

 Norm for informasjonssikkerhet www.normen.no	Utgitt med støtte av: 
<h1>Tilgangsstyring</h1>	Støttedokument Faktaark nr 14 Versjon: 3.1 Dato: 15.12.2010

Målgruppe Dette faktaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input checked="" type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder / sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
Ansvar	Databehandlingsansvarlig er ansvarlig for at tilgang administreres slik at tilgang til helse- og personopplysninger kun gis ved tjenstlig behov. Den enkelte ansatte har taushetsplikt omkring helse- og personopplysninger. Prosjektleder skal påse at tilgangsstyring i forskningsprosjekter er etablert.		
Gjennomføring	Tilgangsstyring må administreres kontinuerlig.		
Formål	Formålet med tilgangsstyring er å sikre at helse- og personopplysninger kun er tilgjengelig etter tjenstlig behov. Dette innebærer: <ul style="list-style-type: none"> • At brukere autentiseres på en betryggende måte • At tilganger tildeles, administreres, kontrolleres og fjernes 		
Omfang	Alle virksomheter i helse-, omsorgs- og sosialsektoren skal sikre at tilgang til helse- og personopplysninger bare gis i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt.		
Hjemmel	Tilgang til helseopplysninger er bl.a. regulert i: <ul style="list-style-type: none"> • Forvaltningsloven § 13 • Helsepersonelloven § 21 • Helsepersonelloven § 25 • Helsepersonelloven § 45 • Helseregisterloven § 11 • Helseregisterloven § 13 • Helseforskningsloven § 7 Andre aktuelle bestemmelser finnes i bl.a. personopplysningsloven, pasientrettighetsloven og pasientjournalforskriften.		
Referanser	<ul style="list-style-type: none"> • Norm for informasjonssikkerhet kapittel 5.2. • EPJ-standard: Arkitektur, arkivering og tilgangsstyring – http://www.kith.no/epj/ • Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, april 2008 		

Pasientopplysninger skal vernes, men helsepersonell som yter helsehjelp må gis mulighet til å søke opp og registrere relevante og nødvendige opplysninger i pasientens journal. Dette ivaretas bl.a. ved tilgangsstyring.

Tilgangsstyring avhenger av autentisering og autorisering. Autentiseringen innebærer at brukeren må identifisere seg overfor IKT-løsningen vha. en autentiseringsmekanisme som brukernavn/passord, smartkort o.l. Autentiseringen skal sikre at rett person autoriseres og får tilgang til helse- og personopplysninger, og at hendelsesregistreringen viser hvem som faktisk har hatt tilgang. Autentiseringsmekanismen må være av tilstrekkelig kvalitet og styrke – og tildeling må skje på en betryggende måte. Autorisering innebærer tildeling, administrering og kontroll av tilgang til informasjon i IKT-systemet. Tilgangen skal baseres på tjenstlig behov.

Autentisering

Autentiseringen skal være av tilstrekkelig styrke for formålet, og ulike anvendelser vil stille ulike krav til styrken:

- For pålogging til interne systemer (nettverk, EPJ internt o.l.) bør det benyttes minimum brukernavn/passord – systemet bør konfigureres til å stille krav om minimum 7 tegn, minst et tall og både store og små bokstaver.

- For pålogging fra eksterne nett, f.eks. hjemmekontor, som gir tilgang til sensitive opplysninger, må det benyttes sikkerhetsnivå 4 for autentisering

Tildeling av brukeridentitet og autentiseringsmekanisme må skje på en betryggende måte, og bør innbefatte personlig oppmøte og identifisering vha. legitimasjonsbevis med mindre den som registrerer brukeridentiteten kjenner brukeren fra før.

Autorisering

Virksomheten skal etablere prosedyre for tildeling, administrasjon og kontroll av tilgangsrettigheter. Tilgang til helse- og personopplysninger kan kun gis når det er nødvendig for å få tilstrekkelig informasjon til å gjennomføre eller bistå ved gjennomføringen av et behandlingstiltak, etter pasientens samtykke eller iht. lovbestemte unntak fra taushetsplikten.

Roller

Klart definerte roller og rollemaler kan være et hjelpemiddel for å definere tilgangsrettigheter i et EPJ-system. Organisatoriske roller vil ikke alene kunne gi tilgang til helseopplysninger. Organisatoriske roller kan avgjøre hvilke typer helsehjelprelaterte beslutninger de som innehar rollen er kvalifisert til å ta (og delta ved gjennomføringen av) samt i hvilken del av organisasjonen de har rett til å ta slike beslutninger. Rollene bør da defineres ut fra organisasjonsstrukturen og det informasjonsbehov ulike grupper ansatte vil ha i en behandlingssituasjon – noen eksempler på roller kan være:

- Lege ved anesthesiavdelingen
- Sykepleier ved sengepost A7
- Lege ved medisinsk avdeling

Eksempler på rollemaler:

- Lege
- Sykepleier

Rolledetaljeringen kan avhenge av virksomhetens størrelse og organisering.

Beslutningsbasert tilgangskontroll

Beslutningsbasert tilgangskontroll betyr at det skal foreligge en beslutning om gjennomføring av et behandlingstiltak ovenfor den aktuelle pasienten før tilgang til pasientens journal gis. En slik beslutningsstyrt tilgang skiller seg fra den mer tradisjonelle rollebaserte tilgangsstyringen ved at det er det konkrete engasjementet i forhold til pasienten og ikke helsepersonellens rolle i virksomheten som er avgjørende for den tilgang som skal gis. Helsepersonellens rolle i virksomheten er derimot avgjørende for hvilke beslutninger om helsehjelprelaterte tiltak den enkelte kan ta og/eller delta ved gjennomføringen av.

I journalen skal det registreres hvilke beslutninger som ligger til grunn for tilgangen, men dette kan i normaltilfellet (yte helsehjelp) registreres automatisk. Dersom tilgangen er begrunnet i for eksempel akutt helsehjelp eller krav om pasientinnsyn bør dette registreres eksplisitt.

Beslutninger om behandlingstiltak, samtykke (og det motsatte, muligheten til å motsette seg) samt lovbestemte unntak fra taushetsplikten er avgjørende når det gjelder tilgang til journalopplysninger. Tilgang kan kun gis når det er nødvendig for å få tilstrekkelig informasjon til å gjennomføre eller bistå ved gjennomføringen av et behandlingstiltak eller andre lovhjemlede tiltak. Dette kan foregå ved at informasjonen gjøres tilgjengelig i et tidsrom når pasienten er henvist til en avdeling for utredning eller behandling, eller ved at helsepersonell som er autorisert for det beslutter et medisinsk tiltak for en pasient. Tilgangsstyring i EPJ er videre beskrevet i EPJ-standarden som er utarbeidet av KITH (se referanser).

Helsepersonell som er aktiv som samarbeidende personell i behandlingen av den aktuelle pasient kan gis tilgang til å gjøre internt oppslag til nødvendige opplysninger i pasientjournal så lenge vedkommende fungerer som samarbeidende personell.

Eksempel på tilgangsstyring for EPJ i helseinstitusjoner (fra EPJ-standarden):

Styring av tilgang til opplysninger i pasientjournaler i helseinstitusjoner kan ut fra dette baseres på følgende hovedprinsipper:

1. Når det er truffet en beslutning om å yte en pasient helsehjelp skal det opprettes journal for pasienten, dersom slik journal ikke allerede er opprettet i forbindelse med tidligere tilfeller av helsehjelp. Jf pasientjournalforskriften § 5.
2. I helseinstitusjoner skal utpekes en person, journalansvarlig, som har det overordnede ansvaret for journalen, jf. helsepersonelloven § 39 og pasientjournalforskriften § 6. For å kunne ivareta sine oppgaver på en forsvarlig måte må journalansvarlig som en hovedregel ha tilgang til hele journalen.
3. Det helsepersonell som skal ha ansvar for gjennomføring av behandling eller annen helsehjelp må gis tilgang til nødvendige opplysninger i journalen. Slik tilgang vil ofte kunne gis implisitt, f.eks. som en følge av at en beslutning om innleggelse til en bestemt form for behandling registreres i en journal på et sykehus. Eller tilsvarende når det i den journal som pleie- og omsorgstjenesten fører, registreres at pasienten har takket ja til et tilbud om sykehjemsplass.
4. Helsepersonell som yter pasienten helsehjelp må gis mulighet til å registrere relevante og nødvendige opplysninger om helsehjelpen i pasientens journal. Jf. helsepersonelloven §§ 39 - 40.
5. Den rollen som helsepersonell er tilsatt i, avgjør hvilke typer tiltak vedrørende gjennomføring av helsehjelp den enkelte kan beslutte iverksatt og hvilke tiltak vedkommende kan delta ved gjennomførelsen av. Slike roller skal imidlertid ikke alene gi tilgang til journalopplysninger. Først etter at det er tatt en beslutning som innebærer at den som innehar en rolle blir involvert i den helsehjelp som ytes en pasient, kan det gis tilgang til nødvendige journalopplysninger.
6. Enkelte beslutninger om tiltak vedrørende helsehjelp vil kunne innebære at journalopplysninger må gis til samarbeidende personell, jf. helsepersonelloven § 25. Ved registrering av et slikt tiltak i journalen kan det automatisk åpnes for at helsepersonell som skal bidra ved gjennomføringen av et tiltak, får tilgang til nødvendige opplysninger. Dette selvsagt under forutsetning av at dette ikke er i strid med det samtykke pasienten har gitt når det gjelder tilgang journalen.
7. Ingen skal gis tilgang til flere journalopplysninger enn det som er nødvendig for å kunne gjennomføre de oppgaver som følger av den rolle vedkommende har. Når behovet for tilgang til journalopplysninger opphører, f.eks. fordi et besluttet tiltak er ferdig gjennomført, skal tilgangen til journalopplysningene opphøre.

Eksempel på tilgangsstyring i EPJ for små virksomheter (for eksempel legekontor)

F.eks. vil følgende kunne være tilstrekkelig når det gjelder EPJ-systemer beregnet for allmennleger:

1. Når en ny pasient mottas til behandling skal legen opprette journal for pasienten. Legen har ansvar for føring av journalen og skal ha tilgang til hele innholdet.
2. Dersom pasienten ikke ønsker at andre enn den faste legen skal ha tilgang til journalen, skal journalen kunne sperres slik at ingen andre kan åpne den.
3. Så fremt pasienten ikke ønsker journalen sperret, skal legen gi samarbeidende personell (legesekretær, andre leger på legesentret mv.) tilgang til hele eller relevante deler av journalen. Ved behov må slik tilgang kunne tidsavgrenses.
4. Dersom pasienten i den faste legens fravær ønsker å motta behandling av en annen lege ved legesentret, kan denne legen gis tilgang til journalen. Før slik tilgang gis må legen registrere den beslutningen som ligger til grunn for å åpne journalen.
5. Dersom en lege overdrar sin praksis til en annen, skal denne kunne registreres som ansvarlig for alle journalene fra et angitt tidspunkt og overta den opprinnelige legens rettigheter i forhold til disse. Dette gjelder dog ikke journaler til pasienter som ikke ønsker behandling hos den nye legen. Disse må håndteres etter bestemmelsene i pasientjournalforskriftens § 15.

Tilsvarende enkle oppsett kan utarbeides for andre typer mindre virksomheter.

Utlevering internt i en virksomhet ifm. pasientbehandling

Utlevering av helseopplysninger skal skje på grunnlag av beslutninger etter en konkret vurdering av behov. Når først en beslutning om utlevering er tatt finnes flere alternativer til å gjennomføre selve utleveringen. Et alternativ er elektroniske meldinger. Et annet alternativ er at de utleverte opplysningene gjøres tilgjengelig for den som har fått opplysningene utlevert.

Kontroll og oppfølging

Tilgang til EPJ skal dokumenteres i journalen med opplysninger om hvem som er gitt tilgang og periode.

Virksomheten bør ha prosedyre for kontroll av hendelsesregistre for å avdekke uautorisert tilgang (jfr. Faktaark 15 – Hendelsesregistrering og oppfølging), samt deaktivering av brukerkontoer som ikke er i bruk.

Tilgangsstyring i forskningsprosjekter

I forskningsprosjekter skal det skilles på tilgang til forskningsdata, koblingsnøkkel/koblingsfil og forskningsfil. Reglene for autentisering og autorisering ovenfor gjelder også i forskningsprosjekter.

Forskningsdata og koblingsnøkkel/koblingsfil skal kun være tilgjengelig for personell som skal tilrettelegge forskningsfilen. Når koblingsfilen ikke er i bruk skal den oppbevares sikret og adskilt fra forskningsfilen.

Tilgangsstyringen skal sikre at forskningsfilen kun er tilgjengelig for personell som deltar i forskningsprosjektet. I et forskningsprosjekt kan det være nødvendig å skille på ulike roller ift hva brukeren skal kunne utføre (lese, rette, slette), men oftest vil deltagere i et forskningsprosjekt ha samme rettigheter.

Prosjektleder skal avgjøre om koblingsnøkkel/koblingsfil skal oppbevares i forskningsprosjektet, innenfor rammen av REKs forhåndsgodkjenning, av virksomheten (personvernombud) eller eksternt hos en tiltrodd pseudonymforvalter (TPF) / tiltrodd tredjepart (TTP). Beslutningen skal være basert på akseptkriterier (for eksempel omfanget av forskningsdeltagere {100 vs 100.000}, spesielle personvernutfordringer og spesielle utfordringer ved multisenterstudier).