N O T A T

Arbejdspapir

Amtsråds-
foreningen

26-07-2004
J.nr. 106-335426
Jonas T. Petersen
Tel. 3529 8291
E-mail: jtp@arf.dk

Afrapportering fra sikkerhedsgruppen

Sikkerhedsgruppen i regi af den fælles EPJ-strategi ønsker med denne rapport af afrapportere fra sit arbejde. Afrapporteringen består at denne rapport samt den tilhørende bilagssamling.

Versionsstyring

Version	Beskrivelse	Forfatter	Dato
0.8	Arbejdspapir – endelig udgave	Sikkerhedsgrup-pen i regi af den fælles EPJ-strategi	30-08-2004

Resumé

Primo 2004 blev sikkerhedsgruppen i regi af den fælles EPJ-strategi etableret med henblik på at:

- vurdere behov og muligheder for fælles amtslige sikkerhedsløsninger i forbindelse med EPJ, herunder et centralt brugerstyringskatalog,
- vurdere, hvor snittet mellem centrale og decentrale sikkerhedsløsninger bør ligge – i første omgang med fokus på brugerstyring.

Gruppen har nu afsluttet sit arbejde. I denne afrapportering redegør den kort for hvorfor der er behov for fælles amtslige sikkerhedsløsninger, opridser forskellige muligheder og kommer med anbefalinger set fra et "sikkerhedsperspektiv".

Sikkerhedsgruppen anbefaler at der etableres et centralt brugerkatalog, som indeholder data, der er relevante for at løse opgaver i forhold til sikkerheden i nationale systemer, f.eks. sundhed.dk. Det centrale brugerkatalog skal kombineres med mere detaljerede decentrale brugerkataloger, som bruges af de enkelte amter til håndtering af egne brugeres adgang til amtets egne systemer.

Tilsvarende anbefales etablering af et centralt patientindeks som kan tilvejebringe de mest kritiske sundhedsoplysninger i en akut diagnosticerings- og behandlingssituation samt oplysninger om patientens forløb og kontakter til sundhedsvæsenet med henblik på at fremskaffe yderligere information. Sikkerhedsgruppen kommer med en række andre anbefalinger af relevans for sikkerheden i amtslige EPJ-løsninger og relaterede systemer.

Indholdsfortegnelse

Ordliste/begrebsafklaring

Herunder nævnes en række begreber, der er centrale for arbejdet med fælles systemarkitektur og sikkerhed:

Patientdata	Dette omfatter data om patienten: stamdata, behandlingsdata mv.
Sikkerhedsrelevante patientdata	Dette omfatter data om den enkelte patient, der har sikkerhedsmæssig betydning, f. eks. patientens samtykke og ønske om hvilke personer der må/ikke må se data.
Adgangskontrol/ Autentifikation	Betegner den del af sikkerhedssystemet, der sikrer brugerens identitet.
Rettighedsstyring/ Autorisation	Betegner den del af sikkerhedssystemet, der styrer hvilke processer og data, brugeren har adgang til. Det kan være statisk eller dynamisk: - Ved statisk rettighedsstyring vedligeholdes for hver bruger en liste over hans rettigheder - Ved dynamisk rettighedsstyring vedligeholdes et regelsæt, som fortolkes i form af relevans.
Relevans	Betegner den proces, der på grundlag af patientdata, brugerdata, sessionsdata og rettighedsdata afgør brugerens adgang til at læse/skrive *data*. Det er relevansen, der afgør hvilke data en bruger har adgang til. Patient-behandlerrelationen er central i fastlæggelse af relevans.
Rolle	Begrebet "rolle" anvendes som et samlebegreb med flere dimensioner, f.eks. arbejdsfunktion, organisatorisk tilknytning og uddannelse/sundhedsfaglig autorisation. Det er rollebegrebet, der afgør hvilke *applikationer* brugeren har adgang til.
Sundhedsfaglig autorisation	Henviser til autorisationer af personale i sundhedssektoren i henhold til Sundhedsstyrelsens klassifikationer.
Uddannelse	Henviser til uddannelser som f. eks. læge, sygeplejerske, fysioterapeut, lægesekretær, jurist. Uddannelse har en begrænset funktion i forhold til at give rettigheder, idet det afgørende oftest vil være den sundhedsfaglige autorisation eller arbejdsmæssig funktion.
Organisatorisk tilknytning	Betegner tilknytningen til en godkendt orga-

	organisatorisk enhed i sundhedsvæsenet, f. eks. enheder med ydernumre i praksissektoren eller sygehusenheder i en revideret sygehusafdelingsklassifikation.
Arbejdsfunktion	Betegner et sæt af standardiserede arbejdsopgaver i sundhedssektoren, som er relevant i sikkerhedsmæssig sammenhæng. Der eksisterer ikke i dag et sådant sæt af standarder.
Brugeradministration	Betegner den del af sikkerhedssystemet, hvor brugerne administreres: oprettelse, ændring, nedlæggelse
Rettighedsadministration	Betegner den del af sikkerhedssystemet, hvor rettighederne administreres: hvilke roller har adgang til data og applikationer
Kontrol	Betegner opgaver i forbindelse med kontrol af, at brugerne kun tilgår de processer og data, de har adgang til.
SEI	Sundhedsstyrelsens Elektroniske Indberetningssystem
EPJ	Elektronisk patientjournal
OIO	Offentlig Information Online

1. Sikkerhedsgruppens etablering og opgave

Primo 2004 blev sikkerhedsgruppen i regi af den fælles EPJ-strategi etableret. Sikkerhedsgruppen består af Pia Jespersen, (Københavns Amt, gruppens formand), Jørn Knudsen (H:S), Bo Guntofte (Roskilde Amt), Peter Holbech (Fyns Amt) og Jens Kjellerup (Århus Amt). Desuden har Ronnie Eriksson fra sundhed.dk deltaget i gruppens møder. Jonas Tyle Petersen fra Amtsrådsforeningen har ydet som sekretariatsbistand.

Dette notat indeholder afrapportering fra sikkerhedsgruppen. Notatet berører blot en delmængde af de sikkerhedsproblematikker, der opstår i forbindelse med udbredelsen af elektroniske patientjournaler. Den delmængde der fokuseres på omfatter imidlertid elementer, der ikke håndteres i dag, men som er væsentlige for udviklingen af sammenhængende EPJ-systemer i den nærmeste fremtiden.

Notatet indeholder en række vurderinger og anbefalinger (anbefalinger i teksten er markeret med en ramme). Sikkerhedsgruppen mener, at de fortsat vil være gældende – og formentligt aktualiseret– efter regionsdannelsen.

1.1 Afgrænsning af sikkerhedsgruppens opgaver

Sikkerhedsgruppen har fået til opgave at:

- vurdere behov og muligheder for fælles amtslige sikkerhedsløsninger i forbindelse med EPJ, herunder et centralt brugerstyringskatalog,
- vurdere, hvor snittet mellem centrale og decentrale sikkerhedsløsninger bør ligge – i første omgang med fokus på brugerstyring.

Gruppen har løst opgaven ved at fokusere på (1) basale krav til lokale/decentrale sikkerhedsløsninger og (2) modeller for fælles sikkerhedsstruktur på tværs af amter. Desuden deltager medlemmer fra sikkerhedsgruppen i arbejdet med at udarbejde et beslutningsgrundlag for et nationalt brugerkatalog for det danske sundhedsvæsen. Arbejdet sker i en arbejdsgruppe der refererer til sundhed.dk's projektstyregruppe og sekretariatbetjenes af Sundhedsstyrelsen.

Sikkerhedsgruppens betragter tilgængelighed, kvalitet, fortrolighed og sporbarhed som grundlæggende sikkerhedsparametre. Det er en væsentligt målsætning, at amternes sikkerhedsløsninger gør det muligt at sikre disse.

I sit arbejde har gruppen fokuseret på problematikker omkring rettighedsstyring, herunder eksempelvis kontrol og opfølgning herpå. Gruppen har afgrænset arbejdet i forhold til arbejdsgrupperne vedr. afprøvning af digitale certifikater og brugerkatalog såvel som arbejdsgruppen vedr. IT-arkitektur. Endvidere har gruppen afgrænset sig fra at se på en række tilstødende områder, herunder fysisk sikkerhed, backoffice/net og adgangskontrol (se i øvrigt kommissoriet og præciseringen af kommissoriet, bilag 1 og 2)

1.2 Baggrund for sikkerhedsgruppens arbejde

Baggrunden for at undersøge behovet for sammenhængende sikkerhedsløsninger i sundhedssektoren skal findes visionerne om en sammenhængende sundhedssektor og i den teknologiske udvikling.

Visionerne om en sammenhængende sundhedssektor med patientforløb på tværs af praktiserende læger, speciallæger og sygehuse betyder, at der er behov for at journalerne følger patienterne i systemet, og at sundhedspersonalet kan få adgang til data om patienter selvom de har været be-

været behandlet af en anden sundhedsaktør. Sundhed.dk er en af de løsninger, der skal bidrage til at nå denne vision.

Den teknologiske udvikling betyder helt konkret, at amternes sygehuse skal have EPJ inden udgangen af 2005. I sig selv er det en meget stor opgave, der kræver udvikling af sikkerheden, så data er til rådighed, når de skal bruges, men også så borgerne har sikkerhed for, at kun relevant sundhedspersonale har adgang til disse meget fortrolige data.

For amterne betyder disse tendenser en række udfordringer i forhold til den ønskede sikkerhed for patienternes data.

- den elektroniske patientjournal er en udviklingsopgave, hvor der skal skabes sikkerhedsmæssige løsninger på et komplekst lovgrundlag og i forskellige organisatoriske og tekniske miljøer. Hvis amterne udvikler sikkerhedsløsninger i fællesskab undgås forskellige løsninger og det er muligt at få dialog med Sundhedsstyrelse og Datatilsyn om de juridiske udeståender.
- Sundhed.dk og andre tiltag på tværs kræver, at amterne udveksler data om patienter og sikkerhedsrelevante data om personalet. For at skabe sikkerhed og effektivitet, bør der være standarder for data, der udveksles, og data bør fødes som en del af EPJ-systemerne. Hvis det skal være muligt, skal der være sammenhæng i sikkerhedsløsningerne for EPJ og for sundhed.dk mv.
- opbygningen af EPJ betyder, at der skal skabes integration til produktionssystemer og medico-tekniske systemer fra mange forskellige leverandører i sygehusene (røntgen, blodbank, laboratorium). For at undgå en situation, hvor der opbygges skræddersyede integrationer mellem hvert produktionssystem og hvert EPJ-system, skal der opbygges standardgrænseflader, herunder også standarder for sikkerheden. Der skal således også være sammenhæng mellem sikkerhedsmo-

sammenhæng mellem sikkerhedsmodellerne i EPJ og de kliniske systemer.

Alternativet til visionen om sammenhængende sikkerhedsmodeller for sundhedsvæsenet er, at amterne får store administrative byrder til at vedligeholde sikkerhedsdata om personalet i mange forskellige systemer i og udenfor amtet. En meget kompleks løsning vil give risiko for brud på sikkerheden.

2. Arkitektur

En skitse til en samlet arkitektur for IT-systemer i sundhedsvæsenet må tage udgangspunkt i de tre niveauer: Nationale systemer, EPJ-systemer og andre lokale systemer.

En samlet arkitektur må desuden designes med skyldigt hensyn til sikkerhedsmæssige krav, for kravene til tilgængelighed, kvalitet, fortrolighed og sporbarhed har særdeles høj prioritet i sundhedsvæsenets systemer.

Det er af stor betydning for både sikkerheden og systemernes effektivitet, at sikkerhed indgår i alle led i den samlede arkitektur og i alle faser lige fra vision over modellering og programmering til praktisk anvendelse. Der er desværre mange eksempler på, at man først sent i udviklingsprocessen "klistrer" sikkerhedsløsninger på et program, så hverken program eller sikkerhed fungerer tilfredsstillende. I G-EPJ indgår sikkerhed kun indirekte, f. eks. er G-EPJ tværfaglig, uden at modellen forholder sig til de sikkerhedsmæssige udfordringer, det giver.

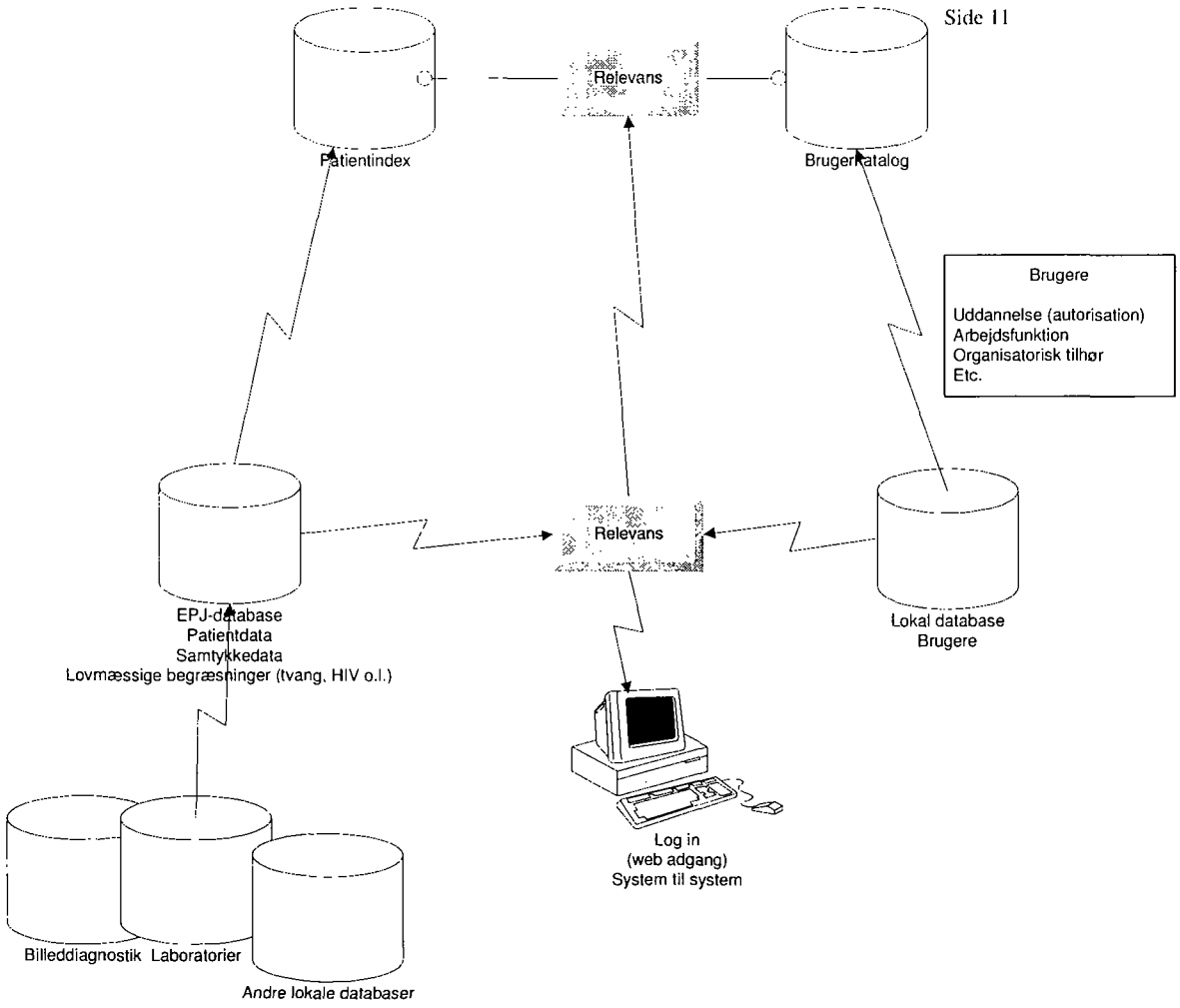
En samlet arkitektur må i den nuværende fase på sikkerhedsområdet indeholde følgende:

- en definition af grundlæggende begreber (f. eks. autentifikation, autorisation, brugeradministration, rettighedsadministration)

- arkitekturelementer (brug af OCES-certifikat, placering af brugeroplysninger i brugerkatalog, ikke i certifikat)
- sikkerhedskomponenter
- fælles regler (f. eks. for kontrol og arbejdsdeling)
- standard for udveksling af data om brugere
- aftaler om kontrol og opfølgning

Arkitekturen skal på samme tid fastlægge rammer for det videre arbejde og give rum for nyskabelser i et stærkt udviklingspræget miljø.

Figuren viser sammenhængene mellem amtslige systemer og nationale systemer. Det samlede system består af tre elementer, nemlig patientdata, brugerdata og en brugersession (login), som beskrives i det næste afsnit:



Figur Fejl! Ukendt argument for parameter.**: IT-arkitektur i sundhedsvæsenet: Generel model**

2.1 Samspil mellem amtslige systemer og nationale systemer

2.1.1. Patientdata

Der overføres patientdata fra en amtslig EPJ til det nationale system, f.eks. sundhed.dk. Ud over patientdata overføres sikkerhedsrelevante data omfattende f.eks. samtykke og information om begrænset adgang til data i forbindelse med tvang og HIV.

Arbejdet med at skabe standarder for patientdata er nået langt, men der er behov for at standardisere de sikkerhedsrelevante data i forbindelse med arbejdet med G-EPJ.

2.1.2. Brugerdata

Der skal overføres et begrænset sæt af data om brugerne fra amterne til sundhed.dk's brugerkatalog og til TDC i forbindelse med OCES-certifikater.

Denne overførsel kræver, at der i amterne er en sikker og effektiv bruger-administration, og der arbejdes derfor i flere amter på at sikre dette, bl.a. ved at etablere sammenhæng mellem lønsystemerne og brugeradministrationen, således at ændringer i ansættelsesforhold straks afspejles i brugerkatalogerne.

Sundhedsstyrelsen har igangsat et arbejde med at etablere et nationalt brugerkatalog for sundhedssektoren, og amterne indgår i dette arbejde. For amterne er det et mål, at de data, der skal anvendes på nationalt plan, kan fødes i amterne som en del af driften, og at der er standarder for de data, der skal overføres, samt regler for hvordan og hvornår, de skal overføres.

Amterne skal oprette og vedligeholde brugere af OCES-certifikater. I forbindelse med et pilotprojekt i Amtsrådsforeningens regi skal der udvikles effektive administrative rutiner hertil.

2.1.2.1 Rollebaseret brugeradministration

For at minimere ressourceforbruget til brugeradministration og samtidig skabe en fælles standard, der kan bruges til rettighedstildeling til fælles nationale systemer, f.eks. på sundhed.dk, og på tværs af sygehusejere, vil det være hensigtsmæssigt at gøre rettighedstildelingen rollebaseret.

Rollebaseret brugeradministration vil kunne løse en del af de problemer, der er med rettighedstildeling, men rollebegrebet er ikke entydigt.

Arbejdsgruppen anbefaler, at der udarbejdes et standardiseret rollebegreb, indeholdende flere dimensioner, herunder uddannelse (faglig risation), arbejdsfunktion og organisatorisk tilhørsforhold.

Udarbejdelsen af standardklassifikation(er) for roller i sundhedsvæsenet bør ske i tilknytning til specificeringen af det nationale brugerkatalog, som er igangsat i Sundhedsstyrelsens regi.

2.1.3. Sessionsdata

Ved den konkrete brug af det nationale system skal brugeren logge på og angive, at brugeren har patienten i behandling. Det kan ske på "tro og love" eller der kan overføres systemdata fra brugerens system, som viser, at patienten er registreret i behandling i det pågældende system.

Der bør arbejdes på at minimere brugen af tro og lov erklæringer og på at etablere en fælles systemløsning.

2.2 Samspil mellem EPJ-systemer og produktions- og medico-tekniske systemer

En arkitektur for systemerne i den danske sundhedssektor må på længere sigt også omfatte samspillet mellem EPJ-systemerne og produktionssystemer (laboratorium, blodbank, røntgen m.v.) og medico-tekniske systemer.

Status for systemerne er, at sygehusene i dag har valgt EPJ-løsninger fra forskellige leverandører, og at der anvendes en bred vifte af produktionssystemer, med flere leverandører af systemer, der løser samme opgave. Det kan forventes, at der vil komme stadig flere produktionssystemer og

produktionssystemer og mere medico-teknik, som skal løse specialiserede opgaver.

Det er også en del af visionen om EPJ, at der etableres tæt integration mellem EPJ og produktionssystemer, så læger og sygeplejersker fra EPJ kan bestille ydelser og se resultater fra f. eks. blodbanksystemet.

Det betyder en risiko for, at hvert amt/sygehus udvikler en skræddersyet integration mellem EPJ og de lokale systemer. På den ene side betyder det store udgifter til leverandørerne, på den anden side betyder det, at leverandørerne skal binde store ressourcer i at udvikle integrationsløsninger til mange systemer i stedet for at forbedre funktionaliteten i produktionssystemerne.

Det vil være hensigtsmæssigt at opbygge standard-grænseflader mellem EPJ og de øvrige systemer, herunder også grænseflader for sikkerhed. Der er f. eks. behov for sikkerhedsløsninger omkring HIV-data.

I den overordnede arkitektur er sikkerheden i produktionssystemer og medico-teknik kun relevant i den udstrækning der stilles krav til brugerdata fra amternes brugerkataloger. Sikkerhedsspørgsmål som alene vedrører systemet og dets primære brugere (blodbank-, røntgen- og laboratoriepersonale), er ikke omfattet.

Sikkerhed bør derfor indgå i IT-arkitekturgruppens arbejde. En standardiseret IT-sikkerhedsarkitektur bør tage udgangspunkt i internationalt anerkendte standarder.

2.3 Fælles komponenter

Der er allerede truffet beslutning om en række fælles komponenter i den danske sundhedssektor:

- Sundhedsdatanettet
- OCES-certifikat med begrænset indhold og mulighed for opslag af bl.a. CPR-nummer
- Sundhedsstyrelsens autorisationsregister
- Sundhed.dk
- Nationalt brugerkatalog for sundhedssektoren (under specifikation bl.a. med udgangspunkt i eksisterende løsninger)

Sundhedsstyrelsens tiltag med Sundhedsstyrelsens Elektroniske Indberetningssystem (SEI) falder ikke inden for rammerne af ovenstående. På datasiden skal der bruges data som allerede er registreret en gang, hvilket medfører dobbeltregistrering. På den tekniske side er SEI i modstrid med Offentlig Information Onlines (OIO) referenceprofil. Endelig er løsningen på den sikkerhedsmæssige side ikke sammentænkt med eksisterende løsinger, hvilket betyder dobbelt arbejde.

Det anbefales at Amtsrådsforeningen og sundhed.dk arbejder på, at SEI bringes i sammenhæng med de øvrige systemer.

2.4 Kontrol og opfølgning

Lovgivningen stiller krav om, på hvilke betingelser en sundhedsperson må se data om en patient. Grundlæggende gælder, at sundhedspersonen skal have patienten i behandling for at kunne få adgang til patientens data.

Der er dog ikke klart sammenfald i reglerne i Patientrettighedsloven og Persondataloven. Hvor patientrettighedsloven har fokus på patientens behandling, stiller Persondataloven krav om, at programmerne skal have indbyggede "låse", der sikrer mod uretmæssig tilgang til data.

I de tilfælde, hvor en patient er henvist til behandling i et amt, vil et opslag i sundhed.dk kunne ske via det lokale system, som så kan overføre et "bevis" for behandlingen. I nogle tilfælde vil det ikke være muligt, og så må der afgives en erklæring om behandling på "tro og love".

Under alle omstændigheder bør der være en efterkontrol, hvor det kontrolleres, om sundhedspersonen rent faktisk har haft patienten i behandling. I modsat fald må der gribes ind. Der skal informeres om denne kontrol, idet det vil kunne dæmpe et eventuelt misbrug. Det er også muligt at give patienterne selv adgang til at se loggen over, hvem der har haft adgang til data, som det i dag er tilfældet i sundhed.dk.

Da lovgivningen på området giver fortolkningsmuligheder, og da der er en vis usikkerhed i amterne og hos de centrale myndigheder, vil det være hensigtsmæssigt med et samarbejde om fortolkning og eventuel regelafklaring. Det kan sikre, at der er klare linier og samme fortolkning i forhold til sundhed.dk's sikkerhedsmodel og i amternes sikkerhedsmodeller til EPJ.

Ønsket om, at sundhedspersonale kan få adgang til patientdata i "fremmede" systemer, betyder særlige krav til sikkerheden og opfølgningen på den. Når sundhedspersonen tilgår patientdata i eget sygehus, har sygehusejeren forpligtelsen til at kontrollere, at personalet kun tilgår relevante data, og sygehusejeren har muligheden for at kontrollere og i givet fald gribe ind. Når sundhedspersonalet ansat hos en sygehusejer tilgår patientdata hos en ekstern part, kræves der særlige tiltag for at sikre, at der gennemføres den nødvendige kontrol og opfølgning:

- Der skal derfor logges (eller overføres log-data) hos den ansættende myndighed, som så kan kontrollere, om tilgang til patientdata er sket i forbindelse med en behandling hos myndigheden.

myndigheden. Det skal aftales, hvilke procedurer, der skal gælde for logning og opfølgning, herunder hvordan brud på reglerne skal indberettes til den part, der har stillet patientdata til rådighed.

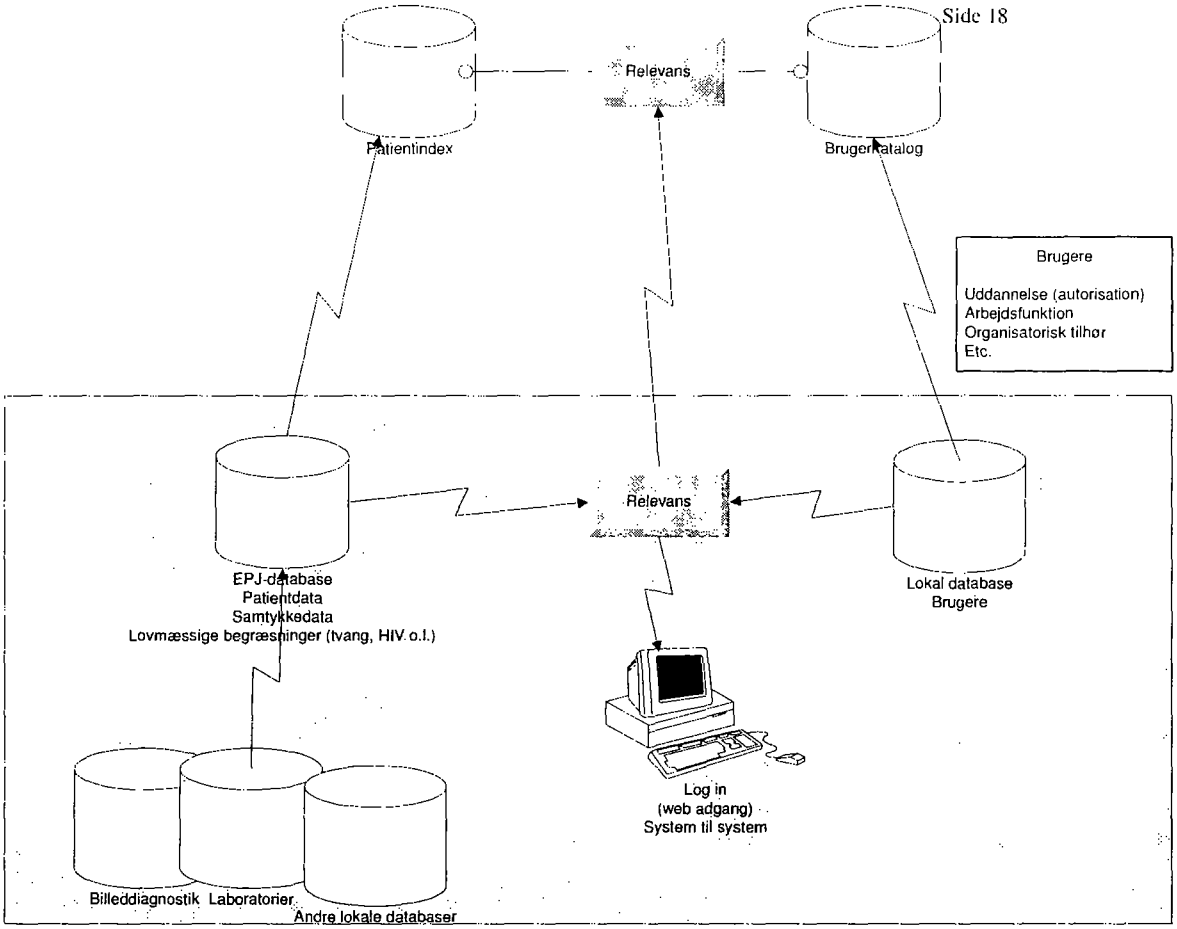
- Der skal logges hos den dataansvarlige, som skal gennemgå loggen. I tilfælde af brud på sikkerheden skal den ansættende myndighed kontaktes efter indgåede aftaler.
- Adgang på "tro og love" bør begrænses mest muligt, og i de tilfælde, hvor det er nødvendigt med adgang på "tro og love", skal den ansættende myndighed have skærpet tilsyn med loggen.
- Da der kan forventes store mængder logningsdata, vil det være nødvendigt med maskinel analyse, og der skal derfor være standarder for udveksling af logningsdata. (se også afsnit 3.7.1, s. 27).

- Endelig kan patienten gives adgang til logoplysninger.

3. Lokale/decentrale sikkerhedsløsninger

Sikkerhedsgruppen har analyseret hvilke krav der bør stilles til decentral/lokale sikkerhedsløsninger. Resultaterne af analysen præsenteres i dette kapitel. For hver hvert område gives oplysninger om relevante problematikker, status for udviklingen og anbefalinger for fremadrettede aktiviteter. Det anbefales, at amterne inddrager de nævnte områder i deres sikkerhedsovervejelser.

Det farvede område i nedenstående figur indikere afsnittets fokus i forhold til den generelle model (**Fejl! Ukendt argument for parameter.**, s. 11).



Figur Fejl! Ukendt argument for parameter.: **IT-arkitektur i sundhedsvæsenet: Decentrale/lokale sikkerhedsløsninger**

3.1 Indledning

Adgangen til patientdata skal være baseret på en række overordnede krav, som skal være opfyldt. Generelt bør der opstilles en central politik, som skal udtrykke såvel krav til identifikation af sundhedsaktør og patient som krav til en relation mellem disse, for at kunne tildele sundhedsaktørerne de relevante adgange til systemfunktioner med patientens data.

En sådan politik kan f.eks. indeholde følgende:

- Adgang til data skal være baseret på behov.

- Patient og sundhedsmedarbejder skal være sikkert identificerede fysiske personer.
- Der skal eksistere en behandlings- eller plejerelation.
- Patienten skal have indflydelse på, hvilke data der gøres tilgængelige for sundhedsmedarbejdere.
- Patientdata skal tilgås efter princip om nødvendighed og tilstrækkelighed.
- Patientdata kan anvendes til forskning, kvalitetssikring, administrativ kontrol og statistik.

3.2 Patient

I dette afsnit beskrives de krav til informationssikkerhed, der knytter sig til patienten som person.

3.2.1. Samtykke til videregivelse

Hvis patientretsstillingslovens krav til indhentning af samtykke skal overholdes, kræver det ressourcer i det daglige arbejde på sygehusene, dels for at indhente samtykke, dels for løbende at sikre, at man overholder patientens ønsker.

Etableringen af en decentral samtykkekomponent kan ske i flere faser.

I første fase etableres et decentralt samtykkemodul til registrering af patientens samtykkeoplysninger pr. behandlingsforløb. Oplysningerne skal kunne tilgås på et hvilket som helst tidspunkt i forløbet.

I en senere fase kan der i tilknytning til en generel sikkerhedsløsning etableres en komponent, som på basis af patientens samtykkeoplysninger automatisk sikrer, at beskyttede data ikke kan tilgås, uden at der genereres en afvigelsesrapport herom.

Det anbefales, at der etableres en standard for samtykkemodul/-komponent. Det bør overvejes, om der skal etableres en generel løsning, der kan anvendes på tværs af sygehusejere og sektorer.

Ovennævnte generelle løsning kan tage udgangspunkt i den samtykke facilitet der er etableret på sundhed.dk til brug for den personlige elektroniske medicinprofil (PEM).

Lovgivningsmæssige og funktionelle krav til samtykkemodul/-komponent fremgår af bilag 9.

3.2.2. Forbehold mod adgang

Forbehold for samtykke omfatter muligheden for at give samtykke til at alle må se oplysninger såvel som mulighed for at blokere enkelte personers adgang til data. Patientretsstillingsloven giver mulighed for, at patienten kan nægte samtykke til videregivelse af oplysninger til bestemte personer. Arbejdsgruppen vurderer, at det vil være vanskeligt at tilgodese dette behov i struktureret form i en IT-løsning.

Det anbefales derfor, at specifikke samtykkeoplysninger indtil videre håndteres manuelt eller evt. via et fritekstfelt i samtykkemodulet samt at der gennemføres nærmere undersøgelser af problematikken.

3.3 Patient-behandler relation

Som nævnt ovenfor, skal sundhedspersonalets rettighed til adgang til EPJ være baseret på behov. Behov opstår gennem en relation mellem sundhedsaktøren og patienten. Herved opstår en relevans, som legitimerer sundhedsaktørens adgang til patientens data.

Relationen vil principielt være bestemt af:

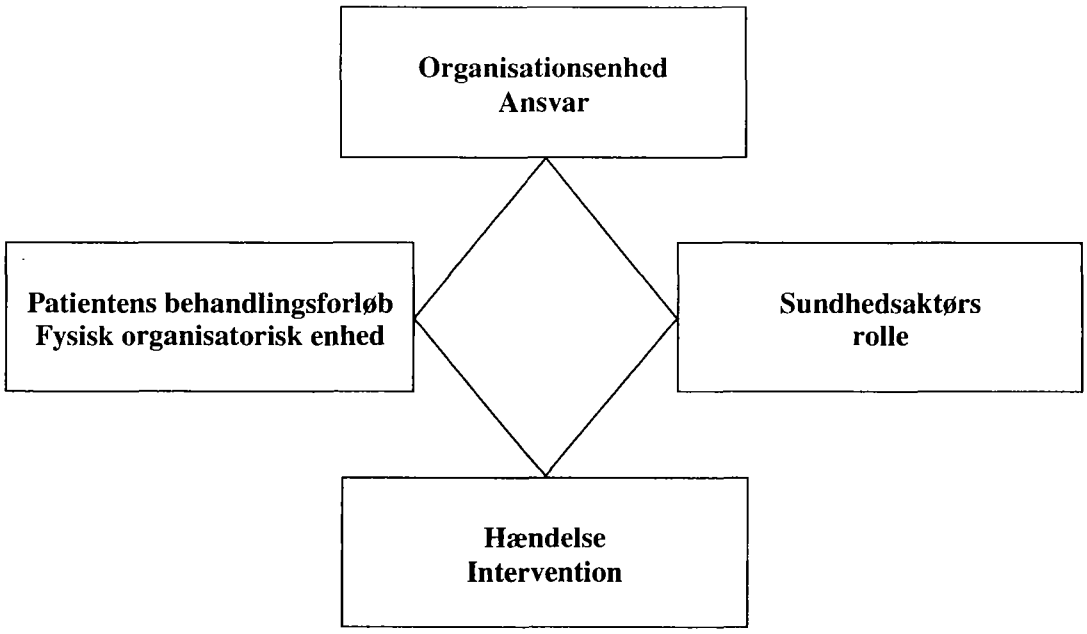
1) organisationstilhørsforhold,

2) sundhedsaktørens rolle,
3) patientens behandlingsforløb samt
4) hændelse/intervention.

Udover at behovet skal være tilstede kræves patientens samtykke.

Når et behov kan konstateres, skal sundhedsaktøren tildeles de nødvendige og tilstrækkelige rettigheder for adgang til patientens data.

Behovsrelationerne kan i en "idealmodel" illustreres således:



Figur Fejl! Ukendt argument for parameter.: **Idealmodel for patient-behandlerrelationen**

I det følgende behandles de fire dimensioner i relation til etablering af behov.

3.3.1. Organisationsenhed

Tilknytningen til en organisationsenhed, der varetager behandlingen af en patient (har behandlingsansvar), giver en sundhedsaktør med behov for adgang til patientens data. Men også sundhedsaktørens tilknytning til en organisationsenhed, der er forløbsansvarlig eller plejeansvarlig kan legitimere et behov.

Andre sundhedsaktører end de her nævnte kan have behov, som principielt er uafhængige af, om der eksisterer en organisatorisk tilknytning i relation til patienten. Sådanne behov bør defineres via opgaven og placeres i hændelses/interventionsdimensionen.

3.3.2. Sundhedsaktørs rolle

Sundhedsaktøren er en entydigt identificerbar sundhedsperson med en klassificeret uddannelse ansat med en bestemt funktion og stillingsbetegnelse.

En sundhedsaktør kan varetage en eller flere roller, som bl.a. defineres af vedkommendes arbejdsfunktioner og ansvar med en vis detaljeringsgrad. Behov for adgang til patientdata opstår således i kraft af disse arbejdsfunktioner og det tilhørende ansvar.

Det vil være muligt også at medtage aktører, som ikke er autoriserede sundhedsaktører i denne dimension. Personale i f.eks. administrative og økonomiske funktioner kan på tilsvarende vis tildeles roller som beskriver arbejdsfunktioner og ansvar.

3.3.3. Hændelse/intervention

Sundhedsaktørens kontakt med patienten sker gennem en hændelse eller en intervention, hvor intervention er en klinisk behandlingsmæssig hændelse. Hændelsesbegrebet kan således opfattes som enhver situati-

situation/anledning, der etablerer et behov hos sundhedsaktøren for information om patienten. Dermed kan det også bringes til at omfatte sundhedsaktører, der gennem deres rolle har behov for patientdata til hændelser som forskning, kvalitetssikring, statistik mv. Hændelser kan eksempelvis også være rekvireringer af ydelser, bookinger, tilsyn mv. Endelig kan det også bringes til at omfatte administrativt personale, som har behov for adgang til patientdata i forbindelse med økonomiske opgørelser mv.

3.3.4. Patientens behandlingsforløb

En patient kan gennemgå et eller flere samtidige behandlingsforløb, som hver for sig kan udløse behov for at en sundhedsaktør får adgang til patientinformation eller til at skabe ny information.

Der vil principielt være behov for at kunne skelne mellem flere forskellige både åbne/aktive og lukkede behandlingsforløb, da rettighederne hertil kan være forskellige.

Forbindelsen (og dermed behovet) mellem patienten og sundhedsaktøren kan opstå enten via den organisatoriske dimension eller via hændelse og interventions dimensionen. Sundhedsaktørens behov opstår således i kraft af vedkommendes rolle kombineret med enten organisatorisk tilhørsforhold eller deltagelse i en hændelse/intervention.

Beskrivelse og anvendelse af det hændelsesrelaterede forventes udbygget i implementeringen af G-EPJ.

3.4 Rettighedstildelingen

Når et behov er konstateret, skal der til sundhedsaktøren tildeles de nødvendige og tilstrækkelige rettigheder. Disse rettigheder vil principielt omfatte adgang til funktioner (system- og forretningsfunktioner) og data i IT-systemerne.

Ved systemfunktioner forstås de generelle typer af systemadgang, der kan gives som læserettighed, skrive/ændrerettighed, ret til oprettelse, nedlæggelse og sletning. Endvidere kan der være tale om ret/adgang til at godkende (ret til at markere data som godkendt), administrere (ret til at specificere andres rettigheder) og vide (ret til at kende til eksistensen af bestemte data). Det skal understreges, at sletning af data ikke sker rent fysisk, men kun logisk ved markering.

Ved forretningsfunktioner forstås de funktioner et givet system stiller til rådighed som støtte for udførelsen af arbejdsmæssige funktioner, f.eks. at ordinere medicin.

Rettighederne kan eventuelt også differentieres på det enkelte systems dataindhold, såfremt dets datastruktur muliggør det. Eksempelvis kan der differentieres på en patients stamdata, demografiske data, aktuelt behandlingsforløb og tidligere behandlingsforløb.

Mulighederne for at differentiere og tildele rettigheder vil være forskellige og afhænge af det enkelte system/moduls funktioner/menuer og datastruktur.

3.5 Problemer ved "idealmodellen"

Der er en række problemer ved de enkelte dimensioner og relationerne imellem dem, som p.t. gør det praktisk umuligt at gennemføre en rettighedsstyring, baseret på "idealmodellen".

Ingen af dimensionerne i modellen kan p.t. siges at være veldefinerede, om end der er en række tiltag i gang i sundhedsvæsenet, som på sigt vil give mulighed for også at basere en differentieret rettighedstildeling herpå.

Den organisatoriske struktur behandles p.t. af Sundhedsstyrelsen gennem nye forslag til klassifikation af organisatoriske enheder på sygehusene.

Det anbefales at den sikkerhedsmæssige dimension inddrages i arbejdet med en ny sygehusafdelingsklassifikation.

Det anbefales desuden, at begreber i G-EPJ modellen beskrives, så de kan anvendes i en sikkerhedssammenhæng.

Ovennævnte bør ikke forhindre, at der i kravene til fremtidige systemer opstilles krav/ønsker, som giver mulighed for etablering af en differentieret rettighedsstyring på alle dimensioner.

En eventuel realisering af den differentierede rettighedsstyring skal dog altid afvejes mod hensynet til at patientens behandling kommer først, og at sikkerhedshensyn ikke unødigt må komplicere brugen af systemerne under dagligdagens opgaver på sygehusene.

3.6 Brugeradministration

Der bruges i dag mange ressourcer på brugeradministration i de applikationer, der anvendes i sygehusvæsenet. På trods heraf er sikkerhedsniveauet generelt for lavt, fordi det er vanskeligt at styre rettighederne korrekt i de mange applikationer. I takt med, at dels antallet af brugere stiger og dels, at kompleksiteten i applikationerne stiger, er der behov for en generel sikkerhedsløsning, der kan håndtere sikkerheden for flere/alle applikationer baseret på medarbejdernes uddannelse, arbejdsfunktion og organisatoriske tilhørsforhold.

Sikkerhedsgruppen anbefaler, at man for at forenkle brugeradministrationen gør den rollebaseret.

Herved opnår man, at der ikke skal specificeres en brugerprofil for hver enkelt medarbejder, men for den gruppe af medarbejdere, der varetager samme arbejdsfunktion.

Eftersom brugere af sundhedsvæsenets systemer skal kunne tildeles rettigheder på fælles applikationer (f.eks. via sundhed.dk og SEI) og ved forespørgsler på eksterne applikationer hos andre sygehusejere, er det nødvendigt, at der etableres en klassifikation af arbejdsfunktioner, som anvendes på tværs af alle sygehusejere. Sundhedsaktører foreligger klassificeret af Sundhedsstyrelsen, men for denne og de øvrige dimension i rollebegrebet forefindes p.t. ingen umiddelbart anvendelig klassifikation.

Det anbefales, at arbejdsgruppen vedr. brugerkatalog, som sekretariatbetjenes af Sundhedsstyrelsen, tager problemet op.

Medlemmer af sikkerhedsgruppen indgår i ovenstående arbejdsgruppe. Klassificering af arbejdsfunktioner på et overordnet fælles niveau bør være output fra denne gruppe.

Beskrivelse af krav til beskrivelse af arbejdsfunktioner findes i bilag 5

3.6.1. Generel brugeradministrationskomponent

For hver applikation skal det være muligt i brugeradministrationskomponenten at beskrive de regler, hvorefter de enkelte grupper af medarbejdere får tildelt rettigheder afhængigt af arbejdsfunktion og evt. organisatorisk tilhørsforhold. For at muliggøre det bør der laves en standard for brugeradministration.

Arbejdsgruppen anbefaler, at sygehusejerne decentralt anvender en generel brugeradministrationskomponent, der kan håndtere rettighedsstyring for alle applikationer.

Arbejdsgruppen anbefaler, at der fastlægges en standard for, hvilken delmængde af data, der skal stilles til rådighed om en bruger, der ønsker at søge på patientinformation i centrale applikationer eller hos andre sygehusejere.

3.7 Kontrol og opfølgning

3.7.1. Krav til logning

Persondataloven stiller krav om, at der foretages adgangs- og transaktionslogning af al aktivitet på de IT-systemer, hvor der er personhenførbare data. Inden for sundhedsvæsenet betyder det, at stort set alle IT-systemer er underlagt disse krav.

Da der potentielt er tale om meget store mængder data, der generes ved transaktionslogning, er det vigtigt at få fastlagt, på hvilket niveau, det er nødvendigt at foretage logningen for at kunne opfylde lovgivningens krav. Dette niveau vil være det normale logningsniveau. I forbindelse med fejlfinding eller i andre situationer, hvor der er behov herfor, kan det være nødvendigt i en periode at hæve logningsniveauet.

For at opnå en enkel og effektiv håndtering af logoplysninger, er det nødvendigt at man kan beskrive regler for, hvilke transaktioner eller kombinationer af transaktioner i hver enkelt applikation, der skal udløse en advarsel eller alarm.

Herudover skal en logkomponent kunne håndtere udtræk af logoplysninger efter en række forskellige kriterier. Udtrækkene skal kunne bruges til

kunne bruges til konkret behandling ved mistanke eller til stikprøvekontroller.

Der skal udarbejdes generelle regler for, hvor længe forskellige typer logoplysninger skal opbevares. Af både praktiske og økonomiske årsager, bør detaljerede logoplysninger om bl.a. forespørgsler kunne slettes efter 6 måneder jf. persondatalovens krav. Ændringer af data skal imidlertid altid kunne dokumenteres i hele journalens levetid, enten i selve journalen eller i særlige ændringslogge, der skal indgå som en integreret del af EPJ-systemet.

Da det drejer sig om store mængder af data fra mange forskellige systemer, vil det være hensigtsmæssigt, at der etableres en generel logkomponent, som kan samle transaktions logoplysninger fra de tilknyttede applikationer og databaser (se bilag 8)

Det anbefales, at der laves en standard for funktionalitet og arbejdsgange for kontrol og opfølgning ved logning (se også afsnit 2.4, s. 15).

3.7.2. Borgerens adgang til logoplysninger

Arbejdsgruppen har vurderet, at det vil være hensigtsmæssigt, at borgerne f.eks. via en Web-klient kan få adgang til deres egne logoplysninger. Det vil bidrage til at øge opmærksomheden hos personalet på, at man kun skal anvende information, der er direkte relevant i forhold til den aktuelle behandling. Det bekræfter behovet for standardiserede logdata.

3.8 Validitet

EPJ-systemer indeholder data, der kan have direkte indflydelse på patientens behandlingsforløb. Der må således ikke herske tvivl om disse datas validitet. Med andre ord skal den enkelte behandler have tillid til de præ-

præsenterende data, herunder også data, der præsenteres af en fremmed sygehusejer.

Præsentationen af valide data forudsætter især to ting: For det første, at der er mulighed for entydigt at identificere patientens data og for det andet at der er enighed om og fælles forståelse af hvilke data, der stilles til rådighed og hvorledes disse stilles til rådighed.

3.8.1. Identifikation af patienternes data

I forbindelse med etableringen af den EPJ og en øget informationsudveksling mellem sygehusene, praksissektoren og kommunerne i Danmark skal det sikres, at patienterne altid er sikkert og entydigt identificeret.

Dette sikres generelt ved anvendelse af CPR-nummeret til identifikation af patientdata. Flere grupper af patienters data lader sig dog ikke identificere via CPR-nummeret, fordi et sådant ikke haves eller er tildelt endnu. Dette gælder bl.a. personer med flygtningestatus (flygtningnummer), udenlandske statsborgere, hjemmefødte børn og personer, der ikke kan identificeres.

Ved kontakt til eksempelvis sygehuset tildeles disse patienter med et erstatnings-CPR-nummer i regi af den enkelte sygehusejer eller det enkelte sygehus. Denne tildeling er lokalt styret og kun i ringe grad koordineret udover det amtslige plan.

Hvis patienten senere (i behandlingsforløbet) tildeles et CPR-nummer udskiftes erstatnings-CPR-nummeret.

Den nuværende brug af erstatnings-CPR-numre giver anledning til to problematiske forhold. Det første og væsentligste er at der på nationalt plan ikke er en unik nøgle til det enkelte individs data. Det andet er at det

enkelte individs erstatnings-CPR-numre oftest ikke er det samme for forskellige behandlingsforløb.

Fordi brugen af erstatnings-CPR-numrene ikke er "synkroniseret" på nationalt plan, har man ved overflytning mellem sygehuse eller amter er således ingen sikkerhed for, at data fra forskellige patienter, oprettet med samme erstatnings-CPR-nummer, ikke blandes sammen.

Ved gentagne behandlinger af personer med flygtningestatus anvendes forskellige erstatnings-CPR-numre, fordi det er tidskrævende at henføre et flygtningenummer til et tidligere erstatnings-CPR-nummer. Konsekvensen er at det er sværere at skabe et overblik over det enkelte individs behandling, og stort set umuligt, på sigt, at fortage en forløbsbaseret indberetning af patientdata, for denne gruppe.

I dag oprettes disse patienter med et erstatnings-CPR-nummer hos den enkelte sygehusejer eller på det enkelte sygehus. Ved overflytning mellem sygehuse og amter er der således ingen sikkerhed for, at data fra forskellige patienter, oprettet med samme erstatnings-CPR-nummer, ikke blandes sammen.

For at øge sikkerheden ved personidentifikationen er det Sikkerhedsgruppens opfattelse, at der bør etableres en landsdækkende service til generering af erstatnings-CPR-numre, der sikrer, at samme nummer kun kan vedrøre én patient, og at en patient kun har ét erstatnings-CPR-nummer.

Det mest hensigtsmæssige vil være, at servicen leveres fra det Centrale Personregister, som er ansvarlig for udstedelsen af CPR-numre. Det anbefales derfor, at der tages kontakt til Indenrigsministeriet, som er ansvarlige for det Centrale Personregister med henblik på at drøfte mulighederne for etablering af denne service.

Alternativt må det overvejes, om man kan etablere en landsdækkende service i samarbejde mellem amterne, evt. som en web-service tilknyttet sundhed.dk.

3.8.2. Standardisering af data til udveksling

Det forhold, at der i forskellige decentrale systemer haves data om det enkelte individ, giver anledning til nogle datatekniske problemstillinger.

Eksempelvis er den enkle dataværdi kun interessant, når omstændigheder hvorunder det er indsamlet er kendte. Tallet 8,9 er intetsigende, mens den omstændighed, at der er tale om en hæmoglobinværdi, gør forholdet mere interessant. Hvis det samtidig er kendt, at der er tale om 8,9 mmol/l og at blodprøven er taget i går, så kan disse informationer (data) også anvendes i klinikken.

Der er således tale om et samlet datasæt med en kendt struktur (vi kan identificere hæmoglobinværdien, prøvetagningsdatoen mv.). En sådan udveksling af, eksempelvis ovenstående simple data, skal kunne ske elektronisk og automatisk, stiller krav om nøje fastlagte udvekslingsprocedurer i form af standarder.

En konsekvens af dette forhold er bl.a., at der er udviklet EDI-standarder i regi af MedCom til udveksling af eksempelvis blodprøvesvar. En standard der i dag benyttes tusindvis af gange dagligt.

Set i et større perspektiv skal for hvert område, hvor der udveksles data, fastlægges en accepteret standard mellem de involverende parter (sygehuse/sygehusejere).

For sundhedsområdet findes i dag en del standarder. Eksempelvis EDI-standarderne fastlagt i regi af MedCom, den internationale DICOM-

standard til udveksling af billeder, HL7 og HISA for individuelle sundhedsdata mv.

Generelt gælder imidlertid, at de gældende standarder er udviklet til praktiske kommunikationsformål som oftest kun dækker specielle specifikke delområder af det samlede sundhedsområde - eksempelvis 'sygehushenvisning', 'udskrivningsepikrise', 'laboratoriesvar', 'recept' etc. Tilbage er et udækket område, hvor der vil skulle udvikles nye standarder eller alternativt benyttes andre måder til udveksling af data.

I forbindelse med standardisering nævnes ofte XML som et svar på næsten alle integrationsbehov. Det er i denne forbindelse vigtigt, at være klar over, at XML kun er et "programmeringssprog" eller en teknisk "kommunikationsform", der ikke i sig selv siger noget om indholdet.

For at blive en anvendelig standard, skal der ud over XML-kode også etableres en fælles og accepteret datamodel med tilhørende fælles begrebslige/semantiske forståelsesrammer og fælles aftalte forretningsregler.

Det anbefales at der laves en samlet oversigt over EPJ-relaterede standarder der anvendes i sundhedsvæsenet.

Udviklingen af nye standarder og forbedringen af eksisterende er en proces, der løbende pågår. Eksempelvis har Sundhedsstyrelsen for nylig udgivet G-EPJ-standarden i version 2, HL7 version 3 er under ratificering osv.

3.8.2.1 Måder til udveksling af data

Det er nærliggende, når standardiseringsarbejdet lader vente på sig, at se efter andre løsningsmodeller end dataudveksling mellem systemer. En måde, der anvendes i dag er visning af data i web-browser.

Brugen af internettet forudsætter, at data vises (håndteres) efter en nærmere fastlagt standard, således at det enkelte system (platform) kan vise data fra internettet, i overensstemmelse med dataejerens intentioner og krav til sikkerhed. Dette forhold kan også udnyttes i EPJ-sammenhæng, hvor eksempelvis sundhed.dk stiller data til rådighed via en web-browser.

Til visningen af data skal gøres to bemærkninger. Der findes i øjeblikket ikke en "standard" for selve visningen af data (skærmbilledet). Dette betyder, at to dataejere vil kunne vise data om samme forhold på vidt forskellig måde. Et forhold, der vil være et irritationsmoment hos den enkelte bruger. For det andet har læger m.fl. (f.eks. jordemødre og tandlæger) en pligt til at dokumentere beslutningsgrundlaget (se f.eks. bekendtgørelse om lægers pligt til at føre ordnede optegnelser (journalføring) LBK Nr. 272 af 19/04/2001). Et forhold der besværliggøres, hvis data kun vises for brugeren.

I systemer hvis data har indflydelse på den lægelige behandling af mennesker, fordres naturligt en høj datakvalitet. Der må således stilles krav om, at datainput og -output valideres. Eksempelvis via modulus 11 på CPR-numre, referencerammer/klassifikationer for indtastede værdier og output.

Sikkerhedsgruppen anbefaler, at sundhed.dk og MedCom vurderer behovet og muligheden for at standardisere visningen af (en anden dataejers) data i en web-browser, således at den enkelte bruger i størst muligt omfang præsenteres for et ensartet lay-out for analoge IT-systemer.

Sikkerhedsgruppen anbefaler endvidere, at der i regi af Amtsrådsforeningen fastlægges en "best practice" for arbejdsgangene i relation til dokumentation af beslutningsgrundlaget ved brug af elektroniske beslutnings-

elektroniske beslutningsstøtte værktøjer, herunder tager stilling til, hvordan historikfunktioner kan anvendes.

Forhold om berigtigelse af data skal afklares. Forholdet bør ikke give anledning til problemer i lokale systemer, hvor historikken er kendt. Men i tilfælde hvor fejlagtige data er distribueret til et andet system eller vist til en person uden for egen organisation, kan det være svært, at notificere om berigtigede data. Mål og metode skal afklares på dette punkt.

3.8.3. Service level agreement (SLA)

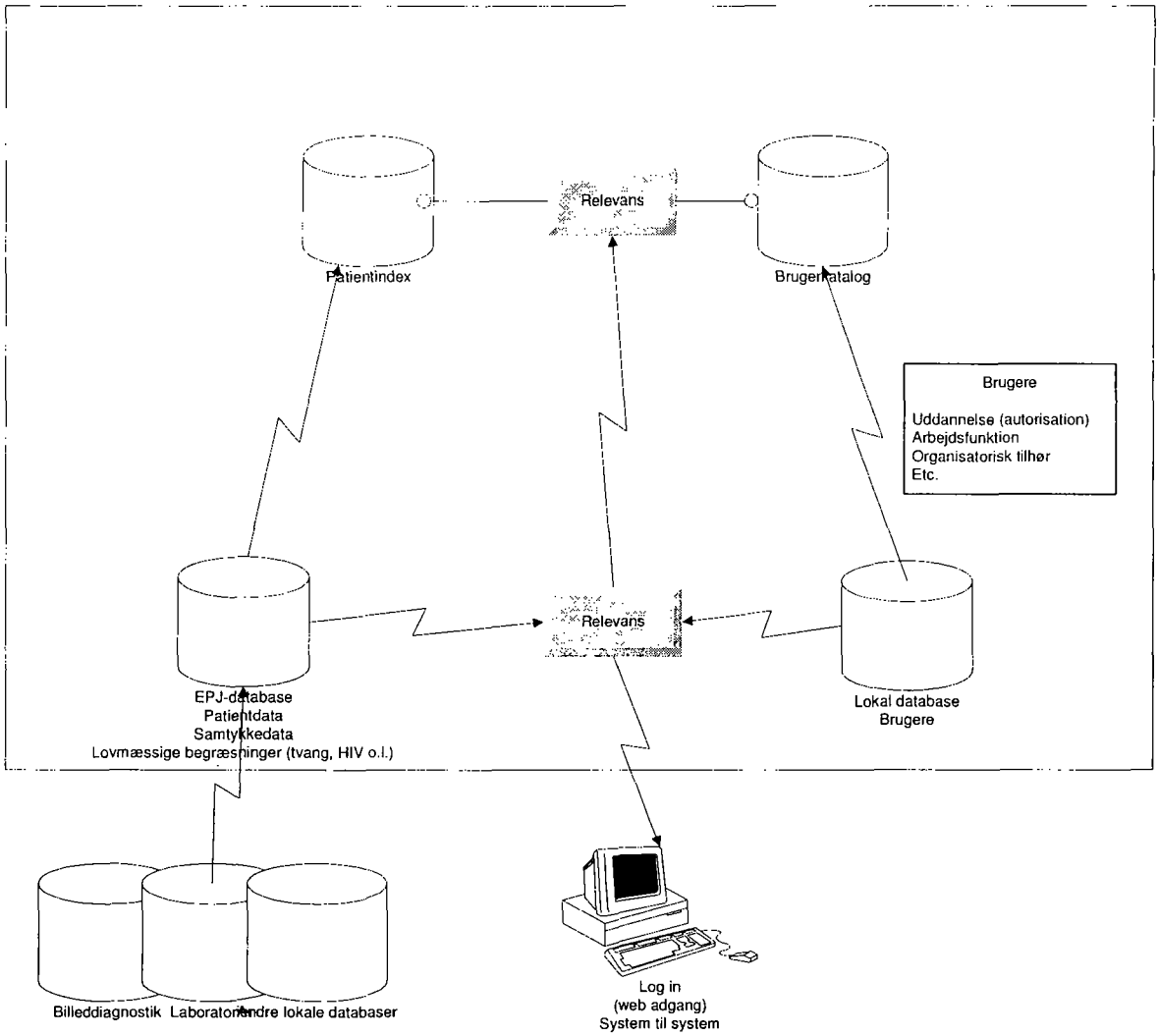
Især for systemer med ekstern anvendelse vil der være behov for, at fastlægge et serviceniveau. Dette gælder eksempelvis hvad der garanteres af oppetid, svartider, fastlagt driftsstop, hvornår systemet serviceres, varsel for orientering om ændringer, nye versioner mv.

Det anbefales at der udarbejdes en fælles amtslig Service Level Agreement, der specificerer krav til oppetid, reaktionstider i forbindelse fejl på viste data osv.

4. Nationale systemer og kommunikation på tværs

Sikkerhedsgruppen har analyseret forskellige modeller for en sammenhængende sikkerhedsstruktur for decentrale amtslige systemer og centrale nationale systemer og registrer. Resultatet af dette arbejde præsenteres i dette kapitel.

Det farvede område i figuren nedenfor indikerer hvilken del af den generelle model (Figur **Fejl! Ukendt argument for parameter.**, s. 11) som kapitlet fokuserer på.



Figur Fejl! Ukendt argument for parameter.: **IT-arkitektur i sundhedsvæsenet: Fælles sikkerhedsstruktur**

4.1 Indledning

Adgangen til relevant og opdateret patientinformation på tværs af sektorer og sygehusejere har længe været et stort behov. Dels er patienter blevet mere mobile, så der er flere aktører involveret i undersøgelse og behandling, dels er informationsmængden blevet så stor, at det kan være vanskeligt at finde den relevante information.

Patientrelaterede sundhedsoplysninger skal således være et fælles aktiv for alle relevante interessenter - herunder patienten selv - og skal kunne

tilgås uafhængigt af (føde)system, tid og lokation, dog under overholdelse af autorisations- og sikkerhedskrav.

Arbejdsgruppen har vurderet forskellige løsninger for at give adgang til patientdata på tværs i sundhedssektoren og sikkerhedsløsninger i sammenhæng hermed.

Gruppen har undersøgt og vurderet modeller med forskellige grader af distribution og centralisering. I vurderingen har der været skelnet mellem løsninger, der giver adgang til "historiske" patientdata, hvor data kun skal *læses*, og adgang til systemer med patienter i fælles behandling, hvor flere parter skal *skrive* data "på samme tid".

Som den ene yderlighed har gruppen vurderet *distribuerede* løsninger, hvor patientdata forbliver i det system, hvor data fødes, og hvor en ekstern sundhedsaktør tilgår dette system direkte. Den tilsvarende sikkerhedsmodel indebærer, at brugeren autentificeres og autoriseres af det databærende system, som kommunikerer direkte med brugersystemer i brugerens hjemamt.

> Fordelene ved distribuerede løsninger er, at data kun ligger et sted, og dermed undgås, at der opstår tvivl om data er de gældende.
>
> Blandt ulemperne ved løsninger, hvor data opbevares og skal tilgås i hvert amt, er, at hvert amt skal oprette extranetløsninger og håndtere sikkerhed i forhold til mange eksterne brugere.
>
> Der er ikke erfaring med de tekniske løsninger, der skal gøre sådanne distribuerede løsninger lette for brugerne og effektive at administrere, og de forventes at kræve en del udvikling.

Som den anden yderlighed har gruppen vurderet *centrale* løsninger, hvor patientdata samles i et nationalt patientindeks, som bl.a. kan tilgås via sundhed.dk, og hvor brugerdata ligeledes samles i et nationalt brugerkatalog. Gruppen anbefaler denne løsning til *læsning af data* i eksterne systemer.

Der er følgende grunde til anbefalingen

- det juridiske ansvar for data overtages af det centrale system, så det enkelte amt kun skal forholde sig til videregivelse af data.
- det enkelte amt skal kun overføre patientdata til en part.
- det enkelte amt skal kun skabe systemforbindelse til en part, patientindekset).
- brugerdata skal kun overføres til en part, det nationale brugerkatalog.
- der er teknologier, erfaringer og konkrete eksisterende løsningers baseret på denne model.
- løsningen har et enklere design med færre krav til standarder.

Opbygning af en sådan løsning kræver standarder for data og grænseflader.

Det er gruppens vurdering at løsninger til skrivning af data kræver yderligere analyse, men at de standarder, der udvikles til læsning af data, samtidig kan være udgangspunktet for de udvidede standarder, som en skriveløsning kræver.

4.2 Nationalt patientindeks

Etableringen af et fælles patientindeks skal understøtte flere formål, såvel klinisk, administrativt som IT-sikkerhedsmæssigt. I forhold til klinikeren skal indekset gøre det muligt via opslag med personidentifikation hurtigt at:

- Tilvejebringe de mest kritiske sundhedsoplysninger i en akut diagnosticerings- og behandlingssituation
- Tilvejebringe oplysninger om patientens forløb og kontakter til sundhedsvæsenet med henblik på at fremskaffe yderligere information

Administrativt skal patientindekset understøtte entydigheden i landsdækkende sundhedsoplysninger ved at tilbyde:

- Generering af en landsdækkende unik patientforløbsnøgle (på tværs af sektorer)

I relation til IT-sikkerhed er patientindeksets formål at:

- Tilvejebringe den nødvendige information til at sikre, at kun sundhedspersoner, for hvem det er relevant, får adgang til patientens data på tværs af sygehusejere og sektorer.

Dette dokument forholder sig primært til den IT-sikkerhedsmæssige vinkel, men i den sammenhæng vil genereringen af en unik forløbsnøgle også være relevant.

Alle aktører i sundhedssektoren er direkte interessenter i patientindekset. I første række vil sygehusene være de primære afgivere og modtagere af information, men på lidt længere sigt vil det være relevant for andre interessenter at kunne afgive og modtage sundhedsoplysninger. De direkte interessenter er udover sygehusene

- Borgerne (patienterne), praktiserende læger og speciallæger, tandlæger, andre autoriserede behandlere, apoteker, redningstje-

redningstjenester, hjemmepleje/plejehjem og sociale institutioner.

Patientindekset skal fungere i et heterogent miljø, bestående af et stort antal kliniske systemer hos de enkelte interessenter. Patientindekset skal indpasses mellem andre landsdækkende tværgående IT-løsninger, f.eks. det forløbsbaserede Landspatientregister og MedCom.

Arbejdsgruppen anbefaler en løsning, hvor der etableres et centralt patientindeks med egen database, der indeholder alle de væsentlige informationer om en given patient.

Dette vil teknisk, sikkerhedsmæssigt og juridisk være den enkleste løsning, som tillige vil kunne etableres forholdsvis hurtigt og tilgås via sundhed.dk.

4.3 Brugerkatalog

Når brugere på tværs af amter, kommuner og andre sundhedsaktører skal have adgang til eksterne systemer, er der behov for fælles metoder til at håndtere disse brugere, som vil være ansat i en organisation og bruge systemer i en anden.

I dag oprettes og administreres brugere i det enkelte amt **manuelt** i brugerkataloger (directories), som anvendes af amtets egne it-systemer. I princippet kan brugeradministration også ske manuelt, når der er tale om systemer på tværs, men i takt med at antallet af brugere stiger, vil det være ressourcekrævende uden direkte udveksling af brugeroplysninger mellem systemer. En sådan system-til-system udveksling vil dog forudsætte, at der i det enkelte amt er skabt en sammenhængende brugeradministration.

Arbejdsgruppen anbefaler en løsning, der baserer sig på et centralt brugerkatalog med data om de brugere, der skal tilgå systemer på tværs i sundhedssektoren, og hvor hvert enkelt system desuden har sit eget brugerkatalog, der er synkroniseret med det centrale brugerkatalog.

Modellen beskrives mere detaljeret i bilag 6.

Amterne overfører et begrænset sæt af data om brugerne til det centrale, nationale brugerkatalog. Da der bruges OCES-certifikat til autentifikation, skal der ikke håndteres password i løsningen.

Da hvert system har sit eget brugerkatalog, er driftssikkerheden knyttet til det enkelte system og kan afpasses efter behovene.

Det nationale brugerkatalog skal kun indeholde data, der er relevant for at løse opgaver i forhold til sikkerheden i sundhed.dk og andre nationale systemer.

4.4 OCES-certifikater

Et væsentligt led i sikkerheden i adgangen til de nationale systemer er brugen af OCES-certifikatet, og der er derfor igangsat et arbejde med at afklare de udfordringer, det giver at anvende denne teknologi. I arbejdet med at løse problemerne omkring brug af OCES indgår det f. eks. hvordan amterne administrerer brugernes certifikater i samspil med certifikatudbyderen (TDC), og denne opgave er parallel med samspillet mellem amterne og det centrale brugerkatalog. Disse to processer skal derfor koordineres.

5. Konklusion

Sikkerhedsgruppen blev etableret for at

- vurdere behov og muligheder for fælles amtslige sikkerhedsløsninger i forbindelse med EPJ, herunder et centralt brugerstyringskatalog.
- vurdere, hvor snittet mellem centrale og decentrale sikkerhedsløsninger bør ligge – i første omgang med fokus på brugerstyring.

Opgaven er blevet løst ved at fokusere arbejdet på hhv.

1. Krav til lokale/decentrale sikkerhedsløsninger.
2. Fælles sikkerhedsløsninger på tværs af amter/H:S og centrale myndigheder.

Desuden indgår flere af sikkerhedsgruppens medlemmer i arbejdsgruppen vedrørende brugerkatalog i Sundhedsstyrelsens regi. Dette arbejde omfattes ikke i denne afrapportering.

Ved at fokusere på hhv. krav til lokale/decentrale sikkerhedsløsninger og fælles sikkerhedsløsninger er der blevet identificeret en række krav/områder, der er behov for at indtænke i de decentrale sikkerhedssystemer for at de kan fungere som elementer i en fælles, sammenhængende sikkerstruktur.

5.1 Behov for fælles amtslige sikkerhedsløsninger

Der er opstået et behov for fælles amtslige sikkerhedsløsninger som en konsekvens af visionerne om en sammenhængende sundhedssektor kombineret med den teknologiske udvikling. Visionerne om en sammenhængende sundhedssektor skaber behov for at patientjournalerne følger patienterne og at sundhedspersonalet på sikker vis kan få adgang til relevante patientoplysninger. Den teknologiske udvikling gør det muligt for amterne at indføre EPJ, hvilket skal ske inden udgangen af 2005 eller snarest derefter (jf. økonomiaftalen for 2005). Det kræver udvikling af sikkerheden så patientdatas tilgængelighed, kvalitet, fortrolighed og sporbarhed

fortrolighed og sporbarhed sikres. Alternativet til etableringen af sammenhængende sikkerhedsmodeller for sundhedsvæsenet er, at amterne får store administrative byrder til at vedligeholde sikkerhedsdata om personalet i mange forskellige systemer i og udenfor amtet. Det vil kræve en meget kompleks løsning som vil give risiko for brud på sikkerheden.

5.2 Muligheder for fælles amtslige sikkerhedsløsninger

Der er forskellige muligheder for at etablere fælles amtslige sikkerhedsløsninger. Der skal være løsninger for håndtering af hhv. patientdata og brugerdata.

Det er af stor betydning for både sikkerheden og systemernes effektivitet, at sikkerhed indgår i alle led i den samlede arkitektur og i alle faser lige fra vision over modellering og programmering til praktisk anvendelse. Der er mange eksempler på at hverken program eller sikkerhed fungerer tilfredsstillende hvis sikkerheden ikke er indtænkt i løsningen fra start.

Der kan opstilles modeller for fælles amtslige sikkerhedsløsninger med forskellige grader af distribution og centralisering. Den ene yderlighed er *distribuerede* løsninger, hvor patientdata forbliver i det system, hvor data fødes, og hvor en ekstern sundhedsaktør tilgår dette system direkte. Den tilsvarende sikkerhedsmodel for håndtering af brugere indebærer, at brugeren autentificeres og autoriseres af det databærende system, som kommunikerer direkte med brugersystemer i brugerens hjemamt.

Som den anden yderlighed findes *centrale* løsninger, hvor patientdata samles i et nationalt patientindeks, som bl.a. kan vises via sundhed.dk, og hvor brugerdata ligeledes samles i et nationalt brugerkatalog.

Blandt fordelene ved distribuerede løsninger er, at data kun ligger et sted. Blandt ulemperne er, at hvert amt skal oprette extranetløsninger og hånd-

håndtere sikkerhed i forhold til mange eksterne brugere. Endvidere er der ikke erfaring med de tekniske løsninger, der skal gøre sådanne distribuerede løsninger lette for brugerne og effektive at administrere, og de forventes at kræve en del udvikling.

Blandt fordelene ved centrale løsninger er at det medfører klarhed over det juridiske ansvar for data, at det enkelte amt kun skal overføre patientdata til en part, at det enkelte amt kun skal skabe systemforbindelse til en part (patientindekset), og at brugerdata kun skal overføres til en part (det nationale brugerkatalog). Desuden er der er teknologier, erfaringer og eksisterende løsninger baseret på denne model, som har et enklere design med færre krav til standarder.

5.3 Snittet mellem centrale og decentrale sikkerhedsløsninger

I sit arbejde har sikkerhedsgruppen skelnet mellem løsninger, der giver adgang til "historiske" patientdata, hvor data kun skal *læses*, og adgang til systemer med patienter i fælles behandling, hvor flere parter skal *skrive* data "på samme tid". Sikkerhedsgruppen finder at det på nuværende tidspunkt kun er muligt at drage konklusioner i forhold til læsning af data. Løsninger til skrivning af data kræver yderligere analyse (For illustration af løsningernes tidsmæssige sammenhæng, se bilag X som er vedlagt selvstændigt dokument og dermed ikke indgår i bilagssamlingen).

Sikkerhedsgruppen vurderer det mest hensigtsmæssigt at centrale og distribuerede løsninger kombineres. For at udnytte fordelene ved centrale løsninger bør der eksistere et centralt brugerkatalog, som indeholder data, der er relevant for at løse opgaver i forhold til sikkerheden i nationale systemer, f.eks. sundhed.dk. Det centrale brugerkatalog skal kombineres med mere detaljerede decentrale brugerkataloger, som bruges af de enkelte amter til håndtering af egne brugeres adgang til amtets egne systemer. Arbejdet med at definere indholdet af det centrale brugerkatalog på-

brugerkatalog pågår allerede i arbejdsgruppen vedr. brugerkatalog i Sundhedsstyrelsens regi.

Tilsvarende bør der etableres et centralt patientindeks som kan tilvejebringe de mest kritiske sundhedsoplysninger i en akut diagnosticerings- og behandlingssituation samt oplysninger om patientens forløb og kontakter til sundhedsvæsenet med henblik på at fremskaffe yderligere information. Der er således ikke tale om at alle patientdata skal findes i det nationale patientindeks, men derimod oplysninger der f.eks. svarer til indholdet i det nuværende landspatientregister suppleret med en epikrise samt en unik patientforløbsnøgle.

I næste kapitel opridses en række af de anbefalinger der er givet i rapporten.

6. Anbefalinger

En række anbefalinger fremgår af de forskellige kapitler i denne afrapportering. I dette kapitel gentages nogle af – men ikke alle – anbefalingerne med henvisning til hvor i afrapporteringen de findes.

ad 2.1 (s. 11ff) Samspil mellem amtslige systemer og nationale systemer

- Der skal i forbindelse med udarbejdelse af standarderne til G-EPJ udarbejdes standarder for sikkerhedsrelevante patientdata. Konkret bør sikkerhed indgå i arbejdet med at udarbejde den næste version af G-EPJ.
- Rollebaseret brugeradministration vurderes at være hensigtsmæssigt i forbindelse med rettighedstildeling til fælles nationale systemer, f.eks. sundhed.dk, og på tværs af sygehusejere. Rollebegrebet er imidlertid ikke entydigt. Det anbefales at der udarbejdelse et standardiseret rollebegreb, indeholdende flere dimen-

indeholdende flere dimensioner, herunder uddannelse (autorisation), arbejdsfunktion og organisatorisk tilhørsforhold.

- Brugeren af det nationale system skal angive at han/hun har patienten i behandling for at kunne tilgå patientens data. Der bør arbejdes på at minimere brugen af tro og lov erklæringer og på at etablere en fælles systemløsning.

ad 2.2 (s. 13f) Samspil mellem EPJ-systemer og produktions- og medico-tekniske systemer

- En arkitektur for systemerne i den danske sundhedssektor må på længere sigt også omfatte sikkerheden i samspillet mellem EPJ-systemerne og produktionssystemer (laboratorium, blodbank, røntgen mv) og medico-tekniske systemer. Sikkerhed bør derfor indgå i IT-arkitekturgruppens arbejde.

Ad Fejl! Ukendt argument for parameter. **(s.14ff)** Fejl! Ukendt argument for parameter.

- Sundhedsstyrelsens Elektroniske Indberetningssystem (SEI) falder ikke inden for rammerne af de øvrige fælles komponenter i den danske sundhedssektor. Det anbefales, at Amtsrådsforeningen og sundhed.dk arbejder på, at SEI bringes i sammenhæng med de øvrige systemer.

Ad Fejl! Ukendt argument for parameter. **(s. 17ff)** Fejl! Ukendt argument for parameter.

- Det anbefales, at der etableres en standard for samtykkemodulkomponent, evt. som en fælles løsning i tilknytning til patientindekset.
- Det anbefales at den sikkerhedsmæssige dimension inddrages i arbejdet med en ny sygehusafdelingsklassifikation.
- Det anbefales, at man for at forenkle brugeradministrationen gør den rollebaseret.

- Arbejdsgruppen anbefaler, at sygehusejerne anvender en generel brugeradministrationskomponent, der kan håndtere rettighedsstyringen for alle de applikationer, der anvendes.
- Det anbefales, at der laves en standard for funktionalitet og arbejdsgange for kontrol og opfølgning ved logning
- Der bør etableres en landsdækkende service til generering af erstatnings-CPR-numre, der sikrer, at samme nummer kun kan vedrøre én patient, og at en patient kun har ét erstatnings-CPR-nummer.
- Det anbefales at der laves en samlet oversigt over EPJ-relaterede standarder der anvendes i sundhedsvæsenet.
- Det anbefales, at der i regi af Amtsrådsforeningen fastlægges en "best practice" for arbejdsgange i relation til dokumentation af beslutningsgrundlaget ved brug af elektroniske beslutningsstøtte værktøjer.
- Det anbefales at der udarbejdes en fælles amtslig Service Level Agreement, der specificerer krav til oppetid, reaktionstider i forbindelse fejl på viste data osv.

Ad Fejl! Ukendt argument for parameter. **(s. 34ff)** Fejl! Ukendt argument for parameter.

- For *læsning af data* i eksterne systemer anbefales en *central* løsning, hvor patientdata samles i et nationalt patienindeks, som bl.a. kan vises via sundhed.dk, og hvor brugerdata ligeledes samles i et nationalt brugerkatalog.
- Løsninger til *skrivning* af data kræver yderligere analyse.

Ad Fejl! Ukendt argument for parameter. **(s. 37ff)** Fejl! Ukendt argument for parameter.

- Arbejdsgruppen anbefaler en løsning, hvor der etableres et centralt patientindeks med egen database, der indeholder de væsentlige informationer om en given patient.

ad 4.3 (s. 39ff) Brugerkatalog

- Der skal i alle amter etableres en sikker og effektiv brugeradministration, der gør det muligt fra 2006 at synkronisere brugerne fra amterne til det nationale brugerkatalog automatisk.

- Der skal i 2005 udarbejdes standarder for de data, der skal overføres fra amterne til det nationale brugerkatalog, samt regler for hvordan og hvornår, de skal overføres.
- Brugerkataloget skal i videst muligt omfang baseres på eksisterende løsninger.

ad 4.4 (s. 40ff) OCES-certifikater

- Arbejdet med planlægning af et centralt brugerkatalog og arbejdet med administration af OCES-certifikater skal koordineres.