

Orientering om situasjonen i Helse Sør-Øst vedrørende styring av tilgang og andre tiltak for å styrke personvernet

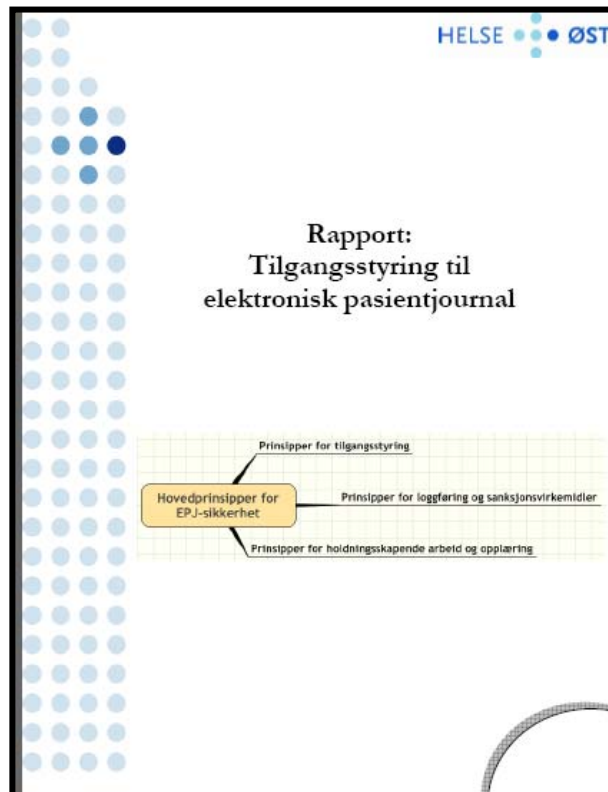
Knut Hellwege
Prosjektleder/Spesialrådgiver IKT
Helse Sør-Øst RHF

knut.hellwege@helse-sorost.no, Mobil:934-01665

Prosjektgjennomføring: januar – april 07:

- Referansegruppen for prosjektet
Dvs: Systemeierforum for DIPS , inkl repr fra UUS og Sunnaas
- Styringsgruppen for prosjektet
Gruppen har vært sammensatt av ressurspersoner fra samtlige helseforetak i Helse Øst samt Lovisenberg Diakonale Sykehus og Diakonhjemmet Sykehus.
- Direktørmøtet i Helse Øst 4. mai 2007, som konkluderte slik:

”...Direktørmøtet anbefaler at vedlagte rapport danner grunnlag for lokal implementering i samtlige HF. Konkretisering av prinsippene må skje i det enkelte foretak



Rapporten finnes [her](#)

Seminar om EPJ og tilgangsstyring

Du er her: [Forsiden](#)

Helse Sør-Øst RHF

Sikrere elektronisk pasientjournal

Den elektroniske pasientjournalen (EPJ) i sykehus inneholder svært mange opplysninger om pasienten som helsepersonell har tilgang til for å kunne yte forsvarlig helsehjelp. Dette stiller store krav for å sikre at opplysningene ivaretas trygt og i tråd med lovverket. Nylig var over 100 deltakere fra helseforetakene i Helse Sør-Øst samlet for å diskutere overordnede prinsipper for å bedre informasjonssikkerheten for EPJ.

Bakgrunnen for samlingen var en rapport med overordnende prinsipper for tilgangsstyring, utarbeidet i tidligere Helse Øst RHF av en arbeidsgruppe med representanter fra helseforetakene og det regionale helseforetaket. Prosjektet ble ledet av Bjørn Magne Eggen, direktør ved enhet for medisinske fag og strategi ved Akershus universitetssykehus HF.

- Tilgang til EPJ er avgjørende for å sikre forsvarlig helsehjelp. Samtidig skal vi styre tilgangen slik at pasientopplysningene ikke er tilgjengelig for andre enn dem som skal yte helsehjelpen. Dette er selve grunnprinsippet for god tilgangsstyring, sier Bjørn Magne Eggen.

Sykehus er kompliserte organisasjoner med mange forskjellige aktører som har ulike roller.

- Våre medarbeidere kan arbeide på tvers av avdelingsgrenser og profesjoner, og de vil ha ulike arbeidsoppgaver ikke bare ut fra profesjon, men også etter hvor i organisasjonen de arbeider. Derfor er det viktig å sikre rett tilgang etter hvilken rolle den ansatte har ovenfor pasienten, sier Eggen.

Sikrere EPJ

Sosial- og helsedirektoratet har i Norm for Informasjonssikkerhet (2006) definert at informasjonssikkerhet omfatter fire ulike aspekter; konfidensialitet (taushetsplikt, personvern), integritet (at data er korrekte og beskyttet mot å bli urettmessig endret eller manipulert), tilgjengelighet (den som skal ha tilgang til opplysningene, får dem når hun/han trenger dette), og også kvalitet. En sikrere EPJ forutsetter at alle disse fire aspektene blir ivarettatt.



-Vi må styre tilgangen til pasientopplysningene slik at de ikke er tilgjengelig for andre enn dem som skal yte helsehjelpen, sier Bjørn Magne Eggen. Han har ledet prosjektet om EPJ og tilgangsstyring.

 Abonner på Nyheter

► VEDLEGG

Rapport tilgangsstyring 0,42 MB

Innledning v/ Bjørn Magne Eggen 0,37 MB

Prinsipper for tilgangsstyring v/ Gunhild Rognstad 0,07 MB

Prinsipper for loggføring og sanksjonsvirkemidler v/ Jan Gunnar Broch 0,27 MB

Prinsipper for opplæring og holdningskapendearbeid v/ Bente Teilstad og Anne Nørsett 0,38 MB

Tilgangsstyring innenfor dagens lovgivning (IS 7/2006) v/ Nina Fladsrud 0,05 MB

Tilgangsstyring innenfor dagens lovgivning (IS 7/2007) v/ Tor Ottersen 0,04 MB

Praktisk bruk av risikovurderinger v/ Heidi Thorstensen 0,15 MB

- Seminar om EPJ og tilgangsstyring 11. og 12. september 07
 - 120 deltakere
 - alle HF i Sør-Øst
 - Datatilsynet
 - Shdir
 - KITH
 - Helsetilsynet
 - EPJ-leverandører
 - etc

Status implementering av prinsipper i Helse Sør-Øst pr. september 08

- Meget stor variasjon i status
- Flere HF har igangsatt eller planlagt å bytte EPJ, eller er i ferd med versjonsoppgradering

Eksempel på status:

Rød	Prinsippet etterleves ikke	7 krav (18%)
Oransje	Prinsippet etterleves i hovedsak ikke, men enkelte tiltak er gjennomført	3 krav (8%)
Gul	Prinsippet er delvis gjennomført, men tiltak er ikke tilstrekkelige	9 krav (23%)
Grønn	Prinsippet etterleves.	20 krav (51 %)

Helse Sør-Øst RHF vil sammen med Akershus universitetssykehus HF (Ahus) og de øvrige helseforetakene prioritere arbeidet med å ivareta personvernet til pasienter, og ønsker i sterkere grad å ha kontroll med innsyn/oppslag i elektronisk pasientjournal (EPJ). - Nå skriver vi kontrakt med leverandør av et verktøy som vil kunne sikre at vi kan avdekke medarbeidere som urettmessig kan få innsyn i informasjon de ikke har behov for i sitt daglige virke, sier konserndir. i Helse Sør-Øst RHF, Steinar Marthinsen.

I desember 2007 ble det nedsatt et nasjonalt prosjekt ledet av Ahus på vegne av Helse Sør-Øst. Prosjektets mandat var å anskaffe en løsning/verktøy for analyse, kontroll og oppfølging av innsyn/oppslag i EPJ.

Formål med anskaffelsesprosjektet har vært:

- Ivareta personvernet
- Innfri kravet om loggkontroll beskrevet i "Norm for informasjonssikkerhet i helsesektoren 2006".
- Muliggjøre og effektivisere loggkontroll ved at det gis bedre kvalitet og tilgjengelighet på loggdata
- Legge til rette for en videre standardisering og samordning innen fagfeltet i samarbeid med valgt leverandør
- Lavere anskaffelses-, implementerings-, drifts- og vedlikeholdskostnader enn om foretakene skal anskaffe og innføre dette hver for seg

- Pasienter som behandles i våre sykehus skal være sikre på at informasjon om dem selv ikke kommer på avveie. Med dette verktøyet styrker vi arbeidet med personvern ytterligere. Vi har nulltoleranse for at personer i sykehusene, som ikke har behov for informasjon om pasienten i sin daglige jobb, snoker i pasientjournaler. Nå har vi i tillegg til systemenes egne kontrollmekanismer, fått et verktøy som loggfører all aktivitet på dette område, sier Steinar Martinsen.



Kontrakten signeres. Fra venstre: Kjetil Dahl (seniorkonsulent mnemonic AS), konserndirektør Steinar Marthinsen Helse Sør-Øst RHF og prosjektleder for anskaffelsen Ellef Mørk (informasjonssikkerhetsleder Ahus).

Logganalyseverktøy

- Kort om anskaffelsen og løsningen:
 - Løsningen samler loggelementer fra de fleste typer systemer
 - I løsningen kan det bygges brukerprofiler. Ved avvik fra normalt arbeidsmønster trigges alarm.
 - Alarmer gis i sanntid - dvs innen 60 sekunder og kan sendes definerte mottakere for umiddelbar oppfølging
 - Samtlige regionale helseforetak har vært representert i prosjektet. Videre har Helsedirektoratet og Datatilsynet har vært observatører i prosjektets referansegruppe.

Utfordringer:

Omstillingsprosessen i Helse Sør-Øst

- Organisatoriske endringer jmf bl.a funksjonsfordeling
- Juridiske enheter
- Tilgangsstyring
 - Utveksling av arbeidstakere på tvers mellom HF
 - For eksempel i Oslo-området
 - Fødselsnummerbruk i administrering av ansettelsesforhold (herunder tilgangsstyring)
 - Lovverk krever korrekt tilgangsstyring i forhold til rolle, men må dokumentere nødvendig bruk av fødselsnummer
 - 69.000 ansatte, -og identifisering av korrekt medarbeider er nødvendig

Mulighetsrommet

- **Kompetanseprogram**
 - *Bl.a. innenfor:*
 - Tjenstlig behov
 - hvor og når snakker du, med hvem, om hva (relatert til personvern)
- **Tekniske løsninger**
 - Logganalyse
 - IdM – Identity Management systemer (Identitetsstyring)
- **Felles løsninger, - samhandle på tvers**
(jmf omstillingsprogrammet)
- **Robuste løsninger**
 - Gode kontinuitetsløsninger som gir deg tilgang når du har behov, f.eks: drift på flere lokasjoner
 - Felles løsninger som gir lik håndtering

Informasjonssikkerhet – Igangsatt:

- Har etablert forum for informasjonssikkerhet hvor alle HFeene er med.
- Gjennomgang av informasjonssikkerheten og personvernet i kvalitetsregistre og andre tilsvarende registre som GOPP og NISSY.
- Tolkning av forståelse av lovverk knyttet til informasjonssikkerhet innenfor helsesektoren
- Vurdering av bruk av fødselsnummer i forbindelse med administrering av ansettelsesforhold (personinformasjon/HR, tilgangsstyring, opplæring)

Informasjonssikkerhet – **Planlagt igangsatt høst 2008:**

- Prosedyre for risikovurdering
- Revidering av felles styringssystem
- Rolle- og ansvarsavklaring
- Etablere IKT sikkerhetshåndbok
- Kompetanseprogram – nyansatte og kompetansepåfyll eksisterende medarbeidere
- Planlegger en kartlegging av informasjonssikkerheten og personvernet ved alle HFene.
- Avklare behovet for Cert-oppfølgning av helse (følge med på angrep mot infrastruktur) – nasjonalt og regionalt
- PKI – infrastruktur, implementering –i hvilke systemer/prosesser? nasjonalt og regionalt

Informasjonssikkerhet – Planlagt 2009

- Personvernombud HSØ – en sentralisert funksjon på RHFet
- E-læring for informasjonssikkerhet
- Etablering av felles rammer, prosedyrer og rutiner for HFene
- Implementere felles tilgangsstyring (etter HOD rapport, forventet lovendring og ny forskrift)
- Hendelse- og avvikssystem for informasjonssikkerhet
- Utvikle og etablere beredskaps- og reservedriftsplaner for å sikre kontinuitet – bør legges til Felles tjenesteleverandør (FTL)