kunne åpnes dersom sykehuset som mottar meldingen ikke har rett programvare, og i andre tilfeller vil representere så store datamengder at de ikke bør dupliseres i journalene. Et tredje moment er at langt større informasjonsmengder enn nødvendig vil bli lagret, selv om sykehuset som har mottatt informasjonen kanskje bare trengte en liten opplysning. Denne informasjonen vil mest sannsynlig ikke bli oppdatert senere, noe som kan føre til dårligere pasientsikkerhet.

Samhandlingsreformen legger opp til at pasientinformasjonen må følge pasienten. Dette kan bli vanskelig med et for strengt regelverk gitt gjennom forskriften. Et for komplisert regelverk

for styring av tilgang vil kunne føre til dårligere pasientsikkerhet og være i strid med intensjonen i samhandlingsreformen.

Samhandlingsreformen legger opp til at informasjonen skal følge pasienten i et behandlingsforløp. Å sette grensen for flyt ved et organisasjonsnummer synes ikke å sammenfalle med intensjonen i samhandlingsreformen. Personvernet kan unektelig bli forringet ved at mange har for lett tilgang til pasientopplysninger, men på den annen side kan pasientsikkerheten forringes ved at det settes for strenge krav til tilgang.

§ 3

I merknaden brukes betegnelsen to-faktor/fler-faktor for å betegne et høyere nivå av sikkerhet enn ved autentisering ved hjelp av brukerid og passord. Autentisering er delt opp i forskjellige nivåer, og to-faktor er et eksempel på en praktisk løsning for sterk autentisering. Vi mener at begrepet *sterk autentisering* bør benyttes for høyere nivå av sikkerhet enn kombinasjon av brukerid og passord.

§ 9

I merknaden 2. avsnitt: Hva betyr det at helsepersonell som gis myndighet til å treffe beslutning om innholdet i en autorisasjon må ha *helsefaglig kompetanse*? Betyr det at de må ha autorisasjon? I så fall: En leder som ikke er helsepersonell kan ha vide fullmakter til å ansette, men ikke til å gi autorisasjon til medarbeider for det arbeidet han/hun blir ansatt for å gjøre? Vi mener at ledere må ha myndighet til å tildele autorisasjon til sine ansatte når det gjelder tilgang til systemene.

§ 10

Autorisasjon blir omhandlet i mange paragrafer, og det virker som mye blir dobbelt opp. Sikkerheten skal i henhold til personopplysningsforskriften være forholdsmessig, dvs. stå i forhold til sannsynligheten for og konsekvensen av sikkerhetsbrudd. Sikkerheten for et lite system med få brukere må stå i forhold til risikonivået, for eksempel vil et brudd på konfidensialiteten ikke gjelde så mange pasienter og en begrenset mengde informasjon. En risikovurdering skal vise hva som er tilfredsstillende sikkerhet (akseptabelt risikonivå). Kravene som er listet opp i pkt a-c fremstår som svært detaljerte og uttømmende krav. Kravene burde heller stå i merknaden som eksempler på hva som bør vurderes. Det kan også være andre forhold som må vurderes for å få klargjort om sikkerheten er tilfredsstillende. Hvilke opplysninger som skal registreres må stå i forhold til formålet med opplysningen. Er det for eksempel viktig å vite *antall* (i betydningen tall på) registrerte det gis tilgang til? Det som må vurderes er om det er et stort eller lite antall registrerte (for eksempel hele sykehuset/avdeling/post) og det bør komme tydeligere fram i selve forskriften, slik at det ikke kan misforstås. Vi mener at den de detaljerte kravene bør tas ut av forskriften slik at databehandlingsansvarlige selv må tallfeste eller konkretisere hvilke parametre tilgangen skal vurderes og konfigureres etter i henhold til akseptabelt risikonivå og tilfredsstillende sikkerhet.

Vi mener videre at når det gjelder tidsbegrensning av autorisasjoner, så må den følge den ansattes virke. Endres arbeidsforhold/oppgaver, så må autorisasjonen endres.

§ 11
Det står at grunnlaget for *tilgang* skal registreres. Hva menes med det? Menes det grunnlaget for autorisasjonen, eller at man skal oppgi en grunn hver gang man går inn i journalen (slik det gjøres ved aktualisering/eksplisitt tilgang). Dersom det er grunnlag for autorisasjonen, så vil dette fremgå av arbeidsavtale, rolle, avdeling osv. Det som bør fremgå er hvilken rolle og avdeling/post den ansatte har/hadde til enhver tid, uten at det behøver detaljeres hvor det skal finnes. Vi mener at dersom det menes grunnlag for hver tilgang, så burde det være unødvendig med ytterligere registrering av grunnlaget for tilgang dersom det er benyttet tilgang som er innenfor den autorisasjonen som er gitt til den ansatte.

§ 17
Register over autorisasjoner er normalt en integrert del av tilgangsstyringen i et system, dvs. at denne informasjonen ikke dupliseres i et eksternt system/register. En oversikt over bruker, brukerrolle, avdeling/post og start-/sluttdato for de forskjellige autorisasjoner bør være tilstrekkelig.

Vi mener at formål med autorisasjonen ut over det som fremkommer av rolle og avdeling burde være unødvendig. Dersom mer informasjon må tas inn, må dette innarbeides som utvidelser av den tilgangsstyringen som er integrert i systemet.

§ 19
Det er litt uklart hvordan bestemmelsen om at det skal fremgå av journalen hvem som har truffet beslutningen om at det skal ytes helsehjelp skal dokumenteres. Må det spesifikt skrives ned noe sted, eller holder det med at det er logget? Beslutningen vil implisitt fremkomme gjennom dokumentasjon i journalen, og bruk av eksplisitt tilgang vil være dokumentert i journalloggen.

Å innføre beslutningsstyrt tilgang i alle behandlingsrettede helseregistre (store som små) i et helseforetak vil ikke være realistisk, og vil neppe være nødvendig for sikkerheten i et lite og avgrenset system. Dette bør ikke være et krav for mindre system.

Det er positivt at pasientens rett til sperring av opplysninger ikke er absolutt. Det er ikke bare snakk om at pasientsikkerheten reduseres ved sperret journal, men at også helsepersonell har krav på sikkerhet i forhold til for eksempel smitte, voldelig adferd, og andre særlige problemstillinger. Vi mener derimot at det ikke er ønskelig at helsepersonell skal begynne å sperre opplysninger uten at pasienten ber om det. Det bør ikke være opp til det enkelte helsepersonell å vurdere om en opplysning kan bli nødvendig eller ikke for annet helsepersonell i fremtiden.

§ 22
I 1. ledd sies det at tilgang på tvers bare kan omfatte strukturerte helseopplysninger. De elektroniske pasientjournalene har riktignok en struktur, men svært mye av pasientinformasjon er tekst som ikke strukturert på annen måte enn at de er puttet inn i et dokument som ligger på et bestemt sted i journalen. Begrepet strukturert kan derfor lett misforstås. Vi mener at dagens EPJ tilfredsstiller krav om strukturerte helseopplysninger, men vi ser også et behov for å videreutvikle graden av struktur i EPJ.

I 2. ledd er det uklart hva som menes med at formål skal knyttes til *type helsehjelp*. I denne sammenheng tenker vi som helseforetak at det er snakk om spesialisthelsehjelp, men det burde være rimelig implisitt. En avtale mellom spesialisthelsetjenesten og kommunal helsetjeneste må naturligvis avgrenses i forhold til behov, men når det i § 31 benyttes samme begrep, så blir vi usikker på hva som egentlig menes.

Vi er enige i formuleringene om at databehandlingsansvarlig må forsikre seg om at informasjonssikkerheten må være god nok hos den andre virksomheten og at det skal fremgå av avtalen hvilke tekniske løsninger som skal benyttes. Dette samsvarer ikke med bestemmelsen i § 25, der en bestemt teknisk løsning pålegges (kvalifisert sertifikat).

§ 24
Ref. kommentar til § 22 angående strukturert informasjon i journalen.

§ 25
Helse Bergen er i hovedsak enig i at det må være sterk autentisering mellom foretak som har tilgang på tvers dersom disse har atskilte driftsmiljø. Slik det er i Helse Vest, så har journalsystemene ved flere av helseforetakene/sykehusene felles database med logisk skille mellom virksomhetene. Det er vanskelig å forstå argumentasjonen for å kreve sterk autentisering når man teknisk sett gis tilgang til samme database. I praksis vil dette dessuten bety at man må ha sterk autentisering også internt, med de kostnadene dette vil medføre. Skal det benyttes sterk autentisering i et slikt regime, så må dette fremkomme gjennom risikovurderinger som viser at man ellers vil overstige akseptabelt risikonivå. Det er vanskelig å se at for eksempel snoking vil bli mindre ved at det brukes sterk autentisering, og retting og sletting vil ikke være mulig. All autentisering og tilgang vil gjøres internt, og ikke via eksterne kanaler. Tilgang fra utenforstående vil derfor være tilsvarende som ved intern bruk. Helse Bergen er derfor uenig i at det er behov for sterk autentisering for tilgang på tvers når det er snakk om tilgang til samme database i samme driftsmiljø.

Helse Bergen er ikke enig i et obligatorisk krav om kvalifisert sertifikat. Hvilken type sterk autentisering det vil være behov for, vil måtte fremkomme gjennom en risikovurdering av aktuell løsning.

§ 26
Det er uklart hva det betyr at forespørsel (om tilgang på tvers), samt beslutningen om å etterkomme den, eller ikke, skal registreres. Vi oppfatter det ikke sånn at en person skal sitte og vurdere hver forespørsel. Det må være avklart på forhånd mellom partene hva man kan få tilgang til, for eksempel bare epikriser eller bare dokumenter fra avdeling a og b, men ikke c. Er det dette som menes med formuleringen? Vi mener at det er tilstrekkelig at det på forhånd er avtalt mellom partene hvilke deler av den strukturerte journalen ulike roller hos den samarbeidende part kan få tilgang til. Dersom man etterspør dokumenter utenfor det som er avtalt eller dokumenter som er sperret, så vil en slik forespørsel automatisk bli avvist. Øvrige forespørsler vil bli imøtekommet automatisk.

I siste avsnitt i merknaden står det at når det ikke lenger ytes helsehjelp til pasienten (dette eksemplifiseres med at pasienten er utskrevet eller flyttet), så skal det heller ikke være mulig for vedkommende helsepersonell å forespørre om tilgang til helseopplysninger i den eksterne virksomheten. Dette virker uforståelig. Når man trenger informasjon om pasienten, for eksempel hvis det kommer en ny henvisning som skal vurderes eller en telefonisk henvendelse om samme, må man kunne åpne for tilgang. Vi mener at stengning av tilgang på tvers i så fall bør knyttes til at en henvisningsperiode avsluttes, ikke til utskriving eller flytting. Henvisningsperioden må i så fall knyttes til den virksomheten som søker tilgang på tvers. Ingen systemer vil, oss bekjent, i dag tilfredsstille et slikt krav, så her vil det trenges en overgangsordning.

§§ 31 og 32
Krav om dokumentasjon av tilgang i journalen og krav om hendelsesregistrering/logg i § 32 må sees i sammenheng, fordi de til dels er overlappende.

I merknaden til § 31 står det at det ikke er tilstrekkelig å skrive helsehjelp som årsak til at journalen åpnes, men at *type helsehjelp* skal angis. Det er uklart hva som menes, ref kommentar til § 22.

Paragrafene er lite strukturerte i forhold til hva som skal *dokumenteres* (§ 31) i systemet og hva som skal *logges* (§ 32) inne i og/eller utenfor systemet. Det er uklart hva som menes med dokumenteres; er det tilstrekkelig med en logg, eller skal det dokumenteres i et dokument eller lignende? I tillegg er det en del opplysninger som skal dokumenteres både i journal og i logger, dvs. dobbelt opp. Dokumentasjon/logg bør deles tydeligere opp i forhold til det som er *internt* i journalen og det som er *eksternt* i forhold til journalen (i nettverket). Det vil være langt ryddigere med en klar to-deling med oversikt over hva som foregår inne i et system og hva som foregår utenfor systemet. Hvem som dokumenterer i journalen, når osv. er også en del av journalens interne logg. Den dokumentasjonen som er krevd etter journalforskriften kan suppleres med ytterligere logging, som for eksempel årsak til åpning av journalen og hvilke opplysninger det er gitt tilgang til (hvilke dokumenter er åpnet og hvor lenge). Logg over hvilke systemer en bruker har benyttet under påloggingen og forsøk på uautorisert tilgang(?), skjer i nettverket. Å kreve oversikt over stedet hvor vedkommende har vært pålogget fra vil kreve GPS på alle PC'er, med mindre det menes PC'ens IP-adresse. Krav til dokumentasjon og logging bør også vurderes nærmere i forhold til hva opplysningene skal brukes til. Vi mener at det i forskriften ikke bør settes krav om logging utover det som inngår i det enkelte behandlingsrettede system. Ytterligere krav til logging må fremkomme som et resultat av risikovurdering av den øvrige infrastrukturen og besluttes av den enkelte virksomhet.

I merknaden sies det at dokumentasjonen vil være mer lettfattelig enn loggen når pasienter vil ha innsyn i hvem som har hatt tilgang. Dette er nok et eksempel på at differensiering av disse begrepene blir uforståelige. Det lages rapporter som henter data fra det man måtte ønske av opplysninger av det som er logget (eller dokumentert?). Disse behøver slett ikke være komplekse. Helse Bergen har mange års erfaring fra utsending av logger til pasienter, og ingen har bedt om ytterligere forklaring enn det som legges med som standard.

Kravet til sammenstilling av loggen mot tilstedeværelsesregister vil i liten grad kunne bevise brudd på taushetsplikten. Mange helseforetak benytter bærbare PC'er, og arbeid gjøres ofte fra andre steder enn på sykehuset, og gjerne også utenom den oppsatte arbeidstiden/turnusen. Det er ingen indikasjon på at det snokes mer utenfor arbeidstid enn i arbeidstiden. Det eneste dette eventuelt kan brukes til, er å renvaske en mistenkt person, fordi vedkommende umulig kunne ha tilgang på tidspunktet for snoking. Et slikt tilfelle vil likevel avdekke at bruker-id og passord er misbrukt (lånt ut?).

Hva menes med setningen i avsnitt 2 under merknader til § 32: Opphenting av helseopplysninger *fra eget system mot en felles database for helseopplysninger* skal ha tilsvarende registreringer over uautoriserte forsøk og autoriserte påloggінger?

Datatilsynet har tidligere ikke satt krav til logging i små registre fordi de inneholder avgrenset mengde informasjon om relativt få pasienter og få ansatte har tilgang. Dette er knyttet opp mot vurderingen av mulighet for og omfang av sikkerhetsbrudd. Det er ikke behov for å sette krav til at det skal etableres logger for alle behandlingsrettede helseregistre ut fra sikkerhetshensyn.

§ 33
Det er svært vanskelig å avdekke brudd på taushetsplikten gjennom generell loggkontroll, og det er lett å få mange både falske positive og negative. Falske positive vil gå ut over personvernet til de ansatte. Rutinemessige, tilfeldige gjennomganger avdekker per i dag lite. Skal snoking kunne avdekkes uten at det foreligger mistanke, og uten at pasienten er med og kontrollerer, så vil det kreve et avansert verktøy, som for eksempel mønstergjenkjenning som brukes for å avdekke hvitvasking i finanssektoren. Vi mener at pasienten er den beste kontrollør av logger. Videre arbeid med både stikkprøver og automatisert logganalyse vil primært kunne bidra til *preventiv* sikkerhet og til bedre *holdninger* fordi brukerne da vet at de vil kunne bli *oppdaget*.

§ 34
Som nevnt under § 17, vil autorisasjonsregisteret være en del av det enkelte register. Det er derfor ikke behov for sammenstilling av registre – det vil fremkomme av loggen hvem som er autorisert, hvilken rolle og avdeling vedkommende er autorisert i forhold til.

Spørsmål som er ønsket besvart:

Har forskriften god balanse mellom personvern og pasientsikkerhet?
Helse Bergen mener at både personvern og pasientsikkerhet er viktig, men at forskriften ikke har særlig god balanse mellom dem. Noen av tiltakene som er ment å forsterke personvernet er både for detaljerte og unødvendige, og vil neppe styrke personvernet i praksis. Snarere vil det kunne gå ut over pasientsikkerheten. I tillegg til de detaljerte bestemmelsene blir store og små systemer skåret over én kam. Sikkerhet og personvern må belyses gjennom risikovurderinger, men på en del områder vil ikke databehandlingsansvarlig kunne bestemme akseptabelt risikonivå, fordi svært detaljerte og unødvendige krav er satt i forskriften.

Om vi har implementert beslutningsstyrt tilgang?
Helse Bergen har implementert beslutningsstyrt tilgang gjennom DIPS. Dette er imidlertid bare ett av svært mange og viktige behandlingsrettede systemer vi har i bruk.

Når kan vi ha implementert de ulike kravene i forskriften?
For DIPS sin del mener vi at vi har implementert de fleste kravene i forslaget til forskrift, bortsett fra bruk av kvalifisert sertifikat i forhold til tilgang på tvers. Vi tar her forbehold om at vi har tolket høringsutkastet rett og at våre merknader tas til følge. Det er noen mangler i DIPS i forhold til bl.a. logging, men dette jobber leverandøren med. I tillegg har vi sett bort fra de kravene vi har påpekt som unødvendige.

For andre system er det svært uklart når kravene vil kunne bli tilfredsstilt. Noen krav er som nevnt svært detaljerte og i praksis vanskelig å få gjennomført uten store kostnader. Dessuten er omfanget av systemer så stort at det vil ta mange år å få de tilpasset – om det er mulig i det hele tatt.

Skal forskriften kunne etterleves, så må det etableres overgangsordninger med en rimelig lang horisont.

31 AUG 2010

Stavanger Universitetssjukehus
Helse Stavanger HF
Fag- og foretaksutvikling - Seksjon for kvalitet og pasientsikkerhet

Helse Vest RHF

Postboks 303, Forus
4066 Stavanger

Vår ref:	Deres ref:	Saksbehandler:	Dato:
2010/2233 - 32473/2010		Sølve Braut	26.08.2010

Informasjonssikkerhet helseregistre - høring

Høringen har blitt sendt til de ulike divisjonene ved helseforetaket og bygger på de kommentarene som har kommet inn.

Hovedinntrykket er at departementets forslag om informasjonssikkerhet og tilgang til helseopplysninger er nøye gjennomarbeidet. Det er en grundig utredning som allerede har vært ute på en høringsrunde.

Det er et generelt problem hvordan man skal forhindre at opplysninger om pasienter spres unødvendig i helseinstitusjonene, samtidig som at nødvendig informasjon kommer fram til alle behandlere.

SUS bruker DIPS journalsystem, og dette systemet er et eksempel på ett helseregister med god tilgang, men samtidig har det sperrer som hindrer at uvedkommende får tilgang. Det er vanskelig å få denne balansen slik at alle blir fornøyde.

Loven og forskriftens kap. V åpner for tilgang på tvers av virksomheter. Reglene for når dette kan gjøres og hvordan det skal gjøres, bør være klare og lett forståelig. Slik reglene er formulert nå er de ikke umiddelbart lette å forstå, og det synes å etableres et relativt omfattende system for når slik tilgang kan gis. Dette kan føre til at det blir praktisk vanskelig i bruk.

I følge høringen ønsker departementet kommentarer på hvorvidt det bør være mulig å dispensere for kravet om bruk av kvalifisert sertifikat, jf. forskriften § 25. Etter vår vurdering bør det være adgang til slik dispensasjon, særlig i de tilfeller der det er et utstrakt samarbeid om pasienter mellom helseinstitusjoner.

Forskriften gjelder tilgang til helseopplysninger i behandlingsrettede helseregistre. Det er behandlet kort studenter og elevers tilgang, men man savner en omtale av tilgang til disse registre i forbindelse med forskning. Dette er i stor grad dekket av Helseforskningsloven, men en viss presisering i den gjeldende forskrift, med henvisning til Helseforskningsloven er etter vår mening på sin plass.

Videre har en i § 33 en bestemmelse om oppfølgning og kontroll av elektronisk tilgang. Det heter at det dersom det avdekkes uregelmessigheter skal Datatilsynet informeres. Vi vil også påpeke at det vil være rett å informere Helsetilsynet.

Med vennlig hilsen

Ingar Pettersen
Adm. direktør

Mottatt HV RHF
31 AUG 2010

Helse Fonna

- Fremme helse og livskvalitet

Helse Vest RHF
Att. Ivar Eriksen
Postboks 303, Forus
4066 Stavanger

Deres ref:	2010/248-2953/2010	Vår ref:	2010/2123-18518/2010	Kjellfrid Laugaland, tlf 52732045	Haugesund, 25.08.2010

Høring av forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

Helse Fonna viser til brev fra Helse Vest datert 24.06.10 og brev av 10. 05.10 fra Helse- og omsorgsdepartementet vedlagt utkast til forskrift om informasjonssikkerhet m.v. i behandlingsrettede helseregistre. Helse Vest ønsker å samordne innspill fra foretakene i Helse Vest til en felles uttalelse. Det er spesielt bedt om synspunkter på om kravene i forskriftforslagets § 10 første ledd andre punktum er tilstrekkelig fleksible til at helsepersonell kan få tilgang til nødvendige og relevante opplysninger når det er tjenstlige behov for å kunne yte forsvarlig helsehjelp til pasienten.

Generelt.

Det er gjort et grundig arbeid for å finne riktig balanse mellom rask tilgang til nødvendige opplysninger om den enkelte pasient – og personvernhensyn. Forsvarlig diagnostikk og behandling krever rask, enkel og sikker tilgang til nødvendige og tilstrekkelige pasientopplysninger for riktig person til riktig tid.

Spesielt.

Ad §10 første ledd. Utfordringen blir å utarbeide teknologiske løsninger – og rutiner- som sikrer tilgang til nettopp dette - nødvendige og tilstrekkelige opplysninger – og kun dette – uten å samtidig gi innsyn i opplysninger som *ikke* er nødvendige for å løse aktuell problemstilling eller gi den nødvendige helsehjelp. Dette må bety at det stilles strenge krav til strukturert pasientjournal. Ellers må rolletilgang der innholdet i rollene og hva det skal gis tilgang til, defineres tydelig før tilgang til enkeltpersoner gis, og tilpasses daglig drift og pasientflyt for å sikre forsvarlig diagnostikk og pasientbehandling. Vi mener § 10 første ledd er dekkende for behovet.

Nødvendig og tilstrekkelig må ikke defineres for smalt – ikke sjelden har ansvarlig behandlende personell behov for tilgang til alle opplysninger. En risiko kan være at vi bygger opp systemer som gjør daglig drift og pasientflyt tungvint og administrativt for krevende.

Helse Fonna
P.Boks: 2170
5504 Haugesund
Foret.nr: 983 974 694
Bank. 5082.08.47218

Kontaktinfo:
Sentralbord: 52 73 20 00
Telefaks: 52 73 20 19
post@helse-fonna.no
www.helse-fonna.no

Fakturaadresse:
Helse Fonna HF
Regnskap, P.Boks 64
5751 Odda
Tlf: 52 73 20 00

Dokumentert samtykke (§27) til tilgang er en utmerket grunnregel, og vi mener at § 28 gir snevre, men gode nok rammer for fravik om krav om samtykke.

§ 15 sier at "autorisasjon kan gis til personell i pasientadministrasjonen som har behov for det for å kunne administrere helsehjelp til pasient, jfr. helsepersonelloven § 26 andre ledd." Hva er nødvendig og tilstrekkelig for at en klinikkdirektør skal kunne behandle en klagesak (dokumentert samtykke forutsettes)? Skal autorisasjon om tilgang tildeles rollen bredt, eller skal det gis tidsbegrenset tilgang til nødvendig informasjon til enkeltjournalen? Begrensninger til sensitiv informasjon som ikke er nødvendig og evt bryter med taushetsplikten blir utfordrende.

At det er tydeliggjort at lovverket inngår i internkontrollen, er positivt.

Summarisk

Regelverket har fått en grundig og kritisk gjennomgang, og oppfattes som en kilde til forbedring og økt sikkerhet i utøvelse av taushetsplikt og personvern – samtidig som det ivaretar krav om tilgang til opplysninger om pasient for forsvarlig diagnostikk og behandling til riktig person på riktig tidspunkt – og kvalitetssikring og internkontroll. En risiko er at "nødvendig og tilstrekkelig" defineres for bredt – eller for smalt – innenfor de enkelte roller. Utøvelsen må ikke bli til hinder, men til støtte, for en smidig og sikker drift der personvern ivaretas. Målet må være å oppnå ønsket og mulig helsegevinst inklusive personvern for enkeltpasienter og pasientgrupper som står i relasjon til ressursene som brukes, og vi håper at også dette vil bli dokumentert.

Vi ser at oppfølging og gjennomføring av regelverket med prosedyrer, rutinebeskrivelser, IKT-løsninger, opplæring, kontroller og vedlikehold etc. vil bli meget arbeids- og ressurskrevende, og at det blir en stor utfordring å skaffe ressursene til veie.

Helse Fonna HF

Kari Ugland
Adm. Dir.

Kjellfrid Laugaland
fagsjef