UDKAST til Referencearkitektur for Informationssikkerhed

National Sundhed It

November 2012

Version 0.96

Indhold

1 Indledning

1.1 Baggrund

Siden midten af 1970'erne har man anvendt elektronisk registrering af oplysninger om patienter på sygehuse til styrings-, planlægnings- og kvalitetsudviklingsformål. Siden er mængden af informationer, der registreres elektronisk om den enkelte borger i sundhedsvæsenet steget markant.

For at beskytte borgerens personlige oplysninger indførte man i 1987 "lov om offentlige myndigheders registre" og "lov om private registre", som i 2000 blev erstattet af den nuværende Persondatalov. Persondataloven er en implementering af EU's persondatadirektiv i dansk lovgivning, og heri stilles der en række krav til, hvordan man skal håndtere personhenførbare informationer. Loven gælder i modsætning til den tidligere lov ikke kun elektroniske informationer, men også informationer på papir, billeder, video osv.

Udover persondatalovens regler findes der også i anden lovgivning krav, som påvirker den måde, man må og kan arbejde med elektroniske informationer. Det gælder f.eks. sundhedsloven, serviceloven, forvaltningsloven, lov om elektroniske signaturer og arkivloven.

Oprindeligt blev det meste information, der blev registreret elektronisk, anvendt lokalt, f.eks. inden for det enkelte sygehus, og det var også typisk, at den elektroniske registrering foregik i flere forskellige systemer, som ikke kunne udveksle oplysninger. Patientadministrative data blev registreret i et system, laboratorieresultater i et andet system osv.

Men efterhånden som de elektroniske registreringer mere eller mindre har erstattet den tidligere papirjournal som primært værktøj i patientbehandlingen, og der i stigende omfang etableres samarbejde mellem sygehuse, praktiserende læger og kommunernes hjemmepleje, er der stigende behov for at kunne dele aktuelle og relevante data om patienten for at kunne yde den mest optimale behandling.

Adgangen til informationer må derfor ikke være begrænset af system- eller sektorgrænser, og det skal være muligt at tilgå informationerne, uanset deres oprindelse og fysiske placering.

Denne udvikling er hensigtsmæssig i forhold til at anvende ressourcerne i sundhedsvæsenet mest effektivt, yde den bedste behandling og giv borgeren mulighed for at indgå aktivt i sin egen behandling. Men informationssikkerhedsmæssigt er det en stor udfordring, fordi de eksisterende sikkerhedsmodeller er indrettet på, at man beskytter data inden for den enkelte organisation og ofte i hvert sit system.

Situationen er karakteriseret ved, at der hos de forskellige parter ikke er samme tilgang til informationssikkerheden; der opereres ikke med fælles begreber og løsninger baseres kun i begrænset omfang på fælles standarder. Dette besværliggør eller forhindrer adgang til data og vanskeliggør overholdelse af lovgivningen, når det drejer sig om behandling af data på tværs af parter. Der er derfor behov for at fastlægge en fælles referenceramme for informationssikkerhed i sundhedsvæsnet. En fælles arkitektur og fælles standarder, som kan understøtte sikker databehandling på tværs af systemer vil være en del af en sådan fælles referenceramme.

I Aftale om sundheds-it fra den 12. juni 2010 fremgår det, at Indenrigs- og Sundhedsministeriet skal stille krav til en ensartet og effektiv udveksling af relevante patientoplysninger på tværs af

sundhedsvæsenets forskellige systemer. Som et led i at kunne efterkomme dette krav har NSI besluttet, at der skal udarbejdes en referencearkitektur for informationssikkerhed møntet på sundhedsvæsnet. Ansvaret for udarbejdelse af denne referencearkitektur er placeret hos NSI.

National Sundheds-it (NSI) udgav i efteråret 2011 en rapport [STD_RA], der lægger rammen for arbejdet med fastlæggelse af referencearkitektur og standarder for sundhedsvæsenet. Heri er der prioriteret en række indsatsområder, hvor der er behov for at få beskrevet generelle referencearkitekturer og udpeget standarder, der kan understøtte tilgang til information.

Et af de centrale indsatsområder beskrevet i denne rapport vedrører udarbejdelse af en referencearkitektur for informationssikkerhed. Denne referencearkitektur er en grundlæggende forudsætning for en række konkrete forretningsmæssige initiativer, der blandt andet følger af:

- "Aftale om Sundheds-It" fra 2010 mellem regeringen og Danske Regioner.
- Pejlemærker af tværgående karakter fra RSI, 2010.
- Målsætning om kommunal adgang til individdata på sundhedsområdet fra "Aftale om kommunernes økonomi for 2011".
- Overenskomster på sygesikringsområdet, herunder med praktiserende læger og speciallæger.

Et eksempel på et konkret initiativ er "Etablering af et Nationalt Patient Indeks – NPI"; dette initiativ stammer fra "Aftale om Sundheds-It" fra 2010 mellem Staten og Danske Regioner. Eftersom man med NPI samler mange følsomme informationer fra forskellige kilder, er det overordentlig vigtigt at sikre sig, at informationerne beskyttes på et passende niveau, og en referencearkitektur for informationssikkerhed vil således støtte[1] udviklingen af dette initiativ.

1.2 Resumé

It-anvendelsen i sundhedsvæsenet er ved at flytte sig fra den enkelte parts anvendelse af egne data til anvendelse af data opsamlet ved forskellige parter i væsenet.

Sikkerhedsmodellen for anvendelse af data på tværs af parter er ikke blot summen af parternes sikkerhedsmodeller. Forskelle i sikkerhedsmodeller gør det vanskeligt at skabe sammenhængende løsninger.

En referencearkitektur kan fungere som fælles pejlemærke, der medvirker til at sikkerhedsmodeller udvikler sig i samme retning.

I denne referencearkitektur opstiller en fælles vision, fælles værdier og fælles principper. Visionen tegner et billede, hvor bl.a.:

- sundhedspersoner med samme arbejdsfunktion og relation til patienten får adgang til de *samme data* (uafhængigt af behandlingssted)
- den viden borgeren har om eget behandlingsforløb og den personlige interesse borgeren har i at påvirke informationsstrømmen og sikre berettiget adgang til personlige oplysninger udnyttes
- sundhedsorganisationer og myndigheder gives mulighed for at bruge patienternes sundhedsoplysninger til udvikling af sundhedsvæsenet - uden mulighed for, at personer involveret i behandlingen af disse oplysninger kan få kendskab til patienters identitet

[1] Se [STD_RA] for en nærmere redegørelse.

Referencearkitekturen foreslår, at

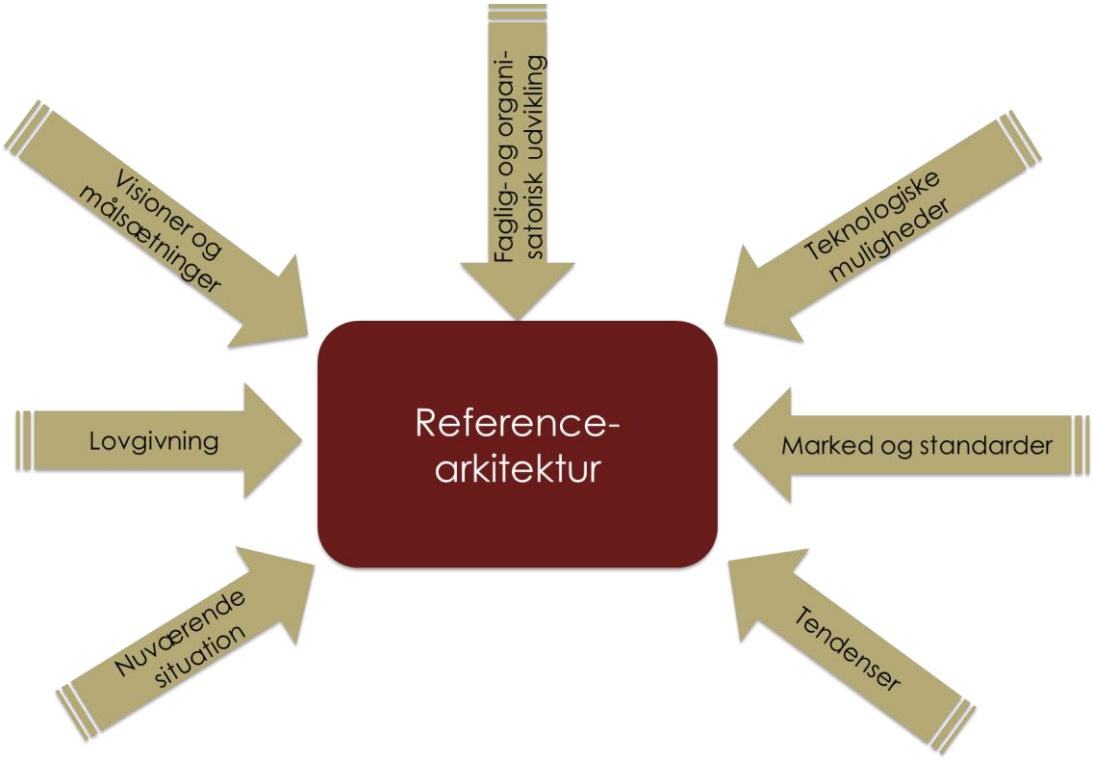
- der arbejdes efter en sikkerhedsmodel som både tillader at der benyttes løsninger som alle har tillid til (”trusted third party” model) og som tillader parterne at have gensidig tillid til hinanden (”federated trust” model)
- at tillid parterne imellem baseres på aftaler, som lever op til en række fastsatte krav / standarder
- at der styres ud fra standardiseret information om borgere, sundhedspersoner, organisatoriske enheder, ansættelsesforhold, arbejdsfunktioner, autenticitetsstyrke (sikkerhed for fastslået identitet af brugere og systemer), styrke for evidens af behandlingsrelation, samtykke, begrundelser for brug af værdispringsregel m.v.

Referencearkitekturen peger på at ensrette de sikkerhedsmodeller, der arbejdes med i dag – ikke at beskrive helt nye og alternative sikkerhedsmodeller. Nogle af principperne række dog længere. Dette skulle gerne åbne muligheden for på sigt at flytte sig over i nyere sikkerhedsmodeller efterhånden som disse modnes og der findes praktiske implementeringer af dem.

Det er i forbindelse med udarbejdelse af referencearkitekturen blevet klart, at der er behov for at arbejde videre med den begrebsmodel for informationssikkerhed, som blev udarbejdet af Sundhedsstyrelsen i 2006. Dette arbejde igangsættes i efteråret 2012.

1.3 Referencearkitekturens centrale indhold

Referencearkitekturen for informationssikkerhed har fokus på at sætte rammerne for ensartet håndtering af informationssikkerhed på et passende højt og dokumenteret sikkerhedsniveau i de kommende digitaliseringstiltag i sundhedsvæsnet. Referencearkitekturen vil tage udgangspunkt i gældende lovgivning, indfange tendenser samt udstille retningen for de kommende år. Referencearkitekturen beskriver sikkerhedsmodeller, ansvarsfordeling og er drevet af grundlæggende principper, der skal sikre at alle relevante aspekter af informationssikkerhed håndteres ”efter samme læst” og prioriteres ensartet hos alle parter.



Figur 1 - Referencearkitekturens væsentligste påvirkninger

Denne referencearkitektur udgør ikke grundlaget for styring af informationssikkerhed generelt (herunder håndtering af sikkerhed omkring papirbaserede arkiver). Virkefeltet for referencearkitekturen er begrænset til sundhedsvæsenets lagring og behandling af digitale informationer. Der er tale om en referencearkitektur, der skal være med til at skabe fælles rammer om de it-løsninger som udvikles og anvendes.

Selvom det er it-løsninger, der er i fokus, er det ikke muligt at afgrænse sig til en række tekniske krav til løsninger. It-løsningerne (med de tekniske sikringsforanstaltninger) vil altid baseres på nogle organisatoriske forudsætninger (eksempelvis krav til organisation og arbejdsgange). Disse vil medtages i det omfang det er relevant for sikkerheden omkring it-løsningerne, men referencearkitekturen gør det altså ikke ud for arbejdet med informationssikkerhed i øvrigt.

Omvendt, kan der være dele af referencearkitekturen (f.eks. af forretningsarkitekturen), der vil kunne benyttes i det mere generelle arbejde med informationssikkerhed (også inkluderende den ikke-digitale del), men referencearkitekturen hævder ikke her at være fuldt dækkende for hele området.

1.4 Referencearkitekturens centrale begreber

En arbejdsgruppe under Det Nationale Begrebsråd for Sundhedsvæsenet udgav i 2006 rapporten "Et begrebssystem for informationssikkerhed" [NBS 06]. Denne referencearkitektur tager udgangspunkt i de grundlæggende begreber defineret i denne rapport, men det er fundet nødvendigt at ajourføre begrebsdefinitioner og begrebsmodel, så det bl.a. afspejler den fælles forståelse, der er opnået gennem arbejde præsenteret for arkitekturråd og informationssikkerhedsråd[2] på

[2] Se eksempelvis [SDSD-Analyserapport].

sundhedsområdet 2008-2010 og arbejdet med vejledning i risikovurdering i regi af IT- og Telestyrelsen i 2008.

I forhold til det oprindelige begrebsarbejde fra 2006, hvor informationssikkerhed blev betragtet som bestående af 3 "dele": Fortrolighed, integritet og tilgængelighed, da fokuseres der nu på flere væsentlige aspekter ved informationssikkerhed:

Autenticitet	Egenskab, der beskriver, om noget er, hvad det giver sig ud for at være (om det er autentisk/ægte). Gennem autenticitetssikring/autentifikation sikres, at en ressource eller person er den påståede.
Tilgængelighed	Egenskab ved service der sikrer, at servicen er til rådighed for en bruger i henhold til fastlagte rammer
Integritet	Egenskab ved et informationsaktiv, der sikrer dettes nøjagtighed og fuldstændighed. Integritet sikrer fx kommunikation, således at en serviceudbyder og en serviceaftager er garanteret, at beskederne ikke ændres mellem afsender og modtager uden at én af parterne opdager det.
Uafviselighed	Egenskab ved information der gør det muligt at bevise, at en given bruger har udført en given handling på et givet tidspunkt
Fortrolighed	Egenskab ved informationssystem der medfører, at kun bestemte brugere har adgang til bestemte data eller bestemt information

I diskussioner om informationssikkerhed i sundhedsvæsenet er det ofte aspektet fortrolighed, der fokuseres på, men det er vigtigt, at man foretager en konkret afvejning af behovet for at tilgodese alle relevante aspekter af informationssikkerhed. Det er ikke hensigtsmæssigt at etablere et højt niveau af fortrolighed, hvis dette sker på bekostning af den nødvendige tilgængelighed til de informationer, de skal bruge for at kunne udføre deres arbejdsopgaver.

To centrale begreber fra begrebssystemet vedr. informationssikkerhed er *"sikkerhedsrisiko"* og *"sikringsforanstaltning"*.

En sikkerhedsrisiko er en hændelse, der vurderes at kunne indtræde med en vis sandsynlighed og som vil have en uønsket påvirkning af forretningens it-aktiver (med negativ forretningsmæssig konsekvens). Jo større sandsynligheden er for at hændelsen indtræder og jo større konsekvensen er for forretningen, jo større vurderes sikkerhedsrisikoen at være.

Sikringsforanstaltninger har til formål at mindske sikkerhedsrisici – enten ved at nedbringe sandsynligheden for at hændelserne indtræder - eller ved at reducere konsekvenserne ved at hændelserne indtræder (eller ved begge dele).

De dele af begrebssystemet, der har været relevante for denne referencearkitektur beskrives nærmere i afsnit 3.1 (med foretagne justeringer). Der er her tale om ret generiske begreber og ikke begreber, der er specifikke for informationssikkerhed indenfor sundhedsdomænet.

Der er imidlertid en del begreber, der knytter sig til Sundhedslovens bestemmelser om adgang til sundhedsdata (f.eks. negativt samtykke, behandlingsrelation, værdispring, mm.). Der er derfor behov for, at modellen udbygges og justeres, således at den kan rumme disse sundhedsspecifikke begreber. Dette er en proces som kræver involvering af flere interessenter over et stykke tid. Dette har ikke været muligt at indpasse tidsmæssigt i arbejdet med denne referencearkitektur, så i stedet er der i bilag B udarbejdet forslag til definitioner af de væsentligste begreber. Disse må så

indarbejdes i begrebssystemet efterfølgende og medtages i senere revision af denne referencearkitektur.

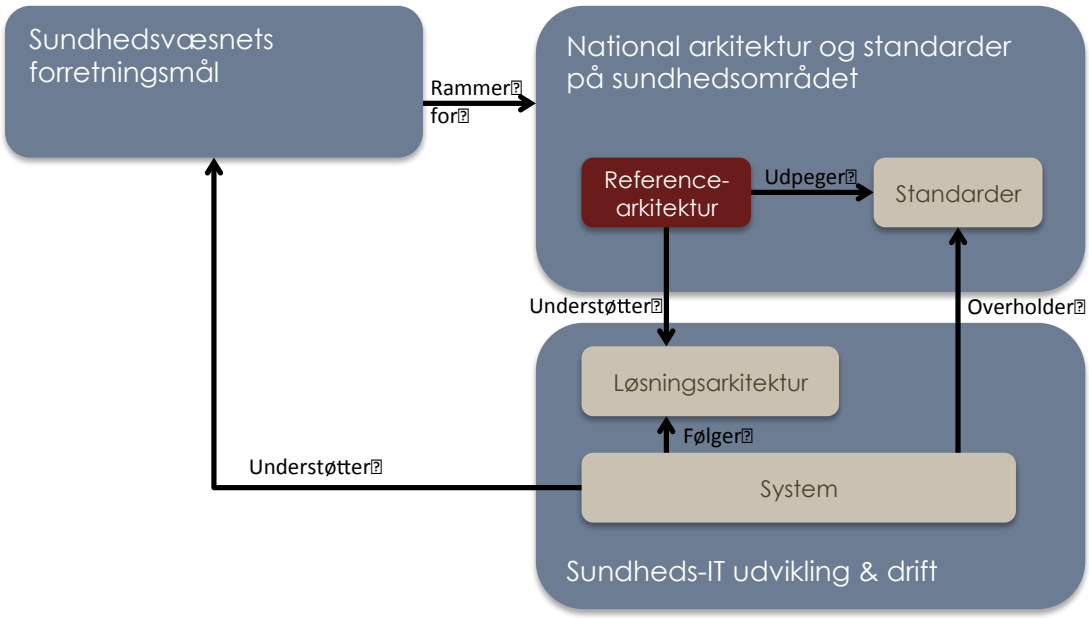
1.5 Referencearkitekturens formål

Referencearkitekturen skal skabe en arkitekturmæssig ramme for, hvordan man skal indrette løsninger så de kan "tale sammen" og udveksle personfølsom information på en sikker og ensartet måde. Referencearkitekturen skal fungere som fælles pejlemærke for udviklingen.

Referencearkitekturen er overordnet set drevet af sundhedsvæsnets forretningsmål. Den skal medvirke til at danne rammerne for *konkrete* løsningsarkitekturer og systemer, der støtter op om forretningsmålene.

Referencearkitekturen skal også bidrage til standardisering af området. Herunder, at der peges på områder, hvor der bør fastlægges relevante sikkerhedsstandarder, som kan bidrage til en ensartet sikkerhedshåndtering af høj kvalitet. Dette kan samtidig være grundlag for en effektivisering af processer, f.eks. minimering af genindtastning, gentagne log-ins mm.

Dette tvedelte formål illustreres i [STD_RA], hvorfra følgende illustration er relevant:



Figur 2: Referencearkitekturens kontekst

Generelt set fastlægger referencearkitekturen begreber, processer og informationsstrukturer for et overordnet område. Nærværende referencearkitektur er af mere grundlæggende karakter og vil typisk indgå som et element i mere specifikke referencearkitekturer.

Formålet med referencearkitektur for informationssikkerhed er derudover:

- At opsamle, fastlægge og konkretiser eksisterende viden, beslutninger, begreber, modeller og processer omkring informationssikkerhed i kontekst af sundhedsvæsnet og dermed biddrage til generel og fælles forståelse af informationssikkerhed.
- At fastlægge principper, aktører, roller og ansvar for området.

- At skabe rammerne for, at sundhedsvæsnets parter kan udarbejde konkrete løsningsarkitekturer (og dermed systemer), der indeholder en ensartet håndtering af informationssikkerhed på tværs af systemer og organisationer.
- At fremme en sammenhængende sikkerhedsarkitektur i sundhedsvæsnets løsninger og derved skabe grundlaget for f.eks. minimering af genindtastning, gentagne log-ins mm.
- At give sundhedsvæsnets parter en ramme, der bidrager til at bygge løsninger, der både lever op til gældende lovgivningskrav, dels er forberedt på fremtiden.

1.6 Hvad er en referencearkitektur

IT- og Telestyrelsens (nu Digitaliseringsstyrelsen) beskriver en referencearkitektur således [OIOEA_BP]:

- *"En referencearkitektur er en velovervejet måde at bygge it-løsninger inden for et specifikt område.*
- *Referencearkitekturen beskriver de overordnede logiske strukturer og begrebsapparatet for det specifikke område, således at der er et godt grundlag at arbejde ud fra, når der skal skabes sammenhængende it-løsninger.*
- *En referencearkitektur beskriver, udover de logiske strukturer og begrebsapparatet, også de grundlæggende logiske forretningstjenester og -begreber inden for referencearkitekturens fokus.*
- *Ofte beskrives på logisk plan også de generiske forretningstjenester og -begreber, som benyttes i grænsefladen omkring referencearkitekturen.*
- *Referencearkitekturer kan beskrives på flere abstraktionsniveauer. På et meget højt abstraktionsniveau vises alene de grundlæggende strukturer og den tilgrænsende omverden. I mere detaljerede niveauer ser man ofte beskrevet logiske tjenester, kernebegreber og interaktion mellem disse.*
- *En referencearkitektur opstiller fælles pejlemærker og principper for udviklingen af området. Referencearkitekturen giver både myndigheder (bestillere) og leverandører (udbydere) fælles sigtepunkter for udviklingen af området.*"

En referencearkitektur dækker således et afgrænset område, hvor man på det øverste niveau fastlægger forretningsmæssige mål og beskriver ønskede egenskaber for løsninger på området. Derefter fastlægges de overordnede principper for løsninger, løsningselementer og processer beskrives, og på baggrund af dette identificeres de områder, der kan blive til genstand for standardisering. En referencearkitektur kan beskrives mere eller mindre i dybden alt efter behov. En referencearkitektur er i sin natur generel og beskriver en klasse af løsninger, der alle udviser det samme mønster, som referencearkitekturen er genstand for.

1.7 Metoderamme

I overensstemmelse med anbefalingerne i [STD_RA] benyttes "OIO Referencearkitektur – best practice anbefalinger" [OIOEA_BP] som metodisk begrebsramme til beskrivelse af referencearkitekturen.

1.8 Målgruppe

Målgruppen er digitaliseringschefer, it-chefer, afdelings- og kontorchefer og andre med rollen som systemejer inden for offentlige myndigheder i stat, regioner og kommuner, der skal gennemføre anskaffelse af sundheds-it løsninger, hvori der indgår krav til informationssikkerhed.

Endvidere skal referencearkitekturen understøtte it-leverandører når de skal designe løsninger til sundhedsvæsnet. Dette skal blandt andet ske i form af fastlæggelse af fælles sikkerhedsmodeller,

sikkerhedsinformationer og -services. Målgruppen er således også leverandører af it-løsninger, særligt deres arkitekter og udviklere.

Herudover er målgruppen også relevante organisationer, der lovgiver omkring informationssikkerhed samt fører tilsyn med, at reglerne på området overholdes.

Endelig er målgruppen personer og organisationer, der udarbejder øvrige referencearkitekturer.

1.9 Læsevejledning

De to første kapitler (”Indledning” og ”Strategiarkitektur”) udgør fundamentet for referencearkitekturen for informationssikkerhed og er relevant for alle målgrupper.

De følgende kapitler går i dybden med henholdsvis forretningsarkitektur (kapitel 3) og teknisk arkitektur (kapitel 4) og henvender sig primært til projektledere, arkitekter og udviklere.

1.10 Tilblivelsesproces

Siden 2003-2004 er der struktureret blevet arbejdet med informationssikkerhed på sundhedsområdet på nationalt plan[3]. Det har været et bærende princip i arbejdet med nærværende referencearkitektur, at der skal bygges videre på det brede fundament af viden, erfaringer og resultater, der allerede findes på området både inden for sundhedsvæsnet, fællesoffentligt og internationalt. Arbejdet har derfor taget afsæt i resultaterne af en række initiativer og projekter indeholdende elementer af informationssikkerhed, og kan i mange sammenhænge betragtes som en konsolidering, bearbejdning og sammenstilling af eksisterende materiale. Blandt de væsentligste input fra sundhedssektoren har været:

- **Sikkerhedsmodeller bag nationale infrastrukturelementer som Sundhed.dk og det internetbaserede sundhedsdatanet (2003-2004)**
  Herunder brugen af digitale certifikater til autentifikation og kryptering af forbindelser (baseret på registrering i MedCom ”aftalesystem”).
- **Beslutninger fra møde i 2004 i amtsrådsforeningen.**
  I 2004 blev der i amtsrådsforeningen besluttet:
  - at amterne fik ansvar for at udvikle løsninger, der gjorde anvendelsen af digitale signaturer på sygehusene muligt
  - at sundhedsstyrelsen fik ansvar for etablering af brugerkatalog.
- **Pilotprojekter med digital signatur i sundhedsvæsenet (2004-2005)**
  I regi af Amtsrådsforeningen blev der 2004-2005 gennemført og evalueret 6 pilotprojekter, der skulle afklare vilkår for anvendelse af digital signatur i sundhedsvæsenet. Erfaringerne herfra skulle være med til at sikre, at der blev truffet de rette valg i forbindelse med implementeringen af digital signatur i væsenet.
- **SOSI projektet (2005-2008).**
  I regi af Amtsrådsforeningen (senere Danske Regioner og slutteligt hos SDSD) blev et projekt vedr. Service Orienteret System Integration (SOSI) gennemført. Projektet etablerede en model for sikker identifikation af sundhedspersoner ved hjælp af Digital Signatur, og opstillede en sikkerhedsmodel for sikker Web Service kommunikation baseret på dette. Projektet etablerede digitale infrastrukturtjenester, der understøtter sikker identifikation baseret på OCES.

[3] Der er naturligvis også gjort sig sikkerhedsmæssige overvejelser omkring den VANS-baserede infrastruktur, der blev etableret af MedCom i midten af 1990’erne. Sikkerheden i denne infrastruktur er imidlertidig udenfor denne referencearkitekturs rækkevidde.

- **Sammenhængende brugeradministration (SBRS projektet, 2009-2010)**
  I regi af SDSD blev der gennemført et projekt, der analyserede mulighederne for at etablere en national ramme for rettighedstildeling baseret på nationale "roller" eller arbejdsfunktioner i relation til nationale og tværgående it-services på sundhedsområdet. Projektet resulterede i et forslag til sikkerhedsmodeller og forslag til fremtidigt arbejde på området.
- **Rådgivende organers behandlinger (2009)**
  SDSD nedsatte i 2009 tre rådgivende organer (Råd for indholdsmæssig standardisering, Arkitekturrådet og Informationssikkerhedsrådet). Rådene havde ansvar for at indstille nationale principper, standarder og implementeringsplaner for standarder til godkendelse i Domænebestyrelsen. Rådene beskæftigede sig ikke kun med egentlige standarder, men arbejdede også med at fastlægge mere overordnede principper, mål og retningslinjer for den nationale it-infrastruktur. Rapporter og andre resultater fra rådene er indarbejdet i nærværende referencearkitektur.
- **Domænebestyrelsens behandling af informationssikkerhed (2009-2010)**
  Domænebestyrelsen for sundhedsområdet har i flere omgange behandlet emner vedrørende informationssikkerhed blandt andet baseret på ovennævnte rådgivende organers indstillinger. Bestyrelsens beslutninger er indarbejdet i nærværende referencearkitektur.
- **Sign-On projektet (2009-2010).**
  I regi af SDSD blev der gennemført et projekt, der dels havde til hensigt at analysere potentialet i forbedring af "log-in" situationen i sundhedssektoren, særligt i regionerne. Potentialet viste sig at være relativt stort og projektet arbejdede derfor videre med udarbejdelse af standarder og it-komponenter, der kunne medvirke til mere effektive og hensigtsmæssige "log-in" mekanismer på sundhedsområdet.
- **NSPi projektet (2010-2011).**
  I regi af NSI blev der etableret et større projekt, der havde til hensigt at etablere den næste generation af national infrastruktur (NSP) herunder etablere services der understøttede området omkring kontrol af behandlingsrelation og opfølgning. Projektets leverancer vil blive tilgængelige for øvrige parter i sundhedsvæsenet i 2012.
- **NPI projektet (2011-2012)**
  I regi af NSI er der etableret et projekt, der har til formål at etablere et indeks (**N**ationalt **P**atient**I**ndeks), der muliggør søgning og fremfinding af patientoplysninger på tværs af organisationer og datakilder. NPI baserer sig på IHE XDS standarden. I tilknytning til NPI-projektet udvikles der services til håndtering af samtykke fra borgeren og til konsolideret overførsel af loginformationer til MinLog på sundhed.dk

I forbindelse med udarbejdelse af referencearkitekturen er der afholdt to workshops med interessenter fra sundhedsvæsenet og leverandører. Efter forelæggelsen i det rådgivende udvalg vil referencearkitekturen blive udsendt til offentlig høring, inden den forelægges den nationale bestyrelse for sundheds-it.

Som opfølgning på referencearkitekturen skal der igangsættes en række projekter med henblik på at fastlægge konkrete standarder i henhold til referencearkitekturen.

2 Strategiarkitektur

2.1 Nuværende situation (as-is)

Størstedelen af de data der behandles i dag er opsamlet lokalt og anvendes lokalt. Adgangen til data er styret af lokale (ofte systemspecifikke) sikkerhedsløsninger, der bygger på lokale eller systemspecifikke sikkerhedsmodeller.

De enkelte parter på sundhedsområdet har inden for deres eget område forsøgt at harmonisere sikkerhedsløsninger, f.eks. ved at stille ensartede krav i forbindelse med udbud og indkøb af it-løsninger.

Men på tværs mellem sundhedsvæsenets parter er det meget begrænset, hvad der er sket af tiltag for at etablere fælles løsninger. Lovgivning, aftaler mellem parterne om at følge fælles standarder (som eksempelvis DS 484) og fælles vejledninger har skabt en vis ensretning, men denne er sket på et så overordnet niveau, at man reelt ikke kan tale om et fælles sikkerhedsniveau og ensartet sikkerhedshåndtering sundhedsvæsenets parter imellem[4].

Udveksling af patientinformation mellem sundhedsvæsenets parter sker hovedsageligt ved at der sendes beskeder fra et system til et andet (på et tidspunkt bestemt af afsendersystemet). Det er afsendersystemet, der har ansvar for at sikre, at informationerne må videregives. Modtagersystemet lagrer herefter de indkomne informationer lokalt og adgangen til disse informationer styres af den af modtagersystemet anvendte (lokale) sikkerhedsløsning.

Denne form for udveksling af data har nogle sikkerhedsmæssige styrker og svagheder.

Tilgængeligheden af data er høj for dem der skal anvende data, da data lagres lokalt i modtagersystemet. Omvendt kan det være svært at sikre aktualitet, korrekthed og integritet af data, når data distribueres til flere systemer, eftersom det er afsendersystemet, der skal holde styr på, hvilke systemer, der har modtaget hvilke data og sende rettelser til disse, og modtagersystemet skal kunne modtage og håndtere rettelser.

Patientens ret til at frabede sig indhentning af oplysninger (ofte kaldt ”negativt samtykke”) udgør en speciel udfordring for systemer, der er integreret på denne måde. Såfremt patienten frabeder sig sundhedspersoners indhentning af oplysninger, som er registreret i forbindelse med en given kontakt på et sygehus, vil disse oplysninger være registreret i det system, der anvendes på det pågældende sygehus. Men hvis information allerede er videregivet til andre systemer, f.eks. til fælles databanker som eJournal, patologidatabank e.l., inden patienten frabeder sig dette, er det svært at sikre, at man ikke kan tilgå informationerne i andre systemer. Det er umuligt for patienten at vide, i hvilke systemer, der findes oplysninger om deres kontakter til sundhedsvæsenet og derfor er det på nuværende tidspunkt næsten umuligt at leve op til lovens krav.

Denne form for kommunikation er hensigtsmæssig, når afsenderen ved, hvilke informationer, modtageren skal bruge, f.eks. i et udskrivningsbrev til patientens egen læge eller ved overførsel af en patient fra et sygehus til et andet i forbindelse med et behandlingsforløb. Men i situationer, hvor

[4] Eksempelvis kan kontrol af, at systembrugeren har en patient er i aktuel behandling (behandlingsrelationscheck) og kontrol af, om patienten har frabedt sig at den pågældende bruger indhenter de aktuelle data (negativt samtykke), være implementeret på meget forskellig måde.

der f.eks. i forbindelse med en akut indlæggelse er brug for at se oplysninger om tidligere behandling, medicinering e.l., er det mere hensigtsmæssigt, at det er den person, der står i den konkrete behandlingssituation, der via sit eget it-system indhenter den relevante information fra det sted, hvor den er lagret.

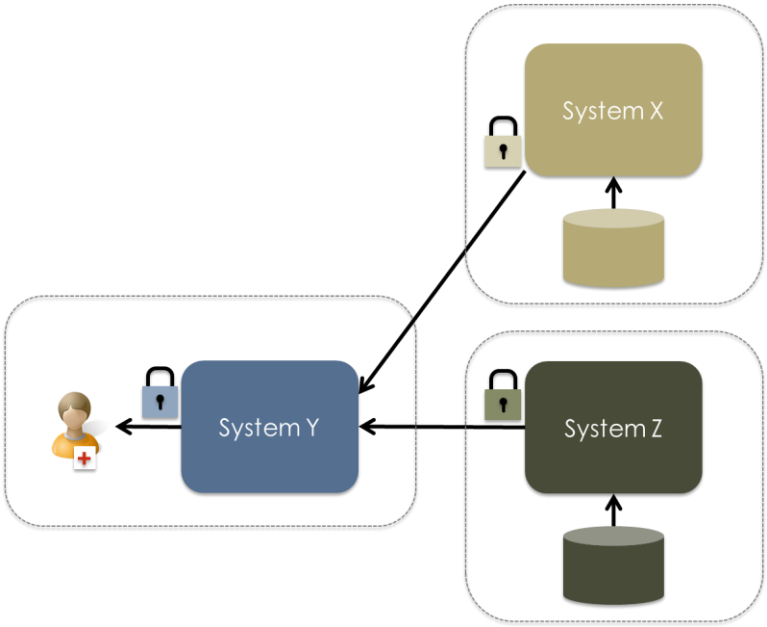
Denne form for systemintegration gør det lettere at sikre informationers aktualitet, korrekthed og integritet, men stiller store krav til infrastrukturen, for at sikre den nødvendige tilgængelighed til oplysninger, der kan være lagret mange forskellige steder.

Risikobilledet ændres også ved etablering af sådanne systemintegrationer, idet det enkelte system nu ikke bare giver adgang til egne (lokale) data, men principielt kan være indgang til indhentning af alle data registreret for den konkrete patient, uanset hvor i sundhedsvæsenet, de er lagret. Det er derfor nødvendigt at vurdere, om de eksisterende sikringsforanstaltninger er tilstrækkelige.

Ansvars- og tillidsforhold ændres også. Hvor det før har været den sikkerhedsansvarlige i egen organisation, der har været ansvarlig for adgangskontrollen til data (hvad enten disse er registreret lokalt eller modtaget fra andre systemer), så ligger dataansvaret og dermed ansvaret for den nødvendige adgangskontrol nu ved den part, der stiller sine data til rådighed for anvendersystemet, dvs. uden for egen organisation.

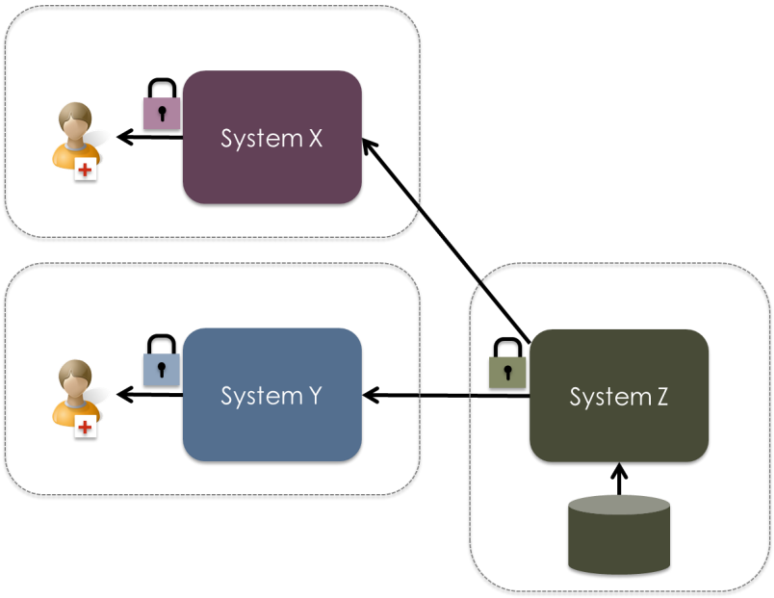
Den dataansvarlige kan enten selv implementere tekniske sikringsforanstaltninger, som begrænser adgangen for anvendersystemer, eller stille krav til anvenderorganisationer og -systemer om implementering af de nødvendige tekniske og organisatoriske sikringsforanstaltninger, men uanset om den dataansvarlige vælger den ene eller anden løsning, risikerer man, at de anvende sikringsforanstaltninger ikke passer sammen med den sikkerhedsmodel, der benyttes i anvendersystemet.

Endnu mere kompliceret bliver det, hvis anvendersystemet tilgår data fra flere parter, der opererer med hver deres sikkerhedsmodel, der stiller forskelligartede - og ikke nødvendigvis forenelige - krav til anvendersystemets håndtering af sikkerhed. Situationen illustreres af nedenstående figur (hvor forskellige sikkerhedsmodeller er illustreret af hængelåse i forskellige farver):



Figur 3 – Anvendersystem tilgår systemer med forskellige sikkerhedsmodeller

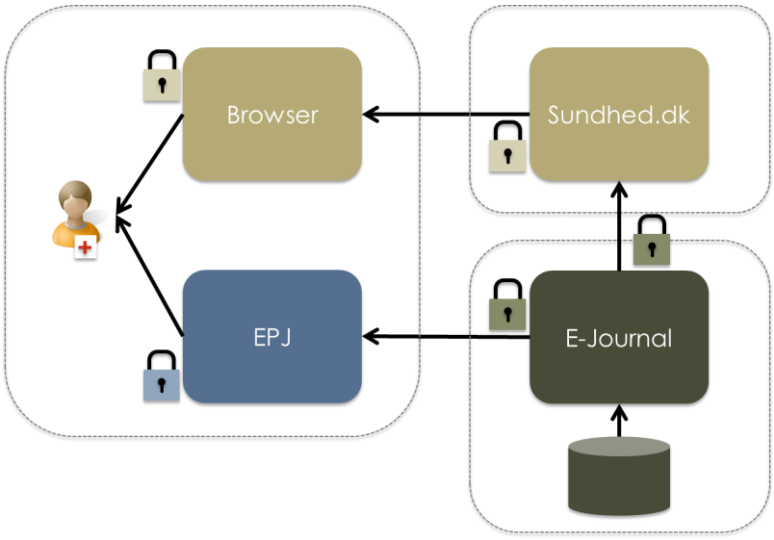
Omvendt betyder forskellige sikkerhedsmodeller hos anvendersystemerne, at sikkerheden bliver håndteret uensartet i forhold til sundhedsvæsenets parter, så informationer, der udstilles fælles nationalt, ikke nødvendigvis er tilgængelig for alle parter, afhængig af sikkerhedsmodellen i deres it-system. Situationen er illustreret af nedenstående figur:



Figur 4 – Forskellige parter har ikke adgang til samme data

I nogle tilfælde kan det endda være, at en person ved anvendelse af forskellige systemer hos den samme part i sundhedsvæsenet har forskellige adgangsrettigheder. Det kan eksempelvis være

tilfældet, at man ikke kan få adgang til data i eget EPJ-system, da dette udfører et check for behandlingsrelation baseret på oplysninger om indlæggelse eller åbne ambulante forløb i EPJ-systemet, men at det er muligt at få adgang til de pågældende data via sundhed.dk, der måske baserer sikkerhedsmæssige check på nationale kilder[5]. Situationen er illustreret af nedenstående figur:



Figur 5 – Forskellige systemer giver adgang til noget forskelligt

Denne problemstilling håndteres i eJournal[6] vha. en såkaldt "knapløsning", hvor det er EPJ-systemet, der opstarter den applikation på Sundhed.dk, der viser E-journal data for den pågældende patient, hvorved det er det lokale system, der sikrer, at der er en behandlingsrelation. På den måde er det muligt at skabe overensstemmelse mellem, hvilke data, der kan ses i det pågældende EPJ-system og hvilke, der kan ses via Sundhed.dk.

Men det skaber ikke den nødvendige overensstemmelse mellem andre systemer og Sundhed.dk.

De forskellige lokale systemer kan have forskellig måde at håndtere en behandlingsrelation. Skal patienten have en kontakt til den afdeling, hvor brugeren, der forespørger, er tilknyttet? - eller er det nok, at det er en patient på samme sygehus? Der er kun et eksempel på, at der i dag ikke findes en ensartet måde at foretage dette og andre sikkerhedsmæssige tjek.

Det betyder derfor, at så længe adgangen til data er baseret på den forskelligartede sikkerhedshåndtering i anvendersystemerne, er det svært at tale om et ensartet sikkerhedsniveau.

Hvis adgangskontrol eksempelvis alene baseres på lokale sikringsforanstaltninger, vil sikkerheden ikke være højere end den til enhver tid svageste sikkerhedshåndtering blandt anvendersystemerne. Brydes sikkerheden i det svageste system, kan dette bruges til at skaffe sig adgang til nationale data om personer.

[5] Der er her tale om en tænkt problemstilling, da E-Journal i dag ikke stiller data direkte til rådighed for EPJ-systemerne.

Opsummerende kan man altså sige, at den nuværende situation er kendetegnet ved følgende:

- Der er ikke et fælles nationalt, dokumenteret sikkerhedsniveau
- Sundhedspersoner ved forskellige parter har ikke nødvendigvis samme adgang til data, selvom de løser samme opgave
- Patienten kan ikke være sikker på, at alle relevante informationer registreret om vedkommende er tilgængelige, hvor de skal bruges
- Patienten har ikke samme mulighed for at frabede sig sundhedspersoners indhentning af oplysninger ved forskellige parter
- Det er svært og ressourcekrævende at skabe interoperabilitet mellem systemer, der bygger på forskellige sikkerhedsmodeller

2.2 Tendenser

2.2.1 Overordnede socio-økonomiske tendenser

En række overordnede tendenser sætter rammerne for it-understøttelsen i sundhedsvæsenet og dermed også for de sikkerhedsmekanismer, der skal tages i anvendelse for at sikre, at de relevante personer kan få adgang til de nødvendige oplysninger i forbindelse med undersøgelse, behandling eller pleje af en patient.

En af de væsentligste socioøkonomiske tendenser er den demografiske udvikling, som betyder, at såvel antallet som andelen af ældre i befolkningen stiger. Det betyder dels, at det vil blive vanskeligere at skaffe personale til sundhedssektoren med deraf følgende personalemangel og opgaveglidning fra nogle personalegrupper til andre.

For det andet medfører den stigende gruppe af ældre et øget behov for ydelser fra sundhedsvæsenet. Sammenholdt med udviklingen inden for gruppen af livsstilssygdomme betyder det, at der bliver flere kronisk syge, som skaber behov for nye behandlingstilbud og øget samarbejde med borgeren og på tværs i sundhedsvæsenet.

Sundhedsvæsenet er kendetegnet ved, at teknologiske og medicinske landvindinger hele tiden åbner nye muligheder for behandling og ændrer de vilkår, under hvilke behandlingen foregår. I nogle tilfælde betyder det øget specialisering, i andre tilfælde mulighed for at udbrede behandlingen, såvel geografisk som i forhold til, hvilke personalegrupper, der kan varetage behandlingen. Det øger behovet for samarbejde, planlægning og koordinering på tværs af sektorer for at sikre sammenhæng i behandlingen.

Stigende velfærd, uddannelsesniveau og øget anvendelse af informationsteknologi betyder, at borgerne generelt har større viden om og derfor stille større krav til sundhedsvæsenet. Borgerne er blevet mere mobile og ønsker at have indflydelse på, hvor og hvordan behandling skal finde sted. Den øgede mobilitet betyder, at der er behov for bedre koordinering ikke kun nationalt, men også internationalt.

Den teknologiske udvikling har medført, at adgang til informationer er blevet mere uafhængig af tid og sted. Anvendelse af internetbaserede tjenester og mobile enheder, betyder, at borgere og sundhedsfaglige kan søge informationer eller kommunikere (synkront eller asynkront), når det er belejligt.

Ligeledes vil den fortsatte udbygning af infrastruktur (lokalt, nationalt og globalt) gøre det muligt at kommunikere data effektivt over stadig større afstande, og dermed gøre brugen mere uafhængig af, hvor data fysisk opbevares.

2.2.2 Sikkerhedsmæssige tendenser

Den overordnede socioøkonomiske, medicinske og teknologiske udvikling medfører, at de anvendte sikkerhedsmodeller i sundhedsvæsenet udfordres og der er behov for at etablere en fælles ramme for informationssikkerhed, som kan tage højde for, at kommunikation og dataanvendelse ikke længere foregår indenfor den enkelte organisation, men i stigende grad på tværs af sektorer, regioner og på tværs af landegrænser.

Rent lovgivningsmæssigt giver det sig udslag i, at man i højere grad ønsker at beskytte borgerne, både ved at give dem større rettigheder i forhold til deres egne informationer og ved at stille større krav til de dataansvarlige, der skal sikre, at informationerne bliver beskyttet mod misbrug. Dette kommer bl.a. til udtryk i det forslag til persondataforordning, som forventes at afløse det eksisterende persondatadirektiv i EU.[7]

Øget borgerinddragelse i egen behandling vil på den ene side øge borgerens fokus på, at deres data behandles med den fornødne fortrolighed og at de selv får indflydelse på, hvem der får adgang til deres oplysninger.

På den anden side giver borgernes anvendelse af internettjenester, herunder sociale tjenester, mulighed for, at følsom information spredes på en helt ny måde. Der vil derfor være behov for at se på sikkerhedsmodeller, der gør det muligt at kommunikere og dele sundhedsoplysninger med sundhedspersoner og andre, f.eks. i netværksgrupper, uden at oplysningerne er personhenførbare.

Øget specialisering, samarbejde på tværs af sundhedssektoren, f.eks. "shared care" og større mobilitet for borgere og sundhedspersonale stiller krav om, at den sundhedsfaglige kan få adgang til alle relevante informationer, når der er brug for dem. Tilgængelighed til informationer skal være uafhængig af geografisk og organisatorisk placering, men afhænge af, hvad det er for en opgave, den sundhedsfaglige skal løse.

Der vil derfor være en bredere vifte af personer, både geografisk og på faggrupper, der vil få adgang til data, men kravet om tilgængelighed til data er ikke i modstrid med kravet om beskyttelse af borgerens privatliv, eftersom adgangen til informationerne er gældende for de personer og for det tidsrum, hvor det er nødvendigt for at kunne udføre undersøgelser, behandling, pleje af patienten eller sikre den nødvendige opfølgning kvalitetsmæssigt og administrativt. Krav til sikkerhed skal implementeres på en sådan måde, at de understøtter og ikke modvirker en hensigtsmæssig arbejdstilrettelæggelse.

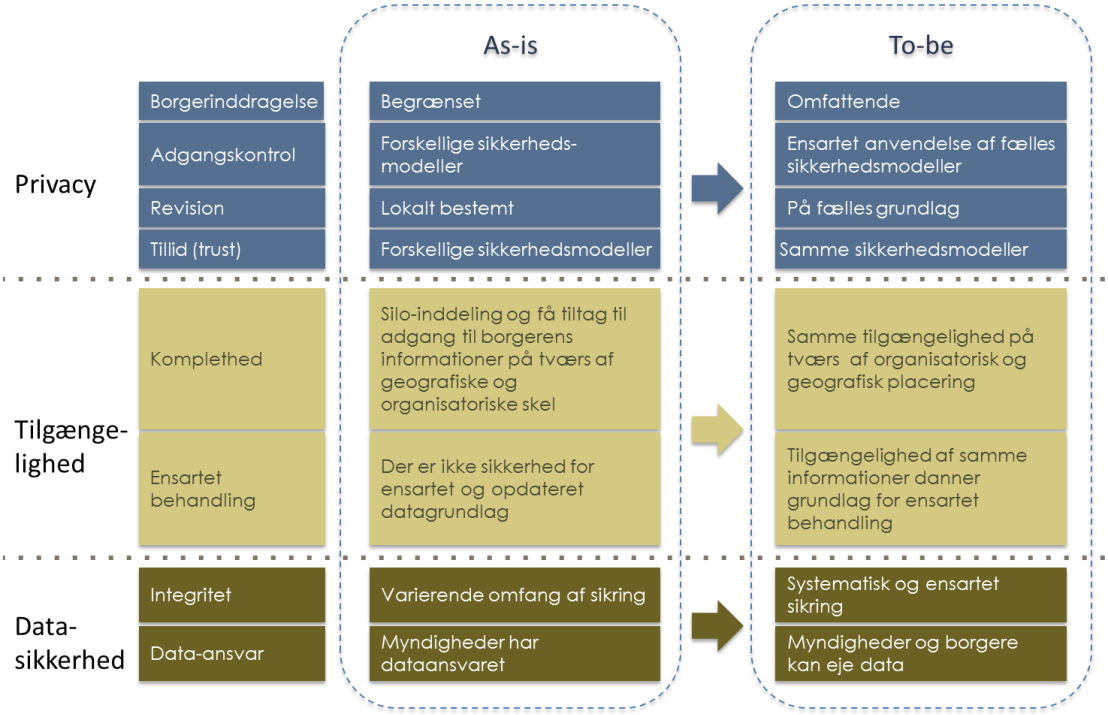
Tilgængelighed til relevante data uafhængigt af tid og sted stiller store krav til infrastrukturen, både for at sikre, at data kan tilgås, når det er nødvendigt, men også for at sikre, at data er korrekte og opdaterede. Da det erfaringsmæssigt er i transport- og transformationsprocesserne at der sker fejl, vil der i den fremtidige situation være et stort behov for gennemgående og ensartet integritetssikring i forbindelse med disse processer.

[7] Forordningen vil være gældende i alle EU-lande og skal ikke som direktivet indføjes i det enkelte lands lovgivning. Dette indebærer, at der vil blive etableret ensartede regler inden for EU's område.

Man kan derfor forestille sig, at den nuværende "silo-opdeling" af informationer bliver opblødt og i en vis grad suppleret med fælles datalagre inden for forskellige domæner (statsligt, fællesregionalt eller fælleskommunalt). Den tværgående informationsudveksling vil stille krav om, at der sker en formalisering og standardisering af snitfladerne imellem aktørerne i sundhedsvæsnet, og der vil være øget fokus på håndtering af dataansvar og de medfølgende forpligtelser.

Den teknologiske udvikling vil ligeledes udfordre de eksisterende sikkerhedsmodeller og stille krav om nye former for sikkerhedstiltag. Den øgede mobilitet betyder, at man skal kunne understøtte forskellige teknologiske platforme på en ensartet måde. Dette sammenholdt med, at den teknologiske udvikling foregår hurtigere – i mindre og flere trin, betyder, at det skal være muligt at etablere forskellige løsninger, uden at dette giver anledning til, at der opstår forskellige sikkerhedsniveauer.

Sammenfattende kan man beskrive de krav til den fremtidige sikkerhedsarkitektur, som følger af de sikkerhedsmæssige tendenser, som vist i nedenstående figur.



Figur 6 Nuværende og fremtidig sikkerhedsarkitektur

2.3 Vision

Referencearkitekturens vision skal bidrage til at skabe enighed om, hvad vi gerne vil arbejde hen imod. Den skal give et billede af den fælles retning, som kan kommunikeres til andre i et klart sprog.

Visionen er idealbilledet. Etableringen af en sikkerhedsinfrastruktur, som understøtter visionen, vil ske løbende – måske kan visionen aldrig opfyldes helt, men man arbejder alle i samme retning.

Implementering af nye og ændrede sikringsforanstaltninger vil ske i takt med, at eksisterende it-løsninger udskiftes, eller det kan være ændringer i ens forretningsbehov eller trusselsbilledet, der betinger, at man er nødt til at foretage ændringer i sin sikkerhedsarkitektur. Det kan også være, at

den teknologiske udvikling teknisk og økonomisk gør det muligt at etablere sikringsforanstaltninger, der nedbringer risikoen for sikkerhedsbrud.

I 2009 formulerede programstyregruppen for infrastruktur, nedsat af Digital Sundhed(SDSD) en vision for den nationale infrastruktur. Visionen var at skabe forudsætningen for, at *enhver aktør indenfor sundhedsvæsnet til enhver tid og på ethvert givent sted kan tilgå de digitale oplysninger, som vedkommende måtte have behov for og ret til at se i den givne situation*.

Referencearkitekturen for informationssikkerhed skal understøtte denne infrastrukturvision, bl.a. gennem formuleringen af en *fælles sikkerhedsmodel*. Denne skal:

- medvirke til at sikre, at sundhedspersoner med samme arbejdsfunktion og relation til patienten får adgang til de *samme data* uafhængigt af behandlingssted
- gøre det *nemt* for brugeren at få adgang til relevante oplysninger på tværs af systemer

Dermed understøtter visionen digitaliseringsstrategiens[8] målsætninger om at skabe større sammenhæng i sundhedsvæsenet gennem sikker kommunikation og at forebyggelse og behandling i højere grad kan ske i lokalområdet eller i borgerens eget hjem.

Digitaliseringsstrategien har også som målsætning at se borgeren som et aktiv. I relation til informationssikkerhed må en vision derfor også rumme borgerens ønske om at selv at have indflydelse på, hvordan deres personlige oplysninger anvendes og af hvem. *Borgeren skal kunne føle sig tryg ved, at oplysninger er tilgængelige og korrekte, og at det kun er personer, for hvem det er relevant, der kan få adgang til dem.*

Men der er en forventning om, at borgeren fremover vil spille en mere aktiv rolle. I digitaliseringsstrategien for sundhedsvæsenet beskrives dette således:

”Borgere og patienter skal inddrages mere, og den viden, som borgere og patienter ofte er i besiddelse af, skal anvendes som et aktiv i forbindelse med forebyggelse og sygdomsbehandling. Digitaliseringen skal lette den enkeltes adgang til at se og afgive egne oplysninger, gå i dialog og danne netværk med andre patienter og sundhedsprofessionelle, og i øvrigt orientere sig om sundhedsvæsenets tilbud. Samtidig skal digitaliseringen give mulighed for, at den enkelte kan deltage aktivt og påvirke sin egen helbredstilstand fx gennem shared care-løsninger, monitorering og behandling i hjemmet mm.”

Og lidt senere:

”Digitaliseringen skal understøtte overgangen til et sundhedsvæsen, der i højere grad lægger vægt på forebyggelse. Det er i den forbindelse vigtigt at stille relevante oplysninger til rådighed for den enkelte borger, og hjælpe vedkommende i selve forebyggelsesindsatsen samt evaluere og følge op på denne.”

I forhold til referencearkitekturen for informationssikkerhed indebærer det derfor, at den også skal:

- udnytte den viden borgeren har om eget behandlingsforløb og den personlige interesse borgeren har i at påvirke informationsstrømmen og sikre berettiget adgang til personlige oplysninger

[8] Den nationale strategi for digitalisering af sundhedsvæsenet 2008-2012

- give borgeren mulighed for aktivt at bruge sine sundhedsoplysninger i sammenhænge bestemt af borgeren

Opsamlede data skal benyttes til andet end umiddelbare behandlingsmæssige formål. I visionen for digitalisering af sundhedsvæsenet er der målsætninger om, at data kan benyttes til forskning, kvalitetsudvikling, øgning af patientsikkerheden, understøttelse af forebyggelsesindsatsen og optimering af den daglige drift. For nogle af disse formål er det vigtigt at vide, at sammenstillede data vedrører samme behandling eller samme patient. Men det betyder ikke, at det er nødvendigt at kende identiteten af patienten. Visionen med referencearkitekturen for informationssikkerhed er, at:

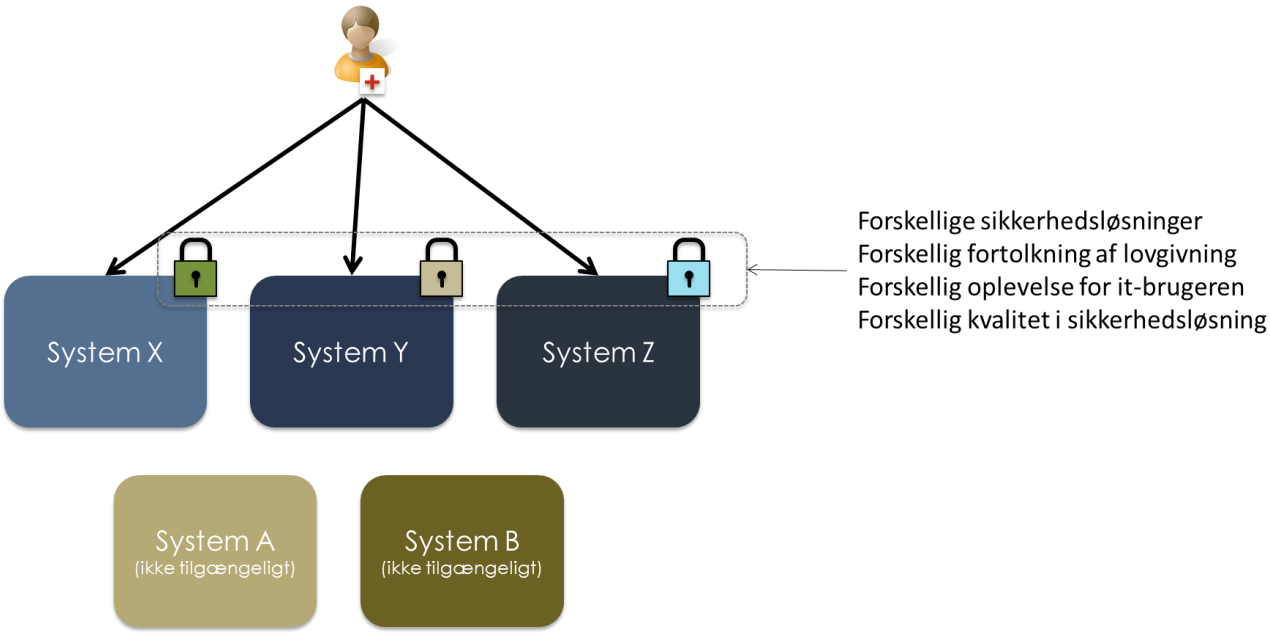
- give sundhedsorganisationer og myndigheder mulighed for at bruge patienternes sundhedsoplysninger til udvikling af sundhedsvæsenet - uden mulighed for, at personer involveret i behandlingen af disse oplysninger kan få kendskab til patienters identitet

Endelig er det også visionen, at den fælles sikkerhedsmodel beskrevet i referencearkitekturen skal:

- bidrage til en mere effektiv ressourceudnyttelse ved design, udvikling, implementering, administration og revision af systemløsninger
- (og dermed) bidrage til at øge hastigheden hvormed der kan digitaliseres.

2.4 Forretningsmæssigt målbillede

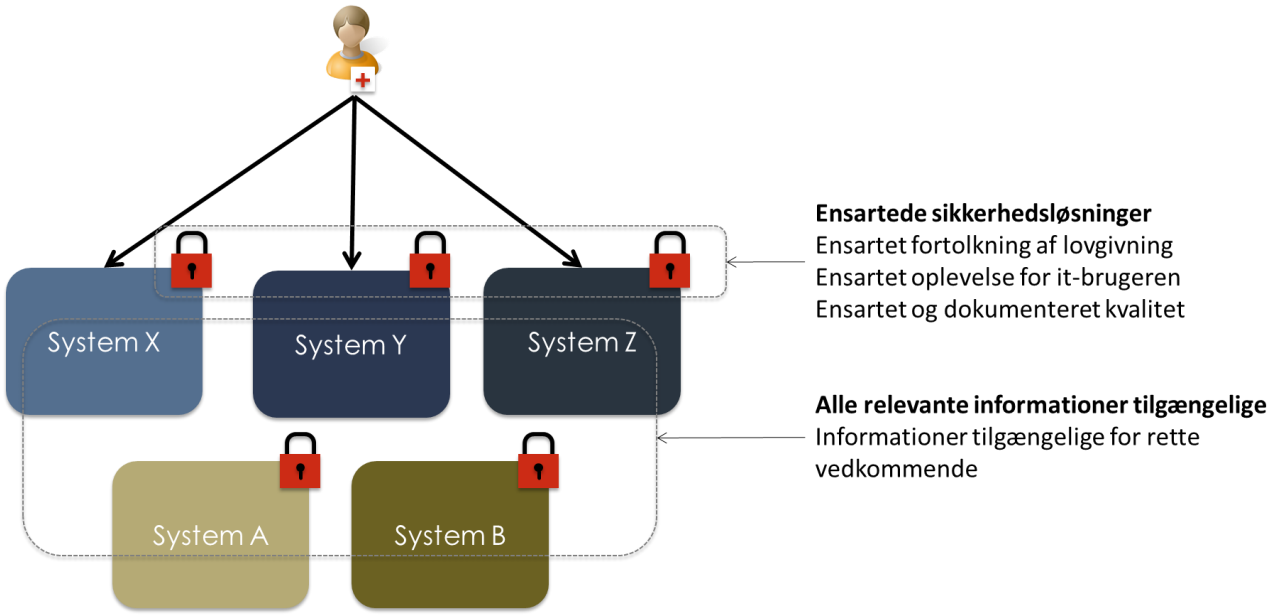
Hvor referencearkitekturens vision er meget langsigtet og kan forekomme ideel, er formålet med referencearkitekturens målbillede at beskrive en konkret sikkerhedsmodel, som inden for de kommende 5-7 år kan bidrage til et højere og mere ensartet sikkerhedsniveau, lettere adgang for de sundhedsfaglige brugere til relevante informationer om de patienter, de har i behandling, og større sikkerhed for, at de informationer, der bruges som grundlag for behandlingen, er korrekte og opdaterede.



Figur 7 - Nuværende situation med eksempel på forskelligartede løsninger og egenskaber og ukomplet datatilgængelighed.

I figuren ovenfor beskrives den nuværende situation, hvor brugeren oplever mange forskellige sikkerhedsløsninger med hver sin brugeradministration og rettighedskontrol.

Nedenfor ses målbilledet, hvor det ved at etablere en ensartet sikkerhedsmodel baseret på en ensartet fortolkning af lovgivningen bliver muligt at gøre alle relevante informationer tilgængelige for brugeren uden at denne skal logge på de enkelte systemer.



Figur 8 - Målbilledet. Sikkerhedsløsninger af ensartet høj kvalitet. Alle relevante informationer tilgængelige.

I målbilledet bruger alle systemer og tjenester de samme "remedier" i forhold til it-sikkerhed. Det betyder også, at hvis it-brugerne først har fået adgang til ét system, der anvender de standardiserede sikkerhedsteknologier, er det alt andet lige meget simplere og billigere at få adgang til det næste.

Et godt eksempel på dette er sikkerheden introduceret med Det Fælles Medicinkort (FMK), der er den første brede anvendelse af den sikkerhedsmodel vedrørende web service, som blev etableret gennem SOSI projektet. I forbindelse med FMK er en del af sektorens it-systemer blevet omlagt til denne sikkerhedsmodel og de tjenester, der omgiver den. Der er planlagt en række nationale tjenester, der genanvender sikkerhedsmodellen (DDV, NPI, og diverse indberetningsløsninger), og integration til disse kommende anvendelser vil derfor hurtigt og omkostningseffektivt kunne tages i anvendelse fra disse systemer.

Borgerens mulighed for selv at styre, hvem der skal have adgang til deres informationer, understøttes af fælles komponenter til at håndtere både patientens ret til at frabede sig indhentning eller videregivelse og til at patienten kan give en sundhedsperson, de ønsker inddraget i behandlingen, et positivt samtykke.

Kvaliteten af de informationer, der lægges til grund for patientbehandlingen sikres gennem fastlæggelse af indholdsmæssige standarder, der sikrer en ensartet forståelse på tværs i

sundhedsvæsenet og gennem aftaler parterne i mellem om, hvordan og hvornår informationer opdateres og hvordan de stilles til rådighed på tværs af domæner.

2.5 Værdiskabelse

Referencearkitekturen for informationssikkerhed skal danne grundlag for udviklingen af en fælles sikkerhedsmodel, der gør det enklere og billigere at etablere nye fælles it-løsninger med det tilstrækkelige sikkerhedsniveau.

F.eks. skal referencearkitekturen benyttes som ramme i forbindelse med videreudvikling, udvikling og anskaffelse af nationale tjenester. En ensartet adgang til nationale tjenester på en sikker og effektiv måde vil over tid kunne bidrage til øget effektivitet, mindre ressourceforbrug og forbedret kvalitet i behandlingen.

Samtidig er det i dag en stor administrativ byrde i at håndtere rettigheder til både lokale og nationale systemer og ikke mindst at sikre, at disse vedligeholdes, når en sundhedsfaglig skifter arbejdsfunktion, skifter arbejdssted, eller får nyt job ved en anden arbejdsgiver. Referencearkitekturen skal bane vejen for, at den ovenfor nævnte administrative byrde minimeres; og det gøres blandt andet ved at tegne et målbillede, hvor adgangen bliver ensartet og bestemmes af tildelte arbejdsfunktioner – ikke ved individuelle rettighedstildelinger.

Nedenstående tabel opsummerer de værdier som ønskes realiseret ved nærværende referencearkitektur for informationssikkerhed.

Resultat	**Værdi**
Fælles begrebsramme	Referencearkitekturen etablerer en fælles begrebsramme vedr. informationssikkerhed, der gør det enklere at kommunikere sikkerhedskrav ved udvikling af nye løsninger
Ensartet terminologi i lovgivning og anden borgerrettet information	Lette kommunikation med borgere omkring rettigheder og sikkerhedsmæssige aspekter
Beskrivelse af domæner og sammenhænge/integrationer mellem disse i referencearkitektur	Klar ansvarsfordeling
Borgeren får mulighed for at selv at påvirke, hvem der skal have adgang til deres data	Større tillid til, at det offentlige opbevarer og anvender følsomme data på en hensigtsmæssig måde
Ensartet sikker adgang til data og tjenester for de sundhedsfaglige på tværs af sektorer og systemer	Øget kvalitet i patientbehandlingen og øget effektivitet ved indhentning af nødvendig information til understøttelse af behandlingen.
Ensartede sikkerhedskrav til løsninger	Gør det lettere for leverandører at udvikle sammenhængende løsninger med genbrugelige sikkerhedskomponenter
Ensartede sikkerhedskrav til løsninger	Forenkler opgaven med at kravspecificere individuelle og sammenhængende løsninger
Mulighed for genbrug og anvendelse af fælles komponenter	Hurtigere og billigere udvikling af løsninger. Nye informationskilder ”tilkobles” hurtigere og mere omkostningseffektivt den samlede mængde af tilgængelige informationer.

Koordinering mellem nationale og internationale standarder	Øget markedspotentiale og større konkurrence
Fælles krav til leverandører	Større mulighed for at påvirke leverandørernes produkter
Ensartede sikkerhedskrav og overholdelse af standarder	Større leverandøruafhængighed
Referencearkitekturens operationalisering af gældende lovgivning	Der skal bruges mindre tid og færre ressourcer på at sikre, sig, at it-løsninger lever op til persondatalovens og sundhedslovens krav
Genbrug af model og løsninger	Gør det lettere at dokumentere overholdelse af lovkrav overfor de relevante myndigheder (f.eks. Datatilsynet) og revision
Standardisering og genbrug af registreringer	Letter administration af brugere og rettigheder

2.6 Principper for informationssikkerhed i sundhedsdomænet

Et af de væsentligste elementer i en referencearkitektur er principperne. Principperne fastlægger trædestenene mellem den nuværende situation og den fremtidige situation. Systemerne bliver ikke ens, men de skabes så at sige "efter samme læst" og er således med til at give it-brugerne og/eller borgeren/patienten den samme oplevelse af det, som referencearkitekturen omhandler – i dette tilfælde informationssikkerhed.

Der tages eksplicit udgangspunkt i de overordnede arkitekturprincipper for Sundhedsområdet, der blev udarbejdet og ratificeret af sundhedsvæsnets parter i 2009 i regi af SDSD [SundPrincip2009]. De overordnede principper er rammesættende for det videre arbejde i sundhedsvæsnet, og principperne i nærværende referencearkitektur forholdes derfor til det eksisterende arbejde.

På det helt overordnede plan henvises der til IT- og Telestyrelsens arkitekturprincipper, der i regi af styrelsen og OIO komiteen blev udgivet i april 2009 til brug for blandt andet tværoffentlig digitalisering. Principperne er relativt generelle, men stadig til en vis grad rammesættende også for informationssikkerhedsindsatsen. Arkitekturprincipperne er vedlagt som bilag C.

2.6.1 Overblik over principperne

De vedtagne arkitekturprincipper for Sundhedsområdet er opdelt i følgende hovedområder:

- Forretningsarkitektur
- Digitaliseringsarbejdets processer og styringsmæssige ramme
- Informationsarkitektur
- Applikationsarkitektur
- Teknisk arkitektur

Denne opdeling følges i beskrivelsen af principperne for informationssikkerhed nedenfor.

Forretningsmæssige principper
F1 Ensartet og sikker adgang til sundhedsdata opnås gennem nationalt fastsatte rammer
F2 Afvejning af borgerens og samfundets interesser sker gennem understøttelse af gældende lovgivning
F3 Specifikke rettigheder for medarbejdere opnås på baggrund af registrerede arbejdsfunktioner
F4 Den rette kvalitet i informationssikkerhedsarbejdet opnås effektivt ved at følge nationale og

internationale standarder
Styringsmæssige principper
S1 Ansvaret for sikring af givne informationer er altid entydigt placeret
S2 Sikringsforanstaltninger fastlægges på baggrund af risikoanalyser
S3 Det nødvendige sikkerhedsniveau etableres gennem entydige og klare politikker og aftaler
S4 Indtænk borgeren som et aktiv i sikringen af information
Informationsprincipper
(p.t. ingen)
Applikationsprincipper
(p.t. ingen)
Tekniske principper
T1 Anvend national infrastruktur til kommunikation mellem sundhedsvæsenets parter
T2 Tekniske sikringsforanstaltninger skal være robuste mod udfald af dele af infrastrukturen
T3 Kvaliteten af de anvendte sikringsforanstaltninger skal løbende forbedres

2.6.2 Principper for forretningsarkitektur

F1:	**Ensartet og sikker adgang til sundhedsdata opnås gennem nationalt fastsatte rammer**
Beskrivelse:	Ved at følge fælles bestemmelser og retningslinjer i lovgivning, referencearkitekturer, standarder og vejledninger opnås en ensartet og sammenhængende sikkerhedshåndtering på et fælles højt sikkerhedsniveau.
Rationale:	Lige adgang til behandling på et ensartet højt kvalitetsniveau forudsætter lige adgang til information. Det er derfor vigtigt, at sundhedspersoner med samme arbejdsfunktion og relation til patienten har samme adgang til information om denne, uanset hvor i sundhedsvæsenet, de er placeret og uanset, på hvilken måde, informationer tilgås. Endvidere skal borgeren / patienten have samme muligheder for at styre adgangen til personlige oplysninger, uanset hvor og af hvem i sundhedsvæsenet vedkommende behandles.
Implikationer:	Princippet medfører, at sundhedsvæsenets parter fremover skal stille krav til deres systemleverandører om at overholde nationalt fastsatte vejledninger og sikkerhedsstandarder i overensstemmelse med denne referencearkitekturs anvisninger og indenfor rammerne af gældende lovgivning. Parterne skal endvidere afstå fra at stille krav til adgangsbegrænsende sikringsforanstaltninger i systemer, som ikke kan begrundes af nationalt fastsatte rammer (lovgivning, referencearkitekturer, standarder, vejledninger etc.). De nationalt fastsatte rammer skal dog give parternes ledelse mulighed for at begrænse medarbejderes adgang til information bestemt af deres arbejdsmæssige funktion (jf. princip F3 nedenfor). Dette fordrer, at de nationale rammer er formuleret tilstrækkeligt præcist, entydigt og operationelt og definerer et hensigtsmæssigt og tilstrækkeligt sikkerhedsniveau.
Referencer:	Arkitekturprincipper for Sundhedsområdet [Sikkerhedsarkitektur]: • Sammenhængende helhedssyn skal danne grundlag for en målstyret udvikling af den nationale sundheds-it-arkitektur og infrastruktur med et internationalt perspektiv.

F2:	Afvejning af borgerens og samfundets interesser sker gennem understøttelse af gældende lovgivning
Beskrivelse:	Love, bekendtgørelser og vejledninger udtrykker en afvejning af de samfundsmæssige hensyn og hensynet til borgerens retssikkerhed og beskyttelse af privatlivets fred. Det er denne afvejning der skal være udgangspunktet for sikkerhedshåndteringen og ikke individuelle opfattelser af, hvad der vil være ret og rimeligt.
Rationale:	Borgernes rettigheder og samfundets interesser er politiske emner, der skal behandles af folkevalgte. Alle borgere i landet bør grundlæggende have samme rettigheder, om end der kan være særlige regler, der vedrører særlige befolkningsgrupper (personer under værgemål etc.), og rettigheder bør grundfæstes i gældende dansk lovgivning.
Implikationer:	Ønsker om ændring af den generelle adgang til information hørende til bestemte grupper af borgere eller patienter skal rejses overfor de lovgivende myndigheder. Der må ikke indføres adgangskontroller, der uden hjemmel i lovgivning diskriminerer bestemte befolknings- eller patientgrupper. Eksempelvis skal der ikke ske en generel begrænsning af adgang til psykiatriske data, men mindre dette er lovbestemt.
Referencer:	Arkitekturprincipper for Sundhedsområdet [Sikkerhedsarkitektur]: • Sammenhængende helhedssyn skal danne grundlag for en målstyret udvikling af den nationale sundheds-it-arkitektur og infrastruktur med et internationalt perspektiv

F3:	Specifikke rettigheder for medarbejdere opnås på baggrund af registrerede arbejdsfunktioner
Beskrivelse:	Parterne på sundhedsområdet skal registrere hvilke ansættelsesforhold en person har og hvilke arbejdsfunktioner vedkommende bestrider i disse ansættelsesforhold. De enkelte systemer og tjenester skal på baggrund af denne information afgøre hvilke specifikke adgangsrettigheder den pågældende medarbejder har til systemet eller tjenesten.
Rationale:	En medarbejder må kun få adgang til oplysninger der er relevante i forhold til vedkommendes arbejdsfunktion. Det er ledelsen i den organisation, som medarbejderen er tilknyttet, der bestemmer vedkommendes arbejdsfunktion og som derfor er ansvarlig for registrering heraf. Omvendt er det den dataansvarlige bag systemer og tjenester, der skal sikre, at en given bruger har ret til at behandle data. Dette sker ved at den dataansvarlige (med systemejeren) fastlægger hvilke konkrete adgangsrettigheder brugere med forskellig arbejdsfunktioner skal have. Ved at operere med fælles (nationale) definitioner og klassifikationer af arbejdsfunktioner, vil brugere med samme arbejdsfunktion kunne tildeles samme adgangsrettigheder i systemer. Opgaven med brugeradministration vil forsimples væsentligt i løsninger, der bygges efter dette princip, idet der alene skal administreres ansættelsesforhold og standardiserede arbejdsfunktioner og ikke individuelle rettigheder i alle specifikke systemer og tjenester (ved alle parter).
Implikationer:	Dataansvarlige og systemejere bør fremover tage udgangspunkt i nationalt fastlagte arbejdsfunktioner (national standard), når der skal tages stilling til konkrete adgangsrettigheder. Såfremt disse ikke findes tilstrækkelige i den konkrete situation, skal muligheden for at ændre i den nationale standard overvejes før adgangsbegrænsningen eventuelt skabes på baggrund af anden styringsinformation. Men mindre tungtvejende grunde taler herfor, skal man som udgangspunkt afstå fra at definere adgangsbegrænsning ud fra oplysninger om faggruppe, ansættelsessted eller anvendte systemer, da der kan være stor variation i hvordan man har organiseret sig om opgaveløsningen forskellige steder i sundhedsvæsenet. Endvidere vil fokus på de konkrete arbejdsfunktioner (frem for bestemte faggrupper/uddannelser) gøre det lettere at understøtte opgaveglidning og tværfagligt samarbejde i sundhedsvæsenet. Lovgivningsmæssigt skal man så vidt muligt fokusere på at fastlægge overordnede rammer for adgang til data frem for at forsøge at fastlægge specifikke rettigheder for medarbejdergrupper. En meget detaljeret lovgivning kan let blive for ufleksibel i forhold til sundhedsvæsenets udvikling.

	Det skal afgøres, hvorledes information om ansættelsesforhold og arbejdsfunktioner ved de enkelte parter gøres tilgængelige overfor systemer og tjenester ved andre parter.
Referencer:	Arkitekturprincipper for Sundhedsområdet [Sikkerhedsarkitektur]: • Tværgående, it-understøttede arbejdsprocesser ejes nationalt og skal spille sammen med decentralt ejede og it-understøttede lokale arbejdsprocesser • Lokale frihedsgrader i opgavevaretagelsen respekteres

F4:	**Den rette kvalitet i informationssikkerhedsarbejdet opnås effektivt ved at følge nationale og internationale standarder**
Beskrivelse:	Nationale og internationale standarder skal effektivt medvirke til at sikre, at væsentlige informationssikkerhedsmæssige risici håndteres i forbindelse med udbredelse af elektroniske informationer.
Rationale:	Styring af informationssikkerhed er en kompleks opgave, der griber ind i mange forskelligartede forhold, hvor mange og selv små detaljer kan gøre en stor forskel på hvor sårbar organisationen er overfor brud på informationssikkerheden. I en sådan situation er det værdifuldt at lade sig guide af rammeværk, standarder og vejledninger for effektivt at kunne opnå den tilstrækkelige informationssikkerhed. Et fælles grundlag i form af standarder, vejledninger, politikker m.v. vil gøre det samlede arbejde med informationssikkerhed mere effektivt (f.eks. er det mere effektivt for en revision at skulle forholde sig til politikker, der følger kendte standarder). Princippet betyder ikke nødvendigvis, at alle skal følge samme detaljerede standarder. Man kan eksempelvis forestille sig fælles overordnede standarder, der profileres til mere detaljerede standarder for parter med samme opgavemæssige og organisatoriske vilkår.
Implikationer:	Denne referencearkitektur vil pege på nationale og internationale standarder, vejledninger, politikker m.v. som parterne bør/skal følge for at få en ensartet håndtering af forskellige aspekter ved informationssikkerhed på et passende kvalitetsniveau. I det omfang, at standarderne er indarbejdet i nationale infrastrukturkomponenter og sikkerhedstjenester, bør udbyderen overveje at anvende disse, idet det yderligere kan sætte fart i digitaliseringen.
Referencer:	Arkitekturprincipper for Sundhedsområdet [Sikkerhedsarkitektur]: • Internationale, nationale og lokale initiativer skal koordineres med henblik på genbrug af såvel nye som allerede etablerede løsningselementer, standarder og infrastruktur. Standarder: DS484:2005 Standard for informationssikkerhed eller ISO/IEC 27001[9].

[9] Fra 2013 afløses DS484 af ISO/IEC 27001, som standard for den statslige sektor

2.6.3 Principper for digitaliseringsarbejdets processer og styringsmæssige rammer

S1:	Ansvaret for sikring af givne informationer er altid entydigt placeret
Beskrivelse:	Ansvaret for informationssikkerheden ligger hos den dataansvarlige organisation, uafhængigt af hvilke sikkerhedsmodeller, der etableres, eller hvilke sikkerhedstjenester der stilles til rådighed hos øvrige myndigheder eller organisationer (herunder leverandører og driftpartnere). Oplysninger kan "videregives" (i persondatalovens forstand). Hermed overtager den modtagende organisation dataansvaret for de oplysninger, den modtager og opbevarer.
Rationale:	Der må ikke være tvivl om, hvem der har ansvaret for at beskytte borgerens informationer, og dermed hvem der har ansvaret for at forebygge, opklare, begrænse og udbedre sikkerhedsbrud, samt evt. at sætte ind med kompenserende foranstaltninger. I forbindelse med oplevede sikkerhedsbrud, skal borgere og sundhedspersoner også vide, hvem de skal henvende sig til med sådanne hændelser.
Implikationer:	Alle parter bør have en fast politik for, hvilke oplysninger de selv er dataansvarlige for og hvilke de databehandler på vegne af andre. Det skal være tydeligt, hvornår der er tale om videregivelse af data til anden dataansvarlig og hvornår der blot er tale om databehandling. Der skal etableres redskaber, som kan synliggøre for parterne selv og for borgerne, hvem der til en hver tid er ansvarlig for sikring af de enkelte data.
Referencer:	Arkitekturprincipper for Sundhedsområdet [Sikkerhedsarkitektur]: • Ved deling af information fastlægges entydig definition af dataejerskab, vedligeholdelsesansvarlig samt anvendelsespolitikker.

S2:	Sikringsforanstaltninger fastlægges på baggrund af risikoanalyser
Beskrivelse:	Beslutning om, hvilke sikringsforanstaltninger, der skal etableres, skal baseres på en risikoanalyse.
Rationale:	Formålet med sikringsforanstaltninger er at beskytte mod hændelser der kan have negativ indvirkning på systemer og data (it-aktiver). Omkostningerne ved at etablere og drive sikringsforanstaltningerne skal imidlertid stå mål med de risici, som hændelserne udgør. En risikoanalyse kan medvirke til, at man får identificeret og vurderet de relevante risici, som det er vigtigt at sikre sig imod, og ikke skaber sikringsforanstaltninger, der er for omkostningskrævende at etablere i forhold til de reelle risici, eller som leder til ineffektivitet i arbejdsprocesser. Risikoanalysen dokumenterer de antagelser, der ligger til grund for de etablerede sikringsforanstaltninger. Antagelser om, hvilke kritiske hændelser, der kan opstå, hvad sandsynligheden er for at de opstår, hvilken indvirkning de har på it-aktiver og hvilke konsekvenser det har for forretningen og for privatlivets fred. Dette danner grundlag for en egentlig risikostyring, hvor ændringer i forretningsmodellen, ny viden om trusler samt erfaringer med de faktisk opståede hændelser, kan give anledning til at man revurderer risici og dermed løbende revurderer behovet for sikringsforanstaltninger.
Implikationer:	Ved etablering af nye it-løsninger skal der foretages en risikoanalyse.

	Ved væsentlige ændringer i forretningsmodel, trusselsbillede eller it-løsninger, skal der ske en revision af risikoanalysen. Der skal løbende følges op på indtrufne sikkerhedsmæssige hændelser og andre hændelser, der har forstyrret driften, for at vurdere, om dette giver anledning til revurdering af risici.
Referencer:	Arkitekturprincipper for Sundhedsområdet [Sikkerhedsarkitektur]: • Sammenhængende helhedssyn skal danne grundlag for en målstyret udvikling af den nationale sundheds-it-arkitektur og infrastruktur med et internationalt perspektiv. Vejledning om risikovurdering, IT- og Telestyrelsen, oktober 2007. Håndbog i privatlivsimplikationsanalyse, IT- og Telestyrelsen, marts 2010. Information security risk management standard ISO/IEC 27005: 2011.

S3:	**Det nødvendige sikkerhedsniveau etableres gennem entydige og klare politikker og aftaler**
Beskrivelse:	Der skal fastlægges et nationalt sikkerhedsniveau, der er veldokumenteret i form af fælles politikker og retningslinjer og som fastholdes gennem aftaler mellem parterne. Politikker, retningslinjer og aftaler skal være indbyrdes konsistente og være udformet på en sådan måde, at det eksempelvis gennem revision kan fastslås om parterne lever op til disse.
Rationale:	Sikkerhedsniveauet skal være beskrevet og må kun ændres gennem formel ledelsesmæssig beslutningsproces. Sikkerhedsniveauet må ikke ændres ubevidst som følge af at verden eller systemerne ændrer sig. Der opereres ikke med ”blind tillid” mellem parter, men med aftalebestemt sikkerhed, der kan gøres til genstand for opfølgning og styring.
Implikationer:	Der skal løbende ske en styring af, at sikkerhedsniveauet (baseline) opretholdes. Der skal etableres redskaber, som kan synliggøre for parterne, hvilke aftaler og hvilke politikker og retningslinjer der er gældende.
Referencer:	Arkitekturprincipper for Sundhedsområdet [Sikkerhedsarkitektur]: • Ved deling af information fastlægges entydig definition af dataejer, vedligeholdelsesansvarlig samt anvendelsespolitikker.

S4:	Indtænk borgeren som et aktiv i sikringen af information
Beskrivelse:	Overvej, hvorledes borgernes interesse i at kontrollere, hvem der har haft adgang til oplysninger om borgeren selv (samt personer som borgeren er værge for), samt eventuelt interesse i at styre, hvem der kan få adgang til sådanne oplysninger, kan udnyttes til at styrke sikkerheden.
Rationale:	Borgeren kender sit sygdomsforløb og har en personlig interesse i at informationer kun tilgås af relevante parter. Ved at lade borgeren se, hvem der har tilgået registreringer om vedkommende, vil borgeren ofte selv foretage en grundig kontrol af adgangen til data. Borgeren er p.t. ikke forpligtet til en sådan kontrol, så sådanne sikringsforanstaltninger må ikke gøres til forudsætninger for at opnå det tilstrækkelige sikkerhedsniveau. Der er udelukkende tale om en supplerende sikringsforanstaltning, der kan være med til at hæve sikkerhedsniveauet yderligere. Som beskrevet i visionen, skal borgere og patienter inddrages mere i egen behandling, og den viden, som de er i besiddelse af, skal anvendes som et aktiv i forbindelse med forebyggelse og sygdomsbehandling. Digitaliseringen skal lette den enkeltes adgang til at se og afgive egne oplysninger, gå i dialog og danne netværk med andre patienter og sundhedsprofessionelle. Dette vil være meget komplekst (umuligt?) at realisere uden at skabe sikringsforanstaltninger, der inddrager borgeren i styring af informationsstrømmen.
Implikationer:	Sundhedsvæsnets parter skal i alle nyanskaffelser samt i større omlægninger af nuværende systemer skulle tage højde for, at borgerne skal kunne indgå som en aktiv part.
Referencer:	Arkitekturprincipper for Sundhedsområdet[Sikkerhedsarkitektur]: • Udviklings- og implementeringsprocesser sikrer, at enhver it-løsning effektivt understøtter medarbejdernes gennemførelse af en eller flere veldefinerede forretningsprocesser, som inddrager borgere og patienter i hensigtsmæssigt omfang og sikrer dem en god service

2.6.4 Principper for informationsarkitektur

P.t. ingen.

2.6.5 Principper for applikationsarkitektur

P.t. ingen.

2.6.6 Principper for teknisk arkitektur

T1:	Anvend national infrastruktur til kommunikation mellem sundhedsvæsenets parter
Beskrivelse:	Al kommunikation sundhedsvæsenets parter imellem skal sikres gennem anvendelse af Sundhedsdatanettet (SDN). Udstilling af (web-) services parterne imellem sker på den nationale serviceplatform (NSP) og under sikring af de nationale sikkerhedskomponenter, der er implementeret på denne. Fælles (web-) applikationer skal kunne nås via den fællesoffentlige sundhedsportal (Sundhed.dk) og videokonferencer skal etableres gennem det af MedCom etablerede videoknudepunkt.
Rationale:	Det er komplekst og omkostningstungt at skabe den fornødne sikkerhed. Jo flere forskellige kanaler, der skal sikres, jo større er omkostningerne herved, og jo større er risikoen for at introducere svagheder, der kan føre til brud på sikkerheden eller som kan lede til et forskelligartet sikkerhedsniveau de forskellige kanaler imellem. Ved at anvende den nationale infrastruktur, er parterne sikre på at operere indenfor nationalt fastsatte sikkerhedsmæssige rammer.
Implikationer:	Sundhedsområdets parter skal afstå fra at etablere alternative kanaler til kommunikation mellem

	parterne, der vil udhule business casen for at drive fælles infrastrukturløsninger. Dette fordrer, at de fælles infrastrukturløsninger er sikret på et tilstrækkeligt højt niveau, og infrastrukturløsningerne skal være de første til at overholder nationale rammer.
Referencer:	Arkitekturprincipper for Sundhedsområdet[Sikkerhedsarkitektur]: • Sikkerhed relateret til tværgående arbejdsgange understøttes af den nationale infrastruktur. • Internationale, nationale og lokale initiativer skal koordineres med henblik på genbrug af såvel nye som allerede etablerede løsningselementer, standarder og infrastruktur.

T2:	**Tekniske sikringsforanstaltninger skal være robuste mod udfald af dele af infrastrukturen**
Beskrivelse:	Ved udarbejdelse af sikkerhedskomponenter, der anvender sikkerhedsinformationer fra eksterne systemer, skal der tages højde for, at eksterne driftsmiljøer kan være kraftigt belastede eller helt utilgængelige.
Rationale:	Selv om det er ønskeligt, kan normal drift af alle systemer ikke opretholdes i 100 % af tiden. Over tid vil der uvægerligt opstå uhensigtsmæssigheder eller uheld, der skaber nedbrud i dele af infrastrukturen. I disse tilfælde må it-sikkerheden ikke blive sat ud af spillet. Sikkerhedsmekanismer skal fortsat foretages selv om dele af organisationen er i "ø-drift".
Implikationer:	Hvis risikoen for sikkerhedsbrud ikke øges uacceptabelt ved at sikkerhedsmekanismer baseres på styringsinformation, der ikke er ajourført i en nærmere fastlagt periode, da skal sikkerhedskomponenter udformes, så informationer fra andre kilder opbevares (caches) lokalt. I tilfælde af eksterne nedbrud eller utilgængelighed til øvrige parter, skal sikkerhedsmekanismerne fortsætte med at fungere, om end de evt. opererer på ikke-ajourførte sikkerhedsinformationer.
Referencer:	Arkitekturprincipper for Sundhedsområdet [Sikkerhedsarkitektur]: • Tilgængelighed understøttes fra starten i nationale arkitekturelementer i alle arkitekturens lag • Understøttelse af tværgående arbejdsgange skal arkitekturmæssigt kunne afkobles fra de lokale systemer, således at udfald ikke blokerer for de primære, lokale arbejdsopgaver.

T3:	**Kvaliteten af de anvendte sikringsforanstaltninger skal løbende forbedres**
Beskrivelse:	I takt med at nye muligheder opstår skal det overvejes om disse muligheder med fordel kan udnyttes til forbedring af de anvendte sikringsforanstaltninger.
Rationale:	Sikkerhed er ikke noget kategorisk, og vil altid kunne forbedres. Dette bør dog kun ske i et omfang at omkostningerne herved i tilstrækkelig grad opvejes af reducerede risici for forretningen. Dette princip udtrykker, at det ikke kun er i forbindelse med udvikling af løsninger eller i forbindelse med væsentlige ændringer i trusselsbilledet at man bør overveje, om der skal ske ændringer i sikringsforanstaltninger. Den øgede digitalisering og den teknologiske udvikling giver nye muligheder for effektivt at beskytte sig mod trusler. Man bør derfor løbende overveje, om man kan skabe forbedringer i eksisterende sikringsforanstaltninger, og derved, om man med rimelige omkostninger kan nedbringe risici for forretningen yderligere, eller om forbedrede sikringsforanstaltninger kan afløse andre sikringsforanstaltninger, som er dyrere at drive (f.eks. ved at behovet for supplerende, kompenserende sikringsforanstaltninger mindskes, eller at man kan afløse dyre organisatoriske sikringsforanstaltninger med billigere tekniske sikringsforanstaltninger).
Implikationer:	Da sikkerhed ikke er noget kategorisk og sikringsforanstaltninger derfor ikke nødvendigvis er ideelle, skal man overveje om der han iværksættes supplerende sikringsforanstaltninger, der kan kompensere for de begrænsninger som de anvendte sikringsforanstaltninger har. Når nye registre etableres eller kvaliteten eksisterende registre forbedres, skal det overvejes, om den forbedrede adgang til mere præcis information kan benyttes til at forbedre kvaliteten af de kontroller,

	der er etableret. Eksempelvis vil elektronisk opsamling af henvisninger i en given periode kunne tages i anvendelse til at udtale sig mere præcist om eksistensen af en behandlingsrelation mellem patienten og medarbejdere ved den sundhedsorganisation, der har modtaget henvisningen. Ved etablering af nye nationale sikkerhedskomponenter og services skal sundhedsvæsenets parter vurdere, om disse med fordel vil kunne bringes i anvendelse til at beskytte individuelle infrastrukturer og systemer.
Referencer:	Arkitekturprincipper for Sundhedsområdet [Sikkerhedsarkitektur]: • Realisering af national arkitektur og infrastruktur skal ske trinvist og behovsstyret med fokus på løbende leverancer med umiddelbar nytteværdi. • Applikationer og komponenter skal kunne indgå som byggesten og serviceudbydere i en national serviceorienteret arkitektur.

2.7 Sikkerhedsmodeller

Både på fællesoffentligt plan og på domæneplan i sundhedssektoren, er der blevet arbejdet med it-sikkerhedsmodeller i en længere årrække. Senest har It- og Telestyrelsen udarbejdet et diskussionspapir [SikModeller] vedrørende nogle nye sikkerhedsmodeller, med særlig fokus på hensynet til privatlivets fred ("privacy by design"). Modellerne vurderes endnu ikke at være tilstrækkelig modne til at få plads i denne referencearkitektur, men efterhånden som der arbejdes med praktisk implementering af disse, bør man løbende forholde sig til, om dele heraf skal indarbejdes heri.

Af mere klassiske sikkerhedsmodeller kan nævnes[10]:

Sikkerhedsmodel	Beskrivelse
Perimeter trust	Perimeterbasered trust er en særlig variant af trust, hvor man indenfor en etableret perimeter har ubetinget tillid til samtlige parter (herunder påstande om egen eller brugeres identitet). Denne arkitektur forudsætter en yderst grundig sikring af perimeteren, idet en angriber, der formår at tiltvinge sig adgang til det beskyttede område, har fuldstændig frie hænder. Denne type trust adskiller sig fra de øvrige ved at der ikke som sådan indgås aftaler mellem aftagere og udbydere, idet alene tilstedeværelsen på det beskyttede område er tilstrækkeligt bevis for troværdigheden af aktørerne. Perimeterbaseret sikkerhed har sin primære berettigelse i små og stramt kontrollerede miljøer, hvor der er et begrænset antal kontaktflader med omverdenen, f.eks. et servermiljø.
Pairwise trust	Pairwise trust er den simpleste trust-model, hvor parterne indgår bilaterale aftaler. Arkitekturen er velegnet når ganske få parter med få it-services indgår et samarbejde , men skalerer Arkitekturen skalerer relativt dårligt, idet tilføjelsen af en ny service kræver at samtlige serviceaftagere skal opdateres med yderligere sikkerhedsinformation. Mængden af aftaler vokser med produktet af antal serviceaftagere og serviceudbydere (2 serviceudbydere og 10 aftagere → 20 aftaler, 3 serviceudbydere og 10 aftagere → 30 aftaler). Pairwise trust har dermed sin primære berettigelse i sammenhænge, hvor antallet af aktører er begrænset.

[10] Disse modeller beskrives i yderligere detaljer i bl.a. publikationen fra National Institute of Standards and Technology: "Guide to Secure Web Services" [NIST800-95].

Brokered trust	En uafhængig tredjepart fungerer som trusted third party (TTP) for både serviceaftager og serviceudbyder. I denne model laver serviceaftager og serviceudbyder hver én aftale (med den fælles TTP). Med brokered trust er antallet af aftaler direkte propertionalt med summen af serviceaftagere og –udbydere (2 serviceudbydere og 10 aftagere → 12 aftaler, 3 serviceudbydere og 10 aftagere → 13 aftaler). Brokered trust har sin primære berettigelse i sammenhænge, hvor aftagere og udbydere har en organisatorisk og/eller sektormæssig egenskab til fælles, eksempelvis tilhørsforhold til sundhedssektoren.
Federated trust	Federated (fødereret) trust er en udvidelse af brokered trust og pairwise trust, idet en organisation kan anvende én TTP, og anvende en service, der baserer sin tillid på en anden TTP, blot de to TTP'er har indbyrdes tillid. Serviceaftagere og –udbydere indgår i brokered trust som beskrevet ovenfor (dvs direkte propertionalitet mellem antallet af aktører og aftaler), og TTP'erne indgår i pairwise trust. Typisk vil antallet af TTP'er være relativt lavt, og antallet af aftaler som konsekvens af pairwise trust mellem TTP'er vil derfor også være lavt. Federated trust har sin primære berettigelse, hvor grupper af aftagere og udbydere på tværs af domæner og sektorer indgår i en sammenhæng.

Nedenfor beskrives en række overvejelser om de enkelte modeller.

2.7.1 Perimeter trust

Denne form for sikkerhedsmodel kan tages i anvendelse, når perimeteren er meget lille (eksempelvis er det sjældent nødvendigt at beskytte interne servicesnitflader på den samme serverplatform), og når det er samme organisation, der har ansvaret for hele perimetersikkerheden.

Modellen er ikke velegnet til at spænde over alle parter og alle systemer på sundhedsområdet.

2.7.2 Pairwise trust

Det er i bund og grund denne model sundhedsdatanettet bygger på. Modellens manglende skalerbarhed giver imidlertid løbende udfordringer. I situationer, hvor de enkelte brugere eksempelvis skal have adgang til en web applikation / portalløsning har det været umuligt at indgå sundhedsdatanetaftaler fra alle arbejdsstationer. Så i stedet oprettes adgang fra de enkelte organisationers firewall til det pågældende system, hvorved alle på netværket i princippet får adgang hertil. Tilsvarende med videokonference: Her har løsningen været at åbne op for alle til et fælles knudepunkt. At system-til-system kommunikation ikke har givet større administrationsbyrde i dag skyldes at hovedparten af denne trafik fortsat sendes som MedCom beskeder via VANS-leverandører (disse agerer som knudepunkter for besked-orienteret kommunikation). Hvis ikke der havde været etableret et serviceknudepunkt (i form af den nationale serviceplatform, NSP), da ville system-til-system kommunikation baseret på web services også fremover give en administrationsudfordring. Modellen kan derfor ikke stå alene.

2.7.3 Brokered trust / Trusted Third Party

Udviklingen af fællesoffentlige løsninger og nationale løsninger på sundhedsområdet er bygget meget op omkring denne model. De ovenfor nævnte knudepunkter (videoknudepunktet etc.) er jo eksempler på løsninger, som alle parter på sundhedsområdet "truster".

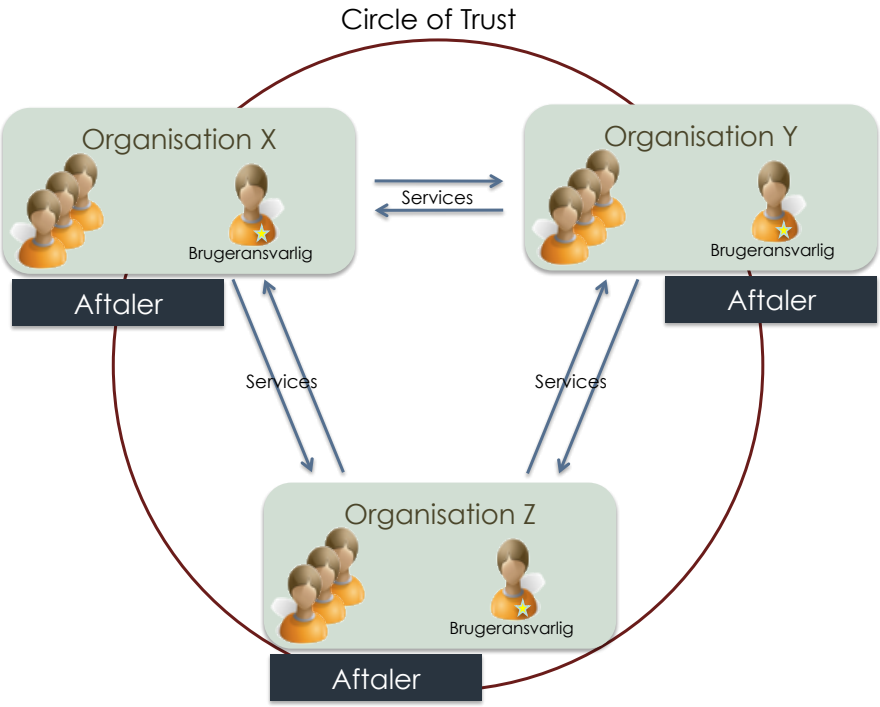
Tilsvarende har vi tillid til at CPR-registret har styr på borgernes identiteter og at OCES operatøren har styr på borgercertifikater, medarbejdercertifikater og virksomhedscertifikater. Alle web applikationer og portalløsninger har tillid til at NemLogin formår at autentificere brugerne korrekt.

Tilsvarende har web services på sundhedsområdet tillid til, at den udviklede billetudsteder, SOSI-STS formår at autentificere brugerne korrekt.

I forbindelse med kommunikation med SOSI-STS og nationale web services over den nationale serviceplatform, skal der kun indgås én aftale med NSP-komplekset (og der er et fast koncept omkring dette).

2.7.4 Federated trust

En føderation er en konstruktion, indenfor hvilken tillid til it-sikkerhedselementer formidles mellem organisationer. Føderationstilgangen gør det muligt for organisationer at udstille og anvende services uden at skulle indgå i bilaterale aftaler med samtlige organisationer i føderationen. I stedet indgår hver organisation en føderationsaftale, hvor et sæt af krav og regler skal overholdes.



Figur 9 – Føderation. Parterne har *tillid* til hinanden i forhold til at overholde de i aftalen beskrevne sikkerhedsforanstaltninger.

Føderationer kan være forskellige i forhold til hvilke krav og regler, der skal opfyldes af føderationens parter (d.v.s. hvordan aftalen skal se ud). I en føderation, hvor de kommunikerede digitale informationer ikke er særligt følsomme, vil kravene i relation til it-sikkerhed typiske være mindre og færre, end i føderationer hvor en brist i it-sikkerheden kan have alvorlige konsekvenser.

2.7.4.1 Internationale standarder vedrørende autenticitet af brugere

Liberty Alliance, et internationalt standardiseringsprojekt, der beskæftiger sig med sikkerhed, identitet og tillid, har udarbejdet en operationel de facto standard for aftaler til føderationer. Standarden, der går under navnet Liberty Identity Assurance Framework (Liberty IAF, eller blot LIAF).

I sin grundform er LIAF et dokument, der beskriver en lang række meget specifikke organisatoriske og tekniske krav, der skal overholdes af de parter, der indgår i en identitetsføderation. LIAF giver

mulighed for at operere med flere niveauer af autenticitetssikring (såkaldt *Assurance Levels*). Overordnet gælder det, at jo højere niveau af autenticitetssikring der ønskes, jo flere og strammere betingelser skal der overholdes. Betingelserne er udformet, således at underliggende niveauers betingelser automatisk er overholdt på højere niveauer, og opnåelse af et højere niveau medfører derfor, at de underliggende niveauer også er opnået.

Skematisk kan niveauerne stilles op som følger:

Niveau	**Sikkerhed**	**Kan anvendes ved f.eks.**	**Konsekvens ved brud på tillid**
1	Lille eller ingen sikkerhed for identitet	Online diskussionsfora, kundelogin til onlinebutikker, etc.	Lille eller ingen risiko for tab eller skade
2	Nogen tiltro	Adgang til forsikringsselskabers online systemer (f.eks. ændring af adresseoplysninger)	Moderat risiko for ”besvær” og uautoriseret tilgang til følsomme data.
3	Høj tillid	Patentansøgninger, finansielle systemer, adgang til stærkt følsomme data.	Betydelig risiko for finansiel skade.
4	Meget høj tillid	Patientsystemer med mulighed for at ordinere og udlevere medicin og plejehandlinger.	Betydelig risiko for finansiel og fysisk skade.

Ovenstående er baseret på niveauer beskrevet i Electronic Authentication Guideline fra National Institute of Standards and Technology (NIST), USA [NIST 800-63].

En organisations anvendelse af LIAF og erklæring om konformitet mod denne giver mulighed for at regulere, hvilket niveau af tillid øvrige parter i føderationen kan have til organisationen og dennes håndtering af identitetssikkerhed. Eksempelvis kan en organisation i en føderation beslutte sig for at følge et givent sikkerhedsniveau, f.eks. niveau 3. Med en certificeret erklæring om at følge LIAF for dette niveau vil organisationen have bevis for at, at de fornødne procedurer mv. overholdes, og øvrige parter har et grundlag for have tillid til identiteten af brugere og systemer fra den pågældende organisation.

LIAF er målrettet rene aftalebaserede føderationer (hvor sikkerheden alene er reguleret af aftaler), og da tilliden her skal være meget omfattende, omfatter LIAF alle aspekter, der har med sikkerhed og identiteter at gøre. Afhængigt af hvilket *Assurance Level* en føderation skal understøtte, kan det være en meget omfangsrig proces at blive certificeret til føderationen. Den rene aftalebaserede føderation har dog den fordel, at hver enkelt organisation i føderationen kan implementere sin egen identitetsløsning uafhængigt af de andre organisationer.

Således vil hver enkelt organisation have det fulde ansvar for håndtering af IT brugerne og deres akkreditiver. Organisationen forestår selv oprettelse af brugere og deres akkreditiver (eksempelvis i et Active Directory eller med smartcards udstedt af organisationen selv), og når en bruger logger på et IT system, er det også organisationen, der har ansvaret for at gennemføre autentificering af brugeren.

Forskellige organisationer kan operere med forskellige akkreditiver og så alligevel leve op til det samme assurance level. Eksempelvis kan man ifølge NIST Electronic Authentication Guideline [NIST 800-63] leve op til niveu 3, såfremt man har en multifaktor løsning (”noget man ved” og ”noget man har”), hvor ”det man har” enten er baseret på enten et engangskode-device, signeringsnøgler i fil, eller signeringsnøgle i hardware device (smartcard eller lignende).

Ved kommunikation på tværs af lande i Europa er det oplagt at basere sig på rene aftalebaserede føderationer, idet identifikation og autenticitetssikring af brugere og sundhedspersoner i de enkelte lande ikke baserer sig på noget fælles system.

2.7.5 Blandede sikkerhedsmodeller (federated trust med trusted third parties)

I LIAF skelnes der mellem sikkerhed for, at et akkreditiv og en fysisk identitet matcher hinanden ved oprettelse (*Identity Proofing*) og sikkerhed for at et akkreditiv i anvendelsesøjeblikket anvendes korrekt (autentifikation og *Credential Management*).

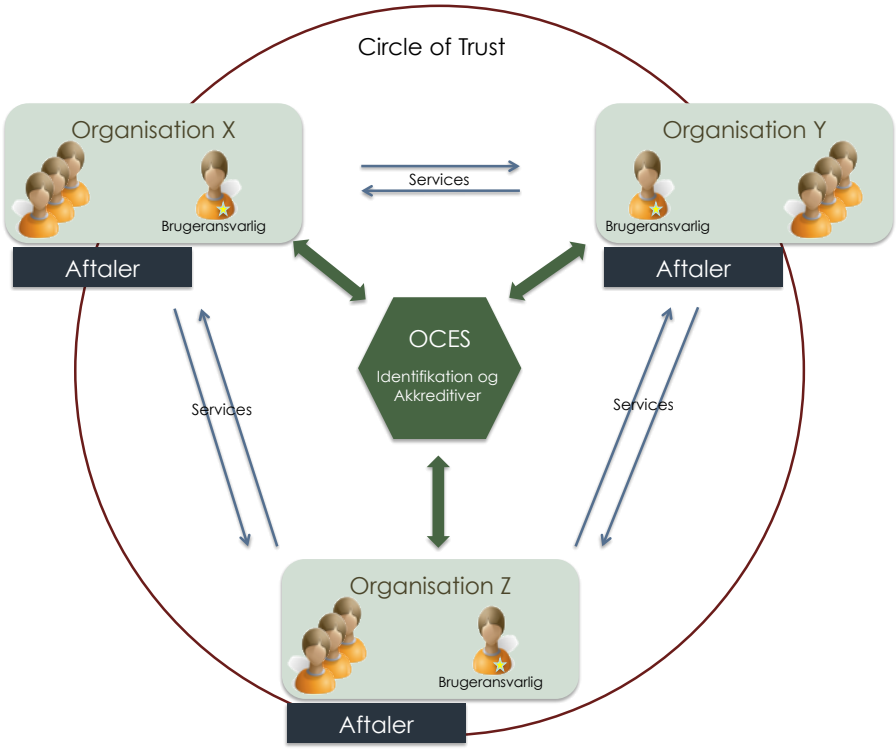
I en aftalebaseret føderation er hver enkelt organisation ansvarlig for begge typer sikkerhed. I nogle situationer, f.eks. som i Danmark, hvor der findes en fælles national løsning med digitale certifikater (OCES), er det dog muligt at uddelegere noget af dette ansvar. OCES operatøren varetager såvel *Identity Proofing* og *Credential Management.* I praksis delegerer OCES operatøren dog *Identity Proofing* ansvaret til udvalgte bemyndigede personer (*Local Registration Authority*, LRA'er), der typisk er ansat hos føderationsorganisationen, og ansvaret for *Identity Proofing* er således reelt placeret hos føderationsparterne selv (i henhold til krav fastsat i OCES certifikatpolitikker).

En række af de krav, der stilles til parterne i en aftalebaseret føderation, varetages dog af OCES operatøren[11], hvilket betyder, at disse ikke behøves at være opfyldt af øvrige parter i føderationen[12]. Derudover kan parterne minimere behovet for tillid til eksterne parter gennem anvendelse af en fælles IdP/STS frem for hver at have deres egen. En ulempe ved denne type føderation er, at parterne mister valgfrihed i forhold til de opgaver og akkreditiver, der varetages af operatøren – eksempelvis vil regionerne ikke kunne anvende deres egne akkreditiver til brug af nationale tjenester.

I nedenstående Figur 10 illustreres en føderation, hvor tillid til autenticitetssikring sikres gennem de procedurer og teknikker, der er etableret gennem OCES / NemID initiativet.

[11] OCES operatøren er underlagt omfattende revisionskrav, der sikrer at disse dele af LIAF er opfyldt.

[12] Omfanget af ansvaret og arbejdsopgaverne er skitseret i bilag A i [SDSD-AUTH].



Figur 10 - Eksempel på føderation med kontrol af vitale sikkerhedselementer, her eksemplificeret gennem anvendelse af OCES / NemID initiativets processer og teknologier i forhold til sikker autenticitetssikring.

2.7.5.1 Konklusioner vedr. sikkerhedsmodeller på nationalt niveau

Adgang til nationale systemer og tjenester kræver i dag at man autentificerer sig op mod nationale tjenester (NemLogin, SOSI-STS), og at man får udstedt security tokens fra nationale tjenester.

Sundhedsvæsenet er ved at bevæge hen mod en føderation, hvor der haves tillid til fællesoffentlige løsninger som NemLogin, om end der endnu ikke er udarbejdet aftaler, der præciserer de krav der skal stilles til parterne i føderationen. Dette bør ske ud fra Libertys Identity Assurance Framework (LIAF) måske tilpasset til danske forhold.

En sådan profilering (med dens formulering af krav til de organisationer, der ønsker at indgå i en føderation) vil være et godt udgangspunkt for at drøfte fordele og ulemper ved at skabe en aftale-baseret føderation alene med parter indenfor sundhedsområdet. Hermed kan der fremover skabes lokale frihedsgrader på et fortsat højt og ensartet sikkerhedsniveau.

Liberty har en ”hård” tilgang til, hvorledes det krævede niveau findes, idet en sikkerhedsanalyse entydigt med LIAF-tilgangen kan afgøre niveauet. Dette er nødvendigt, da standarden vedrører kommunikation over åbne netværk.

I vejledningen fra IT- og Telestyrelsen lægges op til en blødere tolkning:

> […] det nødvendige niveau af autenticitetssikring skal ses i sammenhæng med øvrige sikkerhedsforanstaltninger i et system. Eksempelvis kan en given forretningsproces, der er vurderet til at skulle anvende niveau 3 akkreditiver, sænke it-systemets behov til niveau 2

akkreditiver ved at foretage andre afbødende aktiviteter som fx yderligere systemkontroller, yderligere autenticitetssikring foreholdt kritiske grene af forretningsprocessen etc. [ITST]

I praksis betyder det, at man ved passende tiltag kan opnå et højere niveau af autentifikationssikkerhed, end sikkerhedsforanstaltningerne formelt berettiger til, hvis man indfører passende foranstaltninger, eksempelvis overordnet sikring af transportlaget (alternativt til et åbent netværk).

Den samme tolkning har været gældende på sundhedsområdet, hvor den stringente analyse ville resultere i et behov for autentifikationsniveau 4, idet der med det fælles medicinkort er adgang til stærkt personlige data, og det er muligt at forårsage personskade ved ondsindet brug af systemet. Det er imidlertid besluttet at lægge sig på niveau 3 (baseret på Digital Signatur), hvilket principielt er for lavt, men pga. de omkringliggende sikkerhedsforanstaltninger (primært at transportlaget er sikret og aftalebaseret) er niveau 3 blevet vurderet til at være tilstrækkeligt.

3 Forretningsarkitektur

Nærværende kapitel beskriver informationssikkerhed ud fra et forretningsmæssigt synspunkt. Kapitlet lægger ud med at beskrive centrale begreber, der vedrører informationssikkerhed, og der opstilles en terminologisk begrebsmodel, der viser udvalgte sammenhænge mellem begreberne. Herefter identificeres væsentlige aktører og processer inden for området og der beskrives en række funktioner/services.

3.1 Begreber

3.1.1 Hvad er en referencemodel?

En referencemodel beskriver bl.a. begreber ved hjælp af deres karakteristiske træk og deres indbyrdes relationer. Referencemodellen beskriver et domæne på et passende abstraktionsniveau og er uafhængig af konkrete implementeringer; målet er at skabe en fælles forståelse af domænets begreber løsrevet fra konkrete systemer og leverandører.

Med en referencemodel opnår man:

- Sikkerhed for at systemer og implementeringer på baggrund af konsistente datamodeller forankres i en bagvedliggende fælles begrebsforståelse
- Ressourcebesparelse og kvalitetsforbedring ved at undgå fejl og uklarheder under udvikling af it-systemer
- Dialogforbedring mellem fagekspert og it-udvikler

I litteraturen benyttes termerne ”begrebssystem”, begrebsmodel” eller ”ontologi” ofte i stedet for ’referencemodel’. I nærværende dokument anvendes termen ”referencemodel”.

3.1.2 Kilder og afgrænsning

Der eksisterer en række kilder, der på forskellig vis beskæftiger sig med referencemodeller eller centrale begreber inden for informationssikkerhed. Nedenfor gennemgås et udvalg, der er fundet relevant i forhold til nærværende arbejde.

Begrebsarbejde i regi af det Nationale Begrebsråd for Sundhedsvæsnet (NBS)

NBS har i 2006 udarbejdet et terminologisk begrebssystem for informationssikkerhed [NBS 06]. Den er i denne sammenhæng relevant, idet den udgør et samlet bud på en referencemodel for informationssikkerhed.

Rapport – analyseprojekt vedr. informationssikkerhed

Sammenhængende Digital Sundhed i Danmark har i [SDSD-Analyserapport] fastlagt nogle af de helt centrale begreber i forhold til relevant lovgivning. Udgangspunktet for projektet var de områder i sundhedsloven, hvor der er behov for at analysere og specificere kravene til organisatoriske og tekniske løsninger, inden der kan igangsættes konkrete projekter.

Rapporten omfatter derfor kun centrale begreber i forhold til dette formål, herunder ”behandlingsrelation”, ”samtykke”, ”nødvendighed”, ”værdispring”, men udelader en række andre relevante begreber.

SDSD’s arbejde vedr. sikkerhedsarkitektur

Sammenhængende Digital Sundhed i Danmark har i [Sikkerhedsarkitektur] udarbejdet et udkast til en arkitektur for informationssikkerhed, baseret på OIO-EA-reolen[13]. Dette arbejde fastlægger ligeledes nogle centrale begreber og tilhørende services. Arbejdet kan dog ikke betragtes som indeholdende en egentlig referencemodel, idet der mangler en egentlig definition af begreber samt fastlæggelse af relationer mellem disse.

Vejledning om risikovurdering, IT- og Telestyrelsen, oktober 2007

Dette arbejde fokuserer på en del af en samlet referencemodel, nemlig den del der beskriver sikkerhedsrisici og vurdering af disse. Om end et af formålene med vejledningen er at introducere væsentlige begreber og terminologi indenfor risikovurdering indeholder vejledningen ikke egentlige definitioner og terminologiske begrebsmodeller.

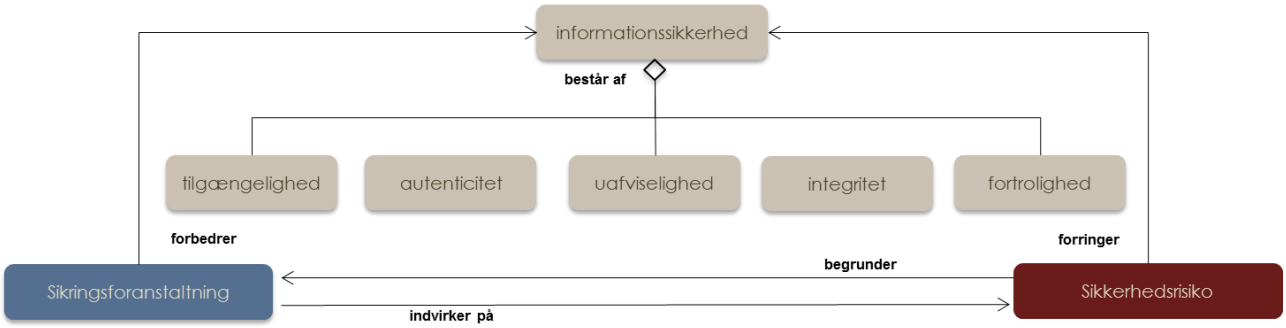
3.1.3 Princip for afgrænsning

Det har ikke været scopet for nærværende arbejde at skabe en referencemodel for informationssikkerhed "fra bunden". Modellen baseres på eksisterende arbejde i det omfang det har været muligt, og kun relevante dele er uddraget med henblik på at tjene referencearkitekturens formål.

Med andre ord fastlægges her kun betydningen af centrale begreber, som er relevante for formålet med nærværende referencearkitektur. I det omfang det har været nødvendigt, har modellen udbygget eller tilrettet eksisterende modeller. Det skal bemærkes at nærværende arbejde skal betragtes som begyndelsen på en proces frem mod en ajourført fælles referencemodel for informationssikkerhed.

3.1.4 Referencemodellen for informationssikkerhed

I nedenstående figur er referencemodellen gengivet på "øverste niveau".



Figur 11: Begrebsmodel for informationssikkerhed på øverste niveau

Der anvendes følgende signatur for beskrivelse af relationer mellem begreber:

- Specialiseringer (typerelationer/generiske relationer; linjer der begynder med en trekant/paraply) har på diagrammerne tilknyttet det aspekt eller træk, der adskiller de aktuelle typer af det pågældende overbegreb.
- Dekompositioner (del-helheds-relationer; linjer der begynder med en rombe) er på diagrammerne betegnet med et navn, der beskriver arten af dekomposition. Arten "består af", angiver typisk funktionelt adskilte dele af en helhed.

[13] Se http://ea.oio.dk/rammeverk

- Associative relationer (linjer med pil) har et navn på relationen. Navnet er placeret i den ende, hvorfra relationen skal "læses".

Ovenstående figur afspejler et syn på informationssikkerhed, hvor sikringsforanstaltninger modsvarer konkrete sikkerhedsrisici. Omkostningerne ved at etablere sikringsforanstaltninger skal m.a.o. opveje reduktionen af sikkerhedsrisiko.

Kigger vi på, hvad en sikringsforanstaltning er, så kan den karakteriseres ud fra bl.a. formål og middel. Bemærk, at samme sikringsforanstaltning i dette arbejde kan dække flere formål.

Figur 12 – Begrebet sikringsforanstaltning med underbegreber

En sikringsforanstaltning kan også have effekt på flere af de ovenfor beskrevne effektområder (tilgængelighed, autenticitet, uafviselighed, integritet, fortrolighed) – dette fremgår dog ikke af figuren.

Distinktionen mellem tekniske og organisatoriske sikringsforanstaltninger er meget central. Informationssikkerheden bestemmes af de samlede sikringsforanstaltninger og de samlede sikkerhedsrisici – herunder kombinationen af tekniske- og organisatoriske sikringsforanstaltninger. Man kan således ikke udelade tekniske sikringsforanstaltninger uden at skabe "huller" i informationssikkerheden, men man kan vælge at kompensere med organisatoriske sikringsforanstaltninger. Nogle gange kan det være mest rationelt at vælge tekniske foranstaltninger, andre gange vil det være mest rationelt at skabe organisatoriske.

Man kan næppe forestille sig sikkerhed alene baseret på tekniske sikringsforanstaltninger. Tilliden til, at et pas er gyldig legitimation, baseres ikke alene på, hvor svært passet er at forfalske, men også på, at der er tillid til de procedurer, der er i forbindelse med udstedelse af et pas (at man har kunnet fastslå personers identitet).

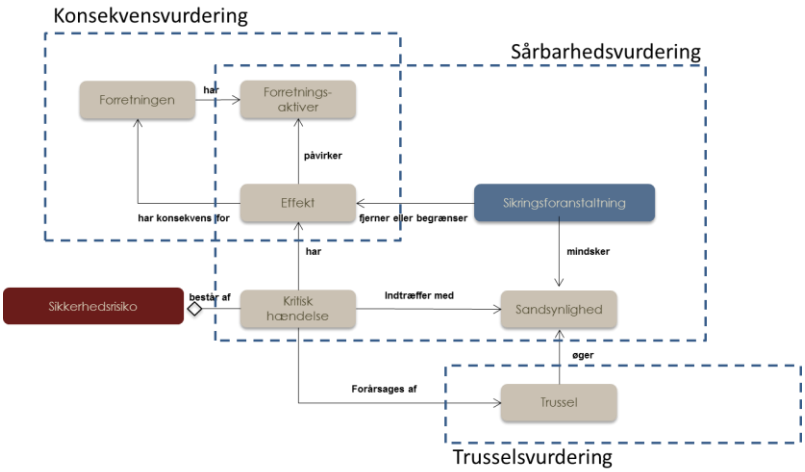
Af organisatoriske sikringsforanstaltninger kan bl.a. nævnes:

- Udarbejdelse af forskrifter
  - Politikker og retningslinjer (ledelse fastlægger)
  - Erklæringer (ledelse afgiver)
  - Aftaler og aftalevilkår (ledelse indgår)
- Beskrivelse og implementering af organisation og processer
  - Herunder beskrivelse af processer for risikoanalyse og -styring
  - Undervisning
- Kontroller
  - Herunder revision

Disse begreber er endnu ikke indarbejdet i modellen.

Vi har indtil nu været fokuseret på den ene side af informationssikkerhed (sikringsforanstaltningerne). Skal man vurdere den anden side (sikkerhedsrisici) kan man tage udgangspunkt i IT- og Telestyrelsens vejledning om risikovurdering [risikovurdering]. Denne baseres på international "best practice" (den såkaldte OCTAVE-metode udviklet ved CERT Coordination Center ved Carnegie Mellon Universitetet's Software Engineering Institute i Pittsburgh, USA[14]).

Vejledningen beskriver risikovurdering som bestående af konsekvensvurdering, trusselsvurdering og sårbarhedsvurdering. Konsekvensvurderingen er med til at kortlægge, hvad sikkerhedsbrud indenfor de forskellige effektområder (tilgængelighed, autenticitet, uafviselighed, integritet, fortrolighed) betyder for forretningen. Trusselsvurderingen beskriver truslerne i den verden, forretningen virker i. Sårbarhedsvurderingen beskriver, hvordan den konkrete forretning med de forskellige aktiver, bestående af bl.a. informationsaktiver og processer og beskyttende sikringsforanstaltninger kan være sårbar overfor de beskrevne trusler. Sammenhængene mellem disse er illustreret i Figur 13:



Figur 13 – Begreber, som indgår i risikovurdering

Ved trusselsvurderingen anbefales det bl.a. at se på:

- Hvilket effektområde er i spil?
- Hvordan kan truslen ramme aktivet? (Via netværket, fysisk)
- Hvor og hvem kan truslen komme fra? (Indefra, udefra)
- Hvad motivet er? (Forsæt, uagtsomhed, hændeligt)

Begreber vedrørende dette er endnu ikke indarbejdet i modellen.

I næste afsnit afdækkes betydningen af en række begreber som benyttes i gældende lovgivning på sundhedsområdet. Disse vil blive indarbejdet i en samlet terminologisk begrebsmodel i efteråret 2012. En række af begreberne med definition er vedlagt som bilag B.

[14] Se: http://www.cert.org/

3.2 Processer og aktører

Informationssikkerhed har en central placering og er en grundlæggende faktor inden for sundhedsvæsnet. Der er som følge heraf mange forskellige instanser og processer i sundhedsvæsnet, der indeholder elementer af informationssikkerhed. Overordnet set kan processerne kategoriseres i følgende hovedgrupper:

- **Brugerens processer**: med disse menes processer der har brugeren i centrum. Et eksempel er en bruger der får adgang til patientoplysninger via et lokalt fagsystem.
- **Patientens processer**: disse er processer, der har patienten (eller borgeren) i centrum. Et eksempel inden for denne kategori er en patient, der åbner "min log" på sundhed.dk.
- **Administratorens processer**: dette vedrører processer, som håndteres af administrativt personale. Et eksempel inden for denne kategori er en lokal administrationsenhed, der varetager administration af akkreditiver som medarbejdercertifikater.
- **Governance processer**: denne kategori rummer processer til håndhævelse af principperne og politikkerne for informationssikkerhed. Et eksempel på dette er Datatilsynets udtalelser, som skal sikre, at databehandling f.eks. af sundhedsoplysninger følger lovgivningens krav. Men der kan også være tale om teknisk understøttelse af principper, f.eks. teknisk validering af, at der findes en aktuel behandlingsrelation.

Nedenfor listes de vigtigste processer.

3.2.1 Brugerens processer

- Forespørgsel på patientoplysninger (indhentning af informationer)
- Kommunikation med andre parter (videregivelse af informationer)
- Delegering af arbejdsopgaver / arbejdsfunktion

3.2.2 Borgerens/patientens processer

- Borgerens adgang til egne oplysninger
- Borgerens adgang til logoplysninger (MinLog)
- Administration af samtykkeoplysninger
- Administration af fuldmagtsoplysninger

3.2.3 Administratorernes processer

- Administration af akkreditiver
- Administration af ansættelsesforhold og arbejdsfunktion
- Administration af systemspecifikke rettigheder
- Administration af organisationsoplysninger

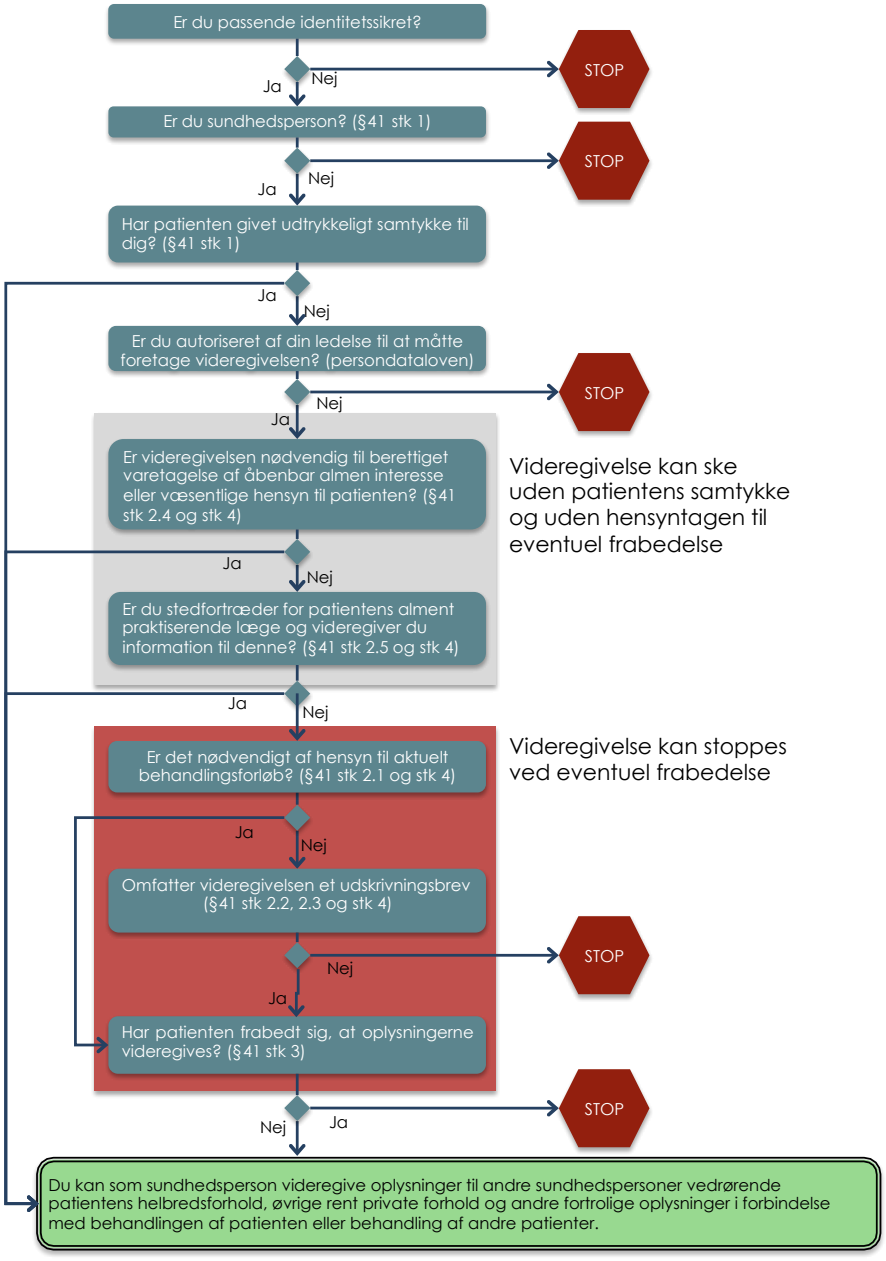
3.2.4 Governance processer

- Styring af adgang til patientoplysninger (adgangskontrol)
- Logning af adgang til patientoplysninger
- Opfølgning på adgang til patientoplysninger

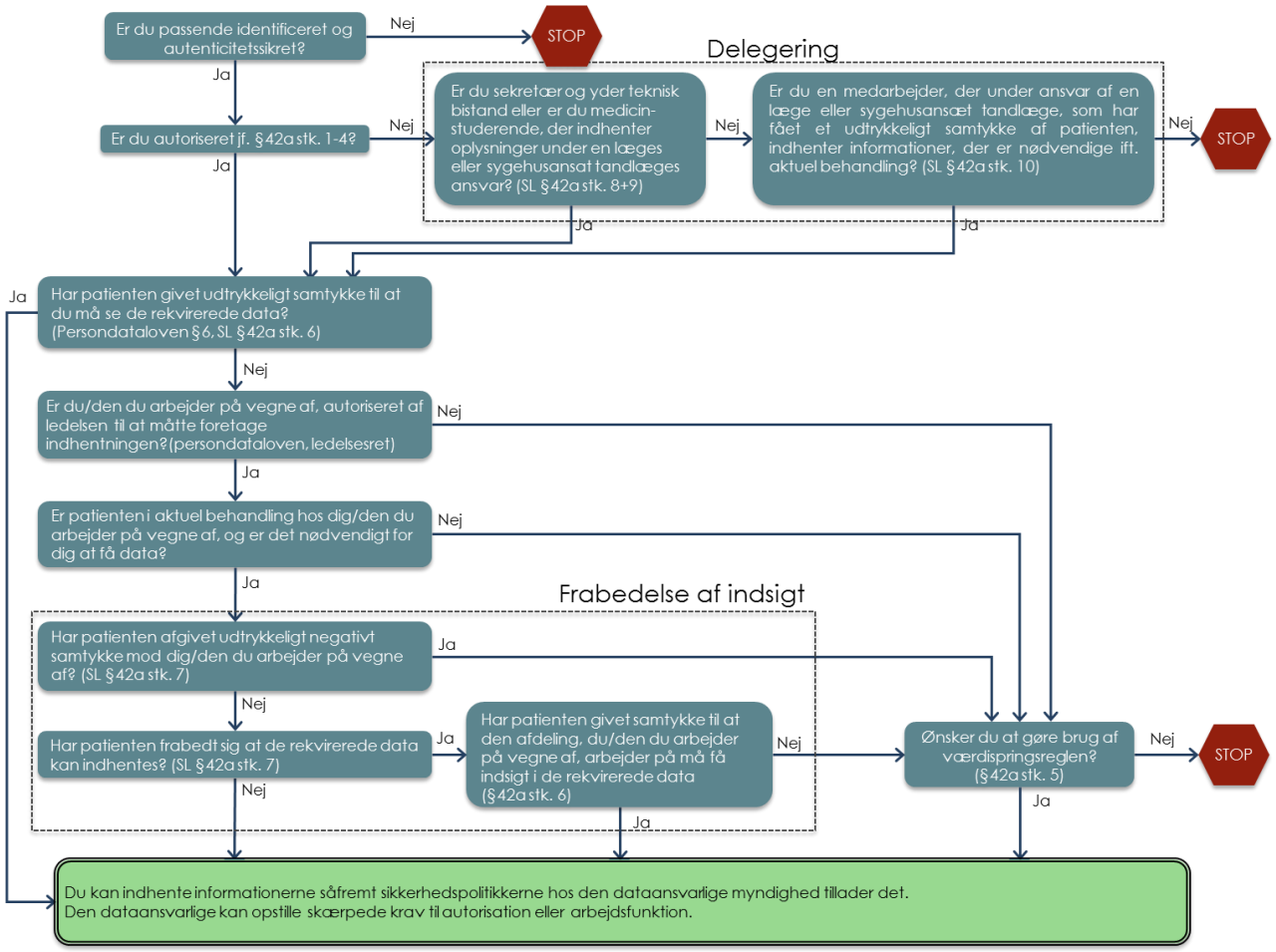
3.3 Lovgivning og sikkerhed i forbindelse med processer

I forbindelse med flere af processerne skal det afgøres om der må indhentes eller videregives oplysninger. Lovgrundlaget er komplekst på dette område, idet forskellige regler fra forskellige love og bekendtgørelser skal efterleves. Det vedrører bl.a. sundhedslovens §41 om videregivelse af informationer og §42a om indhentning af informationer. Disse to paragraffer er illustreret i

beslutningsgrafer nedenfor, hvor også andre dele af lovgivningen (persondataloven, autorisationsloven mv.) og ledelsesretten er medtaget. Graferne viser, at det at afgøre om en person må videregive eller (i særdeleshed) få adgang til informationer, er komplekst, og derfor let kan give anledning til fejl og forskelligartet implementering. Nedenstående grafer kan benyttes som vejledning for fremtidig implementering.



Figur 14 - Beslutningsgraf for informationssikkerhed vedrørende sundhedspersoners videregivelse af informationer i sundhedsvæsenet.



Figur 15 - Beslutningsdiagram for informationssikkerhed i relation til sundhedspersoners indhentning af informationer i sundhedsvæsenet.

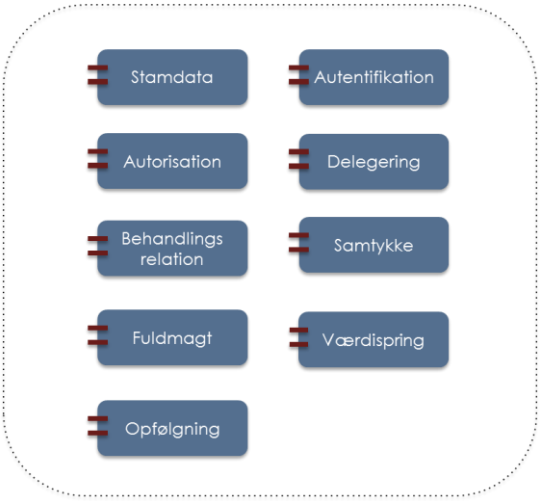
Fokus i dette afsnit har været det samspil mellem de forskellige love og bestemmelser, der er nødvendigt at iagttage, når sikkerhedsmæssige krav til processer skal fastlægges. Nedenfor beskrives de enkelte sikkerhedsmæssige aspekter mere indgående (men med begrænset redegørelse for samspillet). For mere information om de lovgivningsmæssige aspekter henvises i øvrigt til analyserapporten om informationssikkerhed, der blev udarbejdet af en tværgående arbejdsgruppe i 2009 [SDSD-Analyserapport].

3.4 Centrale komponenter i referencearkitekturen

3.4.1 Overblik

Med udgangspunkt i referencemodellen og de beskrevne processer, er det muligt at udpege de centrale komponenter, der skal indgå i sikkerhedsarkitekturen.

Der er ikke tale om en udtømmende liste af komponenter. I takt med, at det bliver teknisk, ressourcemæssigt og organisatorisk muligt, vil der ske en videreudvikling af modellen og der vil blive udviklet flere komponenter, som kan indgå i sikkerhedsarkitekturen.



Figur 16: Centrale komponenter i referencearkitekturen

Nedenfor beskrives overvejelser vedr. det centrale indhold af disse komponenter. Efterfølgende præciseres hvilke operationer det er nødvendig at komponenterne skal realisere for at kunne understøtte de beskrevne processer.

3.4.2 De enkelte komponenter

3.4.2.1 Stamdata

3.4.2.1.1 Lovgrundlag

I forhold til informationssikkerhed er det især oplysninger om (herunder entydig identifikation af) personer og organisationer, der er relevante. Der kan imidlertid også være andre oplysninger, der kan benyttes i forbindelse med håndhævelse af sikkerheden. Eksempelvis kan oplysninger knyttet til medicinske medikamenter være med til at sikre, at forsøgsmedicin kun ordineres af personer, der er godkendt hertil af Sundhedsstyrelsen. Dette afsnit afgrænses imidlertid til at beskrive personstamdata og organisationsstamdata.

Hvad angår personstamdata, da indeholder CPR-registret oplysninger om personer, som 1) folkeregistreres her i landet på grund af fødsel eller tilflytning fra udlandet, 2) inddrages under ATP, 3) ifølge skattemyndighederne skal have et sådant i forbindelse med skattesagsbehandling her i landet[15]. Det følger heraf, at alle personer med bopæl eller fast ophold i landet, samt udlændinge der ansættes af en dansk arbejdsgiver, vil have et personnummer og være registreret i CPR-registret.

Oplysningerne i CPR-registret må i henhold til CPR-loven videregives til offentlige myndigheder efter reglerne i lov om behandling af personoplysninger (persondataloven), og en del af disse kan også videregives til private efter reglerne i CPR-loven og persondataloven. Offentlige myndigheder må ikke videregive beskyttede navne og adresser til private.

M.h.t selve personnummeret (cpr-nummeret) kan offentlige myndigheder behandle personnummeroplysninger med henblik på en entydig identifikation eller som journalnummer (Persondatalovens § 11 stk. 1). Myndigheden har ifølge CPR-lovens §54 pligt til at sikre, at

[15] J.f. Bekendtgørelse af lov om Det Centrale Personregister (CPR loven), LBK nr. 878 af 14/09/2009.

personnumre ikke kommer uvedkommende i hænde (må eksempelvis ikke påføres uden på breve, i rudekuverter eller ved andre forsendelser). Private må behandle oplysninger om personnummer, når videregivelsen er af afgørende betydning for at sikre en entydig identifikation af den registrerede eller videregivelsen kræves af en offentlig myndighed (Persondatalovens § 11 stk. 3).

I forhold til autoriserede sundhedspersoner vil oplysninger om autorisationsstatus m.m. fremgå af Sundhedsstyrelsens autorisationsregister. Autorisation af sundhedspersoner sker i henhold til lov om autorisation af sundhedspersoner og om sundhedsfaglig virksomhed[16].

Den sundhedsfaglige autorisation må ikke sammenblandes med den informationssikkerhedsmæssige autorisation af brugere. Det er kun ganske få rettigheder i it-systemer, der kan tildeles alene på baggrund af en sundhedsfaglig autorisation (ordination af medicin, underskrivelse af dødsattest etc.). Hovedparten af rettigheder i it-systemer tildeles på baggrund af et ansættelsesforhold og varetagelse af en given arbejdsmæssig funktion (se senere afsnit vedr. autorisation). Omvendt kan fratagelse eller indskrænkning af en sundhedsfaglig autorisation betyde, at man mister retten til at udøve en bestemt sundhedsfaglig virksomhed, hvorfor dette betyder, at ens systemmæssige rettigheder skal begrænses.

3.4.2.1.2 Operationalisering

Der er behov for at kunne identificere personer entydigt på tværs af parterne. Det gælder såvel sundhedspersoner som borgere. CPR-numre (og nationalt entydige erstatnings-cpr-numre) vil kunne dække behovet. Der er ikke andre systemer, der i dag kan sikre entydig identifikation og som rummer alle de identiteter, som der er behov for. Stamoplysninger om de enkelte personer hentes fra CPR-registret / nationalt erstatnings-CPR-nummer system.

Der er endvidere behov for at kunne identificere organisatoriske enheder entydigt på tværs af parter. Hertil benyttes SOR-koder (SOR = Sundhedsvæsentes Organisations Register). SOR er det eneste organisationsregister på sundhedsområdet, der kan dække alle typer organisatoriske enheder. Stamoplysninger om de enkelte organisatoriske enheder hentes fra SOR.

3.4.2.2 Autentifikation

3.4.2.2.1 Lovgrundlag

Der er ikke noget formelt lovgrundlag, der vedrører autentifikation.

3.4.2.2.2 Operationalisering

IT- og Telestyrelsen har udgivet en generel vejledning om autentifikationssikring [ITST], hvori "sikkerhedsniveauer" og praktiske forhold omkring implementering af autentifikation beskrives. Sikkerhedsniveauerne er også baseret på niveauerne fra NIST.

[16] Bekendtgørelse af lov om autorisation af sundhedspersoner og om sundhedsfaglig virksomhed (LBK nr 877 af 04/08/2011), se: https://www.retsinformation.dk/Forms/R0710.aspx?id=138178

Tabel 1 – Maksimale størrelser af risici for hvert sikkerhedsniveau

Risiko i forhold til sikkerhedsniveau				
Kategorier af konsekvenser ved fejl i forbindelse med autenticitetssikring	1	2	3	4
Ulempe, kval eller tab af anseelse	Lille	Moderat	Moderat	Stor
Økonomisk tab eller ansvarspådragelse	Lille	Moderat	Moderat	Stor
Skade på myndighedsaktiviteter eller andre offentlige interesser	-	Lille	Moderat	Stor
Ikke-autoriseret frigivelse af sensitiv information	-	Lille	Moderat	Stor
Fysisk personskade	-	-	Lille	Moderat Stor
Mulighed for at begå/modvirke opklaring af ulovligheder	-	Lille	Moderat	Stor

Tegnet "-" angiver *ikke tilstrækkeligt sikkerhedsniveau til hændelser med den givne konsekvens*

Der er brug for mekanismer, der kan fastslå brugeres identitet. Såfremt der er behov for at kommunikere oplysninger om styrken af evidens for brugerens identitet, benytte skalaen 1 – 4, som angivet af It- og Telestyrelsen.

3.4.2.3 Autorisation

3.4.2.3.1 Lovgrundlag

I persondatalovens § 41, stk. 3 er det anført, at der skal træffes de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod at oplysninger kommer til uvedkommendes kendskab. I "bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning"[17], fastsættes i §11, at det kun er de personer, som autoriseres hertil, der må have adgang til de personoplysninger, der behandles. Endvidere fastsættes i §11, stk. 2, at der kun må autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for. I vejledningen til bekendtgørelsen forudsættes, at der fastlægges en formel autorisationsprocedure og at der heri vil indgå en forudgående vurdering af, hvad den enkelte bruger har behov for at være autoriseret til.

3.4.2.3.2 Operationalisering

I dag foregår lokal brugeradministration og tildeling af rettigheder i lokale systemer typisk af de samme personer. Brugeradministration kræver således både kendskab til brugernes arbejdsfunktioner og til brugen af lokale systemer (herunder hvilke rettigheder der skal til for at anvende de forskellige systemfunktioner).

Denne referencearkitektur foreslår, at der sker en opdeling, så lokale administratorer kun skal have kendskab til brugernes arbejdsfunktioner, mens systemejerne for de nationale løsninger skal have indgående kendskab til disse løsninger og deres rettighedsmodel.

[17] Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (BEK nr 528 af 15/06/2000), se: https://www.retsinformation.dk/forms/R0710.aspx?id=842

Ved at fastlægge en national standard for arbejdsfunktioner, vil det være de lokale brugeradministratorers rolle at registrere hvilke arbejdsfunktioner de enkelte brugere bestrider. Det er herefter op til systemadministratorerne bag de nationale løsninger at fastlægge, hvilke konkrete systemrettigheder en bruger med en bestemt arbejdsfunktion får tildelt.

Denne form for brugeradministration er mere effektiv end hvis hver systemrettighed skal administreres individuelt på hver bruger, og den er med til at sikre, at brugere med samme arbejdsfunktion (og samme relation til patienten) kan få adgang til de samme oplysninger.

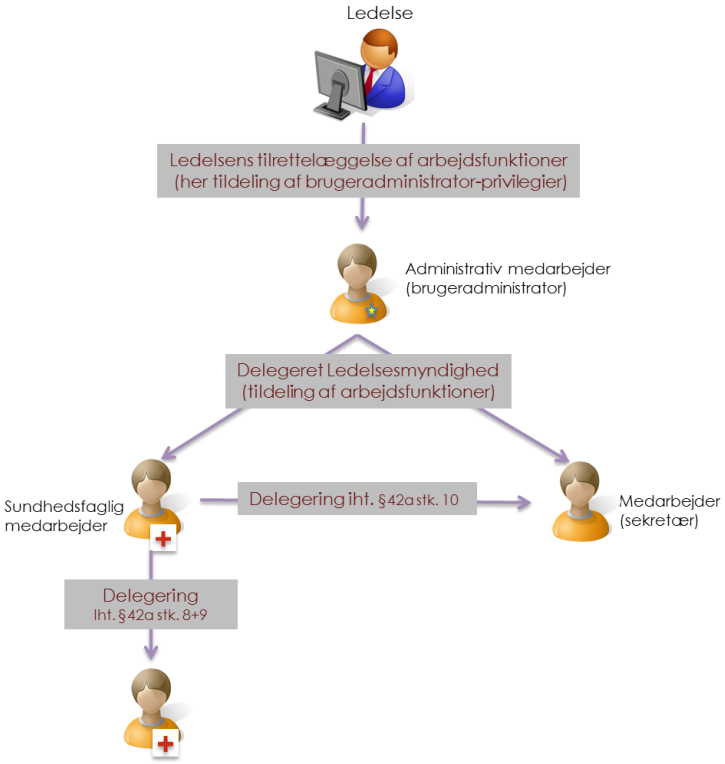
3.4.2.4 Delegering

3.4.2.4.1 Lovgrundlag

Sundhedsfagligt autoriserede personer har mulighed for at delegere udførelsen af en opgave til en anden, jf. Bekendtgørelse om autoriserede sundhedspersoners benyttelse af medhjælp[18]. Ved udførelse af en opgave på vegne af en anden sundhedsperson kan det være nødvendigt, at medhjælpen får udvidede rettigheder til databehandling for at kunne udføre opgaven. Dette kan ske i medfør af sundhedslovens §42a, der indeholder særlige regler om benyttelse af medhjælp ved informationsindsamling.

3.4.2.4.2 Operationalisering

Nedenstående figur illustrerer delegeringssituationerne:



Figur 17 – Delegering

[18] https://www.retsinformation.dk/Forms/R0710.aspx?id=129042

Det skal sikres, at der ikke kan delegeres arbejdsopgaver / arbejdsfunktioner, som den delegerende person ikke har (opnået gennem autorisation/brugeradministration). Ved ændring i ansættelsesforhold (eksempelvis ved ophør af dette eller i ændring af arbejdsfunktioner knyttet til ansættelsesforholdet), skal det derfor checkes, om der er arbejdsfunktioner der er delegeret til andre, som skal fjernes.

I forbindelse med fastlæggelse af nationalt standardiserede arbejdsfunktioner, bør det tydeliggøres hvilke af disse der kan delegeres til andre, og hvilke der ikke kan. Disse oplysninger bør registreres i Identity Management systemer, men selve delegeringen skal kunne foretages af den enkelte sundhedsperson gennem sit fagsystem.

3.4.2.5 Behandlingsrelation

3.4.2.5.1 Lovgrundlag

Offentlige og private dataansvarlige skal – under ansvar overfor Datatilsynet – træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at digitale oplysninger hændeligt, uagtsomt eller forsætligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven, jf. persondatalovens §41, stk. 3.

Specifikt for sundhedsfaglige offentlige registre og elektroniske patientjournaler gælder det, at den, der indhenter oplysninger, skal være en sundhedsperson, der deltager i patientbehandling. Det kræves eksplicit, at der findes en aktuel behandlingsrelation imellem patienten og vedkommende sundhedsperson[19].

3.4.2.5.2 Operationalisering

Elektroniske registreringer i forskellige systemer og registre, kan bruges til at udtale sig om evidensen for at der eksisterer en behandlingsrelation. Hvis eksempelvis et sygehus har henvist til behandling ved privat praktiserende speciallæge, og en sådan speciallæge har hentet den pågældende henvisning (kan verificeres ud fra registreringer i henvisningshotellet), da er der høj evidens for, at den privat praktiserende speciallæge har den pågældende patient i behandling.

Denne referencearkitektur foreslår en fælles skala for, hvor stærk evidensen er ud fra de verificeringer af oplysninger, der kan gøres i forskellige registre.

Nedenstående skala beskriver "styrken" af evidens for relationerne, hvor "A+" aktuelt er den kategori, der beskriver relationer med stærkest evidens for en aktuel behandlingsrelation.

Kategori	Betydning af kategorisering	Anbefalet tolkning

[19] http://www.ft.dk/samling/20101/lovforslag/l171/bilag/7/1001147/index.htm, betænkning over forslag til lov om ændring af sundhedsloven, samt sundhedslovens §41-42a.

Kategori	Betydning af kategorisering	Anbefalet tolkning
A+	”Direkte behandlingsrelation”. Eksplicit relation (f.eks. henvisning) mellem navngiven behandler og navngiven patient	Behandlingsrelationer i denne kategori er for tiden de bedst dokumenterede, og det anbefales derfor at betragte kategori A+ relationer som værende verificerede.
A	”Samme tid, samme behandlingssted” Patient og Behandler var på samme behandlingssted på samme tid	Det anbefales at betragte kategori A relationer som værende verificerede og kræver ikke yderligere tiltag.
B	”Generel behandlingsrelation” Generel behandlingsrelation, f.eks. at patienten har udpeget en læge som ”egen læge”	Med det nuværende datagrundlag anbefales det at lade opfølgningen pågå i 90 dage med en forventning om at opnår kategori ”A” eller bedre.
C	”Historisk betinget behandlingsrelation” Patient og Behandler har været i kontakt tidligere	Med det nuværende datagrundlag anbefales det at lade opfølgningen pågå i 90 dage med en forventning om at opnår kategori ”A” eller bedre.
D	”Kan ikke afklares pt.”	Med det nuværende datagrundlag anbefales det at lade opfølgningen pågå i 90 dage med en forventning om at opnår kategori ”A” eller bedre.
E	”Kan ikke afklares” Ingen evidens hverken nu eller senere	Behandlingsrelationer af denne kategori er ikke verificerede, og kan heller ikke blive senere.

Som det fremgår af ovenstående, kan der være situationer, hvor behandlingsrelation ikke nødvendigvis kan verificeres teknisk. Dette kan være situationer, hvor der ikke digitalt registreres tilstrækkeligt med oplysninger om det pågældende behandlingsforløb (måske bl.a. grundet i at kommunikation og registreringer endnu ikke er digitaliseret), som muliggør verifikation.

Tilsvarende er der situationer, hvor man ikke kan afgøre samtykke på det tidspunkt hvor oplysningerne efterspørges, fordi der ikke på dette tidspunkt haves registreringer, der kan være med til at afgøre evidensen for en behandlingsrelation – men hvor senere registreringer kan give evidens for at der var en behandlingsrelation.

Lægevagten kan eksempelvis være den første kontakt med en patient. Med mindre man automatisk kan opsamle oplysninger om, hvilken telefon der bliver ringet fra og med sikkerhed kan knytte dette telefonnummer til den person som henvendelsen vedrører, da er der ikke registreringer, der kan give evidens for at en given sundhedsperson ved lægevagten har lov til at hente oplysninger der vedrører en bestemt borger. På et senere tidspunkt afregnes lægevagtens ydelser imidlertid med regionerne, hvorfor det på baggrund af den elektroniske afregning kan verificeres, at lægevagten rent faktisk har leveret ydelser til den pågældende patient.

Ved etableringen af nye registre eller ved højnelse af datakvalitet i eksisterende registre bør det overvejes, om disse nye registreringer kan medvirke til at skabe stærkere evidens for behandlingsrelation (m.a.o. om evidens der før kunne verificeres med styrke E nu kan verificeres med styrke D, eller om evidens der før kunne verificeres med styrke B, C eller D måske nu kan verfificeres med styrke A eller A+). J.f. også princippet om, at kvaliteten af de anvendte sikringsforanstaltninger løbende skal forbedres (T3).

Da evidensen for en behandlingsrelation i nogle situationer først kan etableres senere, kan man måske få den tanke, at et check af behandlingsrelation ikke kan bruges til at begrænse adgang til oplysninger (i forbindelse med adgangskontrol). Dette er imidlertid ikke rigtigt – svag eller manglende evidens i forbindelse med adgangskontrol bør i nogle tilfælde resultere i skærpet adgangskontrol til en service.

Et eksempel er den praktiserende læge, der ønsker adgang til en borgers medicinkort i den fælles medicinkort (FMK) løsning. Hvis den pågældende læge er borgerens ”egen læge”, vil der i langt de fleste tilfælde være en opdateret og relativ præcis registrering om dette i sygesikringsregistret. Hvis BRS derfor ikke returnerer med en klasse B relation (”generel relation”) bør det få FMK til at skærpe kontrollen i forbindelse med adgangen, f.eks. ved at gå i dialog med brugeren. Årsagen til en manglende ”generel relation” kan f.eks. være:

- Lægen har uforvarende indtastet forkert CPR nummer og er (ubevidst) ved at tage ”ulovlig” adgang til en tilfældig borgers medicinkort
- Registrering af ”Sikrede” relationen er forsinket
- Lægen er vikar hos et lægehus
- Lægen handler forsætligt og er reelt ved at tage adgang til en (kendt?) persons medicinkort

En simpel dialog med brugeren, hvor FMK (eller systemet, der bruger FMK) informerer lægen om, at vedkommende tilsyneladende ikke er borgerens ”egen læge” eventuelt kombineret med et forslag om at kontrollere CPR nummeret, vil kunne forhindre ”ulovlig” adgang til medicinkortet.

3.4.2.6 Samtykke

3.4.2.6.1 Lovgrundlag

Samtykke i relation til informationsbehandling er generelt defineret i persondatalovens § 3, nr. 8:

> *"8) Den registreredes samtykke: Enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling."*

”Behandling” er defineret i samme paragraf nr. 2, hvor der står:

> *”2) Enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for.”*

Dette dokument omhandler alene elektronisk behandling af data hørende til en identificeret eller identificerbar fysisk person. Elektronisk behandling inkluderer i denne sammenhæng både indhentning og videregivelse af digital information.

I persondatalovens § 6 fastsættes det generelt, at behandling af persondata kun må finde sted med personens udtrykkelige samtykke. Dog fastsætter § 7, stk. 5, at dette ikke gælder for informationer nødvendige for

> *"... forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling, eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt."*

Dermed er det reelt Sundhedsloven, der fastlægger de væsentligste forhold omkring sundhedspersoners indhentning og videregivelse af helbreds- og persondata her i landet.

Sundhedsloven opererer såvel med borgerens samtykke til videregivelse af oplysninger i behandlingsøjemed (§41) og til andre formål end behandling (§43) samt borgerens ret til at frabede sig videregivelse (§41) eller indhentning af oplysninger (§42a).

I relation til elektronisk indhentning af patientoplysninger skal patienten være orienteret om sin ret til at frabede sig indhentning, men der er ikke krav om, at man ved den konkrete indhentning skal udbede sig patientens samtykke. I bemærkningerne til loven er det angivet, at denne ret ved nye it-løsninger skal understøttes elektronisk, dvs. at patienten selv eller en sundhedsperson på patientens vegne skal kunne markere, hvilke oplysninger, man frabeder sig indsigt i.

På det kommunale område skal der skelnes mellem opgaver, der løses på grundlag af sundhedsloven og opgaver, der løses på grundlag af serviceloven.

For sundhedsfaglig pleje og behandling gælder sundhedslovens regler om patientens retsstilling (se ovenfor), mens der i forbindelse med opgaver, der er visiteret på grundlag af serviceloven, som hovedregel skal afgives samtykke til videregivelse eller indhentning. Samtykket skal som udgangspunkt være skriftligt og bortfalder senest et år efter, at det er givet.

Håndteringen i kommunerne kompliceres yderligere ved, at samtykke afgivet henhold til sundhedsloven gælder for det aktuelle forløb, mens samtykke afgivet i henhold til serviceloven gælder for det aktuelle forhold (sag), f.eks. afgørelsen om, hvilke ydelser, en borger har ansøgt om. I flere kommuner har man fortolket reglerne således, at der skal indhentes samtykke, hver gang det drejer sig om et nyt sundhedsproblem, hvilket både medfører, at borgerne skal spørges, ofte med korte intervaller, og med en del registreringsarbejde til følge, idet der er krav om dokumentation af afgivet samtykke.

I dag kan der med hjemmel i lovgivningen sendes adviser mellem sygehuse og kommuner i forbindelse med indlæggelse og udskrivning af borgere, der har en relation til hjemmeplejen. I forbindelse med udarbejdelse af sundhedsaftalerne mellem regioner og kommuner er der ønske om at forbedre kommunikationen og dermed patientens forløb, bl.a. ved at udveksle flere informationer om borgerne end dem, der fremgår af advisen. Dette er et grænseområde, hvor de to lovgivninger på området kan give problemer, fordi der i den ene sektor anvendes positivt samtykke både ved videregivelse og elektronisk indhentning, mens elektronisk indhentning i den anden sektorbaserer sig på patientens ret til at frabede sig indhentningen.

Generelt er der behov for at klarlægge de arbejdsprocesser, hvor informationer indhentes eller videregives til andre sundhedspersoner, for at kunne tydeliggøre reglerne for indhentning af samtykke.

I forhold til elektronisk adgang til sundhedsrelaterede informationer fra udlandet viser de første analyser, at det kræver borgerens udtrykkelige samtykke, før at der må indhentes. Der er her tale om borgerens samtykke til, at det er muligt at indhente informationer fra udlandet gennem særlige kanaler. Samtykket er ikke møntet på navngivne sundhedspersoner eller udvalgte informationer. Indtil videre er det primært epSOS projektet, der driver international adgang, og nærværende notat inkluderer forslag til en løsning, der dækker Danmarks behov i epSOS projektet.

3.4.2.6.2 Operationalisering

I det følgende omtales to typer af samtykke:

- "**Positivt samtykke**" når borgeren/patienten har givet sit udtrykkelige samtykke til at en sundhedsperson, eller en der arbejder på vegne af denne sundhedsperson, må indhente informationer om borgeren/patienten.
- "**Negativt samtykke**" når borgeren/patienten har frabedt sig, at visse informationer indhentes eller videregives - eller at visse sundhedspersoner indhenter informationer.

Positivt samtykke håndteres i dag på meget forskellig vis i sundhedsvæsenet i dag. Ofte er der tale om manuelle arbejdsgange (f.eks. at man undlader at sende oplysninger elektronisk til andre systemer, hvis ikke man har patientens samtykke hertil) frem for tekniske sikringsforanstaltninger. Dette giver udfordringer, når eksempelvis en epikrise (brev fra sygehus til læge) overføres til et andet system (eksempelvis eJournal), hvorfra andre kan hente oplysningerne. Måske ønsker patienten efter denne overførsel at frabede sig andres adgang til disse oplysninger. Patienten skal enten selv vide, at informationerne ligger her eller vedkommende skal henvende sig til det sygehus som har sendt epikrisen og disse skal kunne markere negativt samtykke i eget og i systemer, som der er videresendt til. Det kræver meget veldefinerede og indarbejdede arbejdsprocesser at sikre, at alle informationer beskyttes.

Det synes ikke særligt borgervenligt, hvis borgeren skal have overblik over i hvilke af sundhedsvæsenets forskelligartede systemer given information befinder sig eller hvis borgeren skal have viden om, hvilken kommunikation en given afdeling har haft med andre parter for at sikre, at personfølsomme oplysninger beskyttes af et negativt samtykke.

Nogle løsninger (Fælles Medicinkort etc.) har selv etableret en borgervendt brugergrænseflade og tillader borgeren selv at administrere "privatmarkeringer". Det er muligt at opgaven med at markere de enkelte informationer er håndterbar i forhold til medicin, men en meget detaljeret markering af samtykkeoplysninger, der knytter sig til enkelt-registreringer er uholdbart som generel model for samtykkehåndtering. Dels vil administrationsopgaven blive uhåndterbar stor for det sundhedspersonale, som er forpligtet til at registrere borgerens samtykker (såfremt de ikke selv kan eller vil gøre det), dels er der stort set ingen af de eksisterende systemer, der kan gøre det i dag (og såfremt man ikke vil afskære sig fra at købe markedsløsninger vil der fremover også være systemer,

der ikke vil kunne håndtere dette). Endelig knytter der sig problematikker til at informationen om at et detaljeret informationselement er hemmeligholdt i sig selv kan være følsom, og der knytter sig problematikker til, at hemmeligholdelsen af del-elementer kan give anledning til fejl i forståelsen af den øvrige information (m.a.o. hvad er konsekvensen ved at skjule delvis information?).

Afgrænsningen af, hvad der samlet kan gives samtykke til (eller som borgere kan frabede sig indhentning eller videregivelse af), skal operere på et højere niveau (man skal m.a.o. kunne sige til og fra i større "klumper" af information) og denne skal være meningsfuld for borgeren. Eksempelvis kan det dreje sig om alle data vedrørende et givet sygdomsforløb, en kontakt med sygehusvæsenet eller et besøg ved en behandler.

Det skal være muligt at angive, at der er oplysninger som borgeren generelt set ikke ønsker andres adgang til (negativt samtykke til alle andre personer). Som udgangspunkt registrerer borgeren eller en sundhedsperson på dennes vegne, hvilke dele, der generelt ikke må ses eller videregives. Hvis der er afgivet et sådant negativt samtykke, skal borgeren selektivt kunne åbne for personer eller organisationer, der må se de beskyttede data (positivt samtykke til bestemt person eller til alle personer, der er tilknyttet en given organisatorisk enhed).

Eksempelvis kan en borger frabede sig, at nogen indhenter oplysninger, der vedrører en tidligere behandling. Hvis vedkommende skal behandles igen for en sygdom, hvor de pågældende informationer er relevante at kende for behandleren eller behandlingsstedet, kan borgeren give sit (positive) samtykke til, at disse får adgang til de oplysninger, der i ellers er beskyttet af et negativt samtykke. Når den pågældende behandling er afsluttet, kan borgeren igen "lukke" for det positive samtykke (der ellers bortfalder efter 1 år).

Hvis en borger har valgt negativt samtykke, der gør at ingen kan få adgang til de udpegede data om borgeren, skal sundhedspersonen gøres opmærksom på dette ved forsøg på at få adgang til de beskyttede data. Sundhedspersonen (eller en anden person på dennes vegne) må derefter henvende sig til borgeren for at afgøre om det er relevant og ønskeligt selektivt at åbne for enkeltpersoner eller organisatoriske enheder i sundhedsvæsenet (udpeget på et passende organisatorisk niveau, f.eks. afdelings- eller yder niveau).

En samtykkeløsning bør også dække den mulighed, at borgeren kan frabede sig, at informationer videregives til eller indhentes af (negativt samtykke) bestemte personer ansat i sundhedsvæsenet (naboer, eks-samlevere, etc.). Derimod giver det ikke så megen mening at kunne give et negativt samtykke til organisationer som man ikke har et personligt forhold til og som i øvrigt er i stadig forandring[20].

Med baggrund i ovenstående, foreslår denne referencearkitektur indholdet af et samtykke fastsat som følgende:

Et samtykke (positivt som negativt) kan beskrives ud fra tre dimensioner:

[20] Omvendt vil et positivt samtykke til en organisatorisk enhed være kortsigtet (indtil behandlingsophør og max. 1 år), hvorfor risikoen ved et positivt samtykke som dækker mere end påtænkt grundet sammenlægning af organisationer er minimal. Organisatorisk opdeling vil ikke udgøre nogen risiko, da der bare vil ske en indskrænkning af, hvad samtykket dækker. Er dette uønsket, kan man afgive nye samtykker.

- **”Hvad”**. Hvilke informationer vedrører samtykket?
- **”Hvem”**. Hvilke personer gives samtykket til?
- **”Hvornår (gyldighed)”**. Fra hvilket tidspunkt gælder samtykket og hvornår udløber det?

Hver af disse dimensioners udfaldsrum er defineret i nedenstående tabel. Som det fremgår, er der ikke tale om uafhængige dimensioner. En værdi i én dimension kan påvirke udfaldsrummet i en anden dimension.

Samtykketype	”Hvad” (udfaldsrum)	”Hvem” (udfaldsrum)	”Hvornår” (udfaldsrum)
Negativt samtykke	”Alt” (dvs. intet må ses)	”Alle” eller ”Bestemt person” (note 1)	Gyldig indtil borgeren selv fjerner det
	”Afgrænsede informationer” (note 2)	”Alle”	Gyldig indtil borgeren selv fjerner det
Positivt Samtykke	”Alt” eller ”Afgrænsede informationer” (note 2)	”Bestemt person” (note 1) eller ”Organisatorisk enhed” (note 3)	Gyldighed er max. 1 år, men borgeren kan selv specificere et mindre gyldighedsinterval.
	epSOS Patient Summary/ePrescriptions	”Udenlandske sundhedspersoner generelt” (note 4)	Gyldighed er max. 1 år, men borgeren kan selv specificere et mindre gyldighedsinterval

Note 1 – Bestemt person

CPR-nummeret er en fælles entydig identifikation af personer med dansk statsborgerskab eller fast tilknytning til det danske arbejdsmarked og er derfor velegnet til at registrere, hvem der gives samtykke til. I tilfælde af, at borgeren beder en sundhedsperson registrere samtykke (positivt eller negativt) til en lokal ansat, vil lokale systemer kunne håndtere registreringen af vedkommendes CPR-nummer uden at borgeren behøver at have kendskab til dette.

Såfremt borgerens selv administrerer samtykkeoplysninger gennem selvbetjeningsløsning tilgængelig via sundhed.dk (eller en sundhedsperson skal administrere et samtykke til en anden sundhedsperson, der ikke kan identificeres via eget system), er det nødvendigt at vise andre oplysninger, der kan hjælpe borgeren til at identificere en sundhedsperson entydigt. Information om autoriserede sundhedspersoner er elektronisk registreret i Sundhedsstyrelsens autorisationsregister. Borgere kan i dag via sundhedsstyrelsens hjemmeside søge efter autoriserede sundhedspersoner i dette register ud fra navn, fødselstidspunkt, faggruppe, speciale, tidspunkt for autorisation, autorisationsstatus (gyldig/ikke gyldig) eller entydigt autorisations-ID. Hvis borgeren på baggrund af søgninger i autorisationsregistret kan finde den pågældende sundhedsperson, kan denne sundhedsperson udpeges med det entydige og offentligt tilgængelige autorisations-ID. En samtykkeadministrationsløsning kan omsætte dette autorisations-ID til et CPR-nummer ved opslag i

autorisationsregistret, hvor relationer mellem autorisations-ID'er og CPR nummer opbevares (selvom CPR-oplysningerne ikke udstilles til borgerne).

En svaghed ved autorisationsregistrets søgemuligheder er, at man ikke kan se, hvilke organisationer de pågældende sundhedspersoner aktuelt er knyttet til (eller har været knyttet til i en periode). Såfremt brugere i lokale "Identity Management" / IM -systemer er registreret under CPR-nummer, vil sådanne organisationsoplysninger kunne leveres herfra. Dette er imidlertid komplekst, da der findes mange IM systemer. Hvis sundhedspersonen omvendt har fået udstedt et OCES-certifikat, vil OCES-operatøren kunne levere oplysninger om, hvilke medarbejdere de enkelte organisationer på et tidspunkt har udstedt medarbejdercertifikater til. Hvis man benytter en central autentifikationsmekanisme baseret på digitale certifikater, kan man også ud fra dennes log kunne danne sig et overblik over, hvilke sundhedspersoner, der har benyttet medarbejdercertifikater udstedt af hvilke organisationer.

Man kan også tænke sig MinLog på Sundhed.dk kan levere sådanne oplysninger (dog med begrænsning på, hvor langt tilbage, der kan leveres oplysninger). MinLog kan også mere direkte understøtte borgerne i at udpege personer, der tidligere har haft adgang til en borgers oplysninger m.h.p. at give positivt- eller negativt samtykke til disse personer. Dette fordrer dog, at MinLog kan knytte indgang i loggen til sundhedspersoners autorisations-ID eller CPR nummer.

Brugen af autorisations-ID til at identificere en sundhedsperson har sine begrænsninger. Det er ikke alle uddannelser, hvortil der kræves sundhedsfaglig autorisation for at arbejde i sundhedsvæsenet. Eksempelvis har specialpsykologer i psykiatri samt børne- og ungdomspsykiatri, lægesekretærer, ambulancepersonale, perfusionister (den personalegruppe, som varetager pasning og styring af hjerte-lungemaskine m.v. under åben hjertekirurgi), betjeningspersonale for mammografiudstyr, kommunale sagsbehandlere samt sundhedspersoner under uddannelse ingen sundhedsfaglig autorisation. Skal samtykke kunne dække sådanne faggrupper må det nødvendigvis ske af den organisation, hvori de pågældende arbejder og ved at medarbejderne udpeges ved CPR-nummer. Selvbetjeningsløsning kan p.t. ikke skabes for borgeren.

Note 2 – Afgrænsede informationer

Det ideelle ville være, om borgeren kunne beskytte alle oplysninger hørende til en given sygdom / helbredsproblem. En sådan afgrænsning er imidlertid ikke mulig at skabe, da der ikke findes registreringer, der kan knytte oplysninger sammen på denne måde (i forløb) og da man ikke "algoritmisk" vil kunne afgøre om oplysninger vedrører samme sygdomsforløb eller ej.

Der er i dag defineret et kontaktbegreb, der kan knytte registreringer til samme ambulante kontakt, skadestuekontakt eller indlæggelse, men dette sker kun systematisk for basisregistreringer, der er indberetningspligtige til LPR, og dermed kun en lille del af de samlede registreringer. Ved at medtage kontaktidentifikation med i kommunikation mellem systemer (f.eks. i henvisninger og rekvisitioner) vil det blive muligt at knytte registreringer i flere systemer til de samme kontakter, men der er lang vej før noget sådant kan realiseres bredt (kræver ændringer i mange systemer). Det vil heller ikke nødvendigvis være muligt at gennemføre for alle systemer.

En afgrænsning, som er mulig at realisere, er at give patienter og borgere mulighed for at beskytte alle data opsamlet indenfor en bestemt tidsperiode, evt. begrænset til en given organisatorisk enhed (alle systemer registrerer oplysninger om tid og sted for registreringer). Datamodelmæssigt identificeres "afgrænsede informationer" derfor med tre værdier (informationer vedrørende perioden **<tidsstempel 1>** til **<tidsstempel 2>** på **<organisatorisk enhed>**"). Organisatorisk enhed

kan evt. udelades, hvorved samtykket gælder alle informationer, der blev skabt i den angivne tidsperiode uanset hvor. Tilsvarende vil slutdato kunne udelades, og dermed indikere at alle informationer (eksempelvis fra en given organisatorisk enhed) også fremover skal beskyttes. Dette kan være relevant for patienter der følger langvarig behandling (medfødte sygdomme og handicaps, kroniske sygdomme og andre med komplikationer gennem længere periode).

Reglerne omkring samtykkeverifikation af informationer kompliceres af, at data, hørende til en behandling i organisation X, opstår og registreres i organisation Y. Et godt eksempel er laboratorieprøver, der rekvireres fra behandlingsstedet, men foretages, registreres og i nogle tilfælde videresendes til tredjepart fra prøvestedet.

Konsekvenserne af nuværende begrænsninger er, at såfremt man har flere behandlinger på en afdeling, da kan man ikke holde noget skjult for denne afdeling, hvis man åbner op af hensyn til en anden aktuel behandling.

Det må forventes, at der med tiden udvikles bedre og mere præcise måder at afgrænse informationer på, og datamodeller bør derfor tilrettelægges, så de i et vist omfang er fleksible i forhold til kommende muligheder.

Note 3 – Organisatorisk enhed

Organisatoriske enheder identificeres for nuværende ved forskellige klassifikationer og organisatoriske registre i sundhedsdomænet. På sygehusene benyttes bl.a. Sygehus/Afdelingsklassifikationen (SHAK), mens ydernumre (fra sygesikringsregistret) er det mest udbredte i systemer hos privatpraktiserende enheder (dækker dog kun praksis under overenskomst med sygesikringen).

Borgeren bør kunne udtrykke sine samtykker i en enkel organisationsmodel. Det er ikke særlig borgervenligt at bede borgeren udtrykke sine samtykker i forhold til flere modeller (baseret på forskellige registre og klassifikationer), blot fordi det ikke er lykkedes sundhedsvæsenets parter at konsolidere modellen. Da mange modeller er systemspecifikke, vil det heller ikke være praktisk muligt for borgeren at håndtere alle direkte. Man er derfor nødt til at vælge en model som samtykkeadministration baseres på. De enkelte systemer er derefter nødt til at tolke samtykkeoplysningerne i forhold til den datamodel, som det enkelte system baseres på.

Denne referencearkitektur peger på at benytte SOR (Sundhedsvæsenets Organisationsregister) til at administrere samtykkeoplysninger efter. SOR er netop etableret for at have et samlet register over organisatoriske enheder indenfor sundhedsvæsenet, og SOR giver mulighed for at registrere SHAK-koder og ydernumre til de enkelte enheder (hvorved det bliver muligt for systemer der baserer sig på SHAK-koder og ydernumre at relatere registreringer til samtykkeoplysningerne).

Det skal være muligt for borgeren at angive om samtykket gælder for alle underenheder til den valgte organisatoriske enhed (i SOR registreres under- og overenheder), eller om det alene gælder den udvalgte enhed (og ikke underenheder).

Da SOR-enheder ofte er defineret på et mere detaljeret/fint niveau end eksempelvis SHAK, da kan der findes flere SOR koder for en enkel SHAK kode. Hermed kan det ikke afgøres med sikkerhed, om der er givet samtykke hhv. negativt samtykke til de oplysninger, der er registreret under den mere grove SHAK-kode. I dette tilfælde skal resultatet være, at der ikke er givet samtykke, med mindre der er samtykke til alle tilhørende SOR koder. Ift. negativt samtykke gælder det modsatte,

nemlig at et system ikke må give oplysninger fra sig, såfremt der blot er negativt samtykke til én SOR enhed, tilknyttet den pågældende klassifikation.

Note 4 – Udenlandske sundhedspersoner generelt (epSOS)

I relation til udenlandske sundhedspersoners opslag i danske systemer, er det nødvendigt at en borger kan registrere et samtykke til, at dette er muligt. Samtykket gives pt. ikke til specifikke sundhedspersoner eller organisationer og omhandler alene "patient summary" og "electronic prescription" i epSOS.

Ud over registrering af samtykketype og de tre dimensioner beskrevet ovenfor, er det nødvendigt at registrere hvilken borger samtykket vedrører. For danske borgere kan CPR nummer anvendes og for udenlandske borgere (jf. epSOS) vil et fremtidigt nationalt erstatnings-CPR-nummer kunne anvendes, der tillader tilknytning af nationalitet og national identifikation til erstatnings-CPR-nummeret.

3.4.2.7 Fuldmagt

Borgeren har mulighed for at give en anden, f.eks. til en pårørende ret til at agere på sine vegne. Fuldmagten er ikke nødvendigvis kun gældende på sundhedsområdet, og derfor vil en forretningsservice til understøttelse af denne proces blive udviklet i fællesoffentligt regi.

3.4.2.8 Værdispring

3.4.2.8.1 Lovgrundlag

Værdispringsreglens oprindelse findes i Forvaltningslovens § 28, stk. 2, nr. 3. Efter denne regel er en forvaltningsmyndighed berettiget til at give meget følsomme oplysninger videre til en anden forvaltningsmyndighed uden borgerens samtykke, når der er et klart værdispring mellem på den ene side hensynet til de interesser, der begrunder hemmeligholdelsen selv over for andre myndigheder, og på den anden side afgørende modhensyn til enten private eller offentlige interesser. Serviceloven opererer på samme grundlag.

I sundhedslovens §42a, stk. 5 er værdispringsregelen formuleret således:

Stk. 5. Læger og sygehusansatte tandlæger kan endvidere indhente oplysninger som nævnt i stk. 1, hvis indhentningen er nødvendig til berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, herunder en patient, der ikke kan varetage sine interesser, sundhedspersonen eller andre patienter. Tilsvarende gælder sundhedspersoner med tilladelse efter stk. 4. Tilsvarende gælder endvidere andre sundhedspersoner ved opslag i elektroniske systemer omfattet af stk. 2 og 3 på det behandlingssted, sundhedspersonen er ansat.

3.4.2.8.2 Operationalisering

Formålet er primært at sikre, at en sundhedsperson ikke kommer i en situation, hvor vedkommende mangler vigtig patientinformation og dermed påfører patienten en risiko. På den anden side er det vigtigt, at værdispringsregelen ikke anvendes til at omgå eksisterende sikkerhedsløsninger, og det er derfor vigtigt, at der fastlægges klare regler for dokumentation og opfølgning på anvendelsen, herunder at sikre sig, at der foretages den nødvendige logning af brugernes anvendelse.

Værdispringsregelen betyder derfor ikke, at man kan se bort fra krav om tekniske sikkerhedsforanstaltninger, der regulerer brugernes adgang, men giver en mulighed for at overskride de normalt gældende adgangsrettigheder, hvis der er behov herfor.

Informationssikkerhedsrådet i regi af Digital Sundhed vedtog i 2010 følgende princip vedr. dokumentation for anvendelse af værdispringsregelen:

Princip	Anvendelsen af værdispringsregelen skal dokumenteres elektronisk
Definition	Der skal ved enhver anvendelse af værdispringsreglen ske en elektronisk registrering af dette og begrundelsen herfor. Det skal være muligt at kontrollere, hvornår der sker anvendelse af reglen og med hvilke begrundelser. Den dataansvarlige har en forpligtelse til skærpet opmærksomhed omkring anvendelse af reglen, bl.a. logopfølgning
Konsekvens	Det skal være muligt via logningen på it-systemerne at se, at værdispringsregelen har været anvendt. Den dataansvarlige fastsætter retningslinjer for anvendelse af og opfølgning på anvendelse af værdispringsreglen.
Status	Godkendt i informationssikkerhedsrådet 25.08.2010

Det er op til den enkelte dataansvarlige at sikre, at den anvendte it-løsning kan håndtere dokumentation og opfølgning på anvendelse af værdispringsregelen, eftersom det er tæt knyttet til systemanvendelsen.

Et forhold, som ikke berøres i ovenstående princip er, at brugeren altid bør være vidende om, at værdispringsreglen tages i brug (det skal altså være brugerens aktive beslutning og være et systemmæssigt valg).

Det bør overvejes, om der kan fastsættes en national standard for begrundelser (klassifikation). Eventuelt kan man indledningsvis lade systemerne kommunikere deres egne begrundelser (fritekst) og så benytte erfaringerne med dette til at fastsætte standarder.

3.4.2.9 Logning og opfølgning

3.4.2.9.1 Lovgrundlag

I "bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning"[21], fastsættes i § 19:

[21] Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (BEK nr 528 af 15/06/2000), se: https://www.retsinformation.dk/forms/R0710.aspx?id=842

"Der skal foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år."

Hvad "alle anvendelser" er præciseres i vejledningen til bekendtgørelsen. Om fremsøgning af oplysninger står eksempelvis: " Logningen skal bl.a. omfatte en angivelse af den person, som de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Foretages der en søgning på en person ved angivelse af personnummer, skal således det anvendte personnummer eller anden entydig identifikation af den pågældende person registreres i loggen. Hvis der søges på fødselsdato, skal den angivne dato (søgekriteriet) registreres i loggen, men der er ikke krav om registrering af identifikation af de enkelte personer, som indgår i søgeresultatet, dvs. alle fundne personer med den angivne fødselsdato. Angivelsen i loggen af det anvendte søgekriterium giver mulighed for efterfølgende at rekonstruere behandlingen, herunder hvilke personer som indgik i behandlingen, hvilket bl.a. er formålet med logningen."

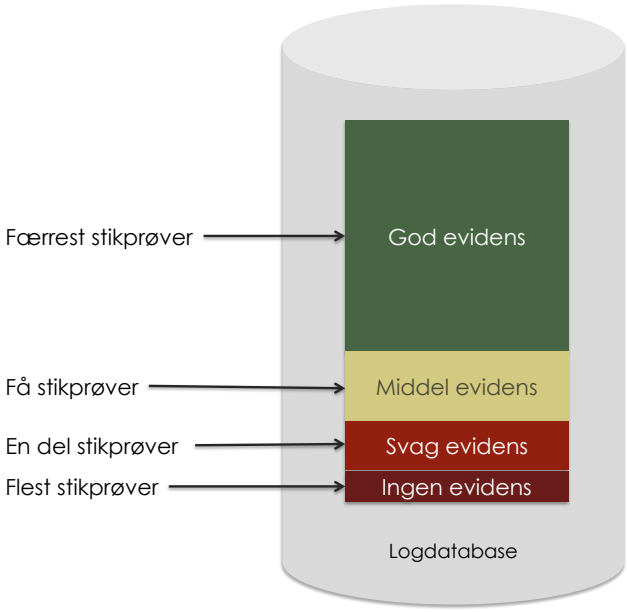
3.4.2.9.2 Operationalisering

Som udgangspunkt skal it-løsninger sikre, at kun personer, for hvem det er relevant, kan få adgang til data, men i nogle situationer kan det være svært elektronisk at afgøre relevansen på det tidspunkt, hvor oplysningerne efterspørges. I disse situationer kan logning understøtte sikkerheden, dels ved, at brugerne er bekendt med, at deres aktivitet logges, dels ved, at der kan foretages opfølgning på, at brugernes adgang til data har været berettiget.

Traditionelt foregår opfølgning ved udtagelse af stikprøver af loggede hændelser og brugere bedes redegøre for de udtagne hændelser. Når stikprøverne udtages blandt alle loggede hændelser vil sandsynligheden for at konstatere et misbrug være relativ lille.

I stedet kan man overveje løbende automatisk opfølgning. Hvis en tjenesteudbyder ved adgangskontrol eksempelvis kun finder "middelgod" evidens for behandlingsrelation, kan vedkommende gentage verifikationen et antal gange (eks. dagligt) i en periode (eks. 60 dage). Hvis der i mellemtiden registreres oplysninger, der kan være med til skabe tilstrækkelig evidens for behandlingsrelation, så kan de gentagne check stoppe, og behandlingsrelationen betragtes som værende verificeret. Der er således ikke længere behov for at følge manuelt op på, om der var evidens for behandlingsrelation ved den pågældende adgang til patientoplysninger. Det er kun hvis der heller ikke senere kan findes den fornødne evidens indenfor et nærmere angivet tidsrum, at tjenesteudbyderen kan overveje at sætte en manuel opfølgningsproces i værk for at få udredt adgangen.

Ved løbende at foretage automatisk verifikation og ved løbende at registrere resultatet, kan man mere målrettet foretage stikprøvekontrol, således at stikprøverne koncentreres om de adgange til patientoplysninger, hvor gentagne verifikationer ikke har kunnet hæve styrken af evidens tilstrækkeligt – se nedenstående figur.



Figur 18 – Log - opfølgning

Ved etablering af nye nationale løsninger anbefaler denne referencearkitektur, at man fastlægger hvor stærk evidens man vil have for behandlingsrelation og at man samtidig forholder sig til, om der skal ske løbende opfølgning og hvor længe. Der henvises i øvrigt til [behandlingsrelation].

Man kan også forestille sig andre former for automatiseret (eller delvis automatiseret) opfølgning. F.eks. kan manglende evidens i verifikationer afføde notificering af patienten.

En sidste opfølgningsmulighed som skal nævnes her er at give borgeren / patienten mulighed for at overvåge tilgangen til vedkommendes egne oplysninger. Dette er realiseret ved MinLog på sundhed.dk.

3.4.3 Operationer

I dette afsnit beskrives komponenterne ud fra deres snitflader til omgivelserne (interfaces). Et interface beskriver en række operationer, som komponenten realiserer. Eksempelvis vil komponenten ”Samtykke” stille et interface til rådighed med en række operationer der skal gøre det muligt at håndtere borgerens samtykker. Der tages i referencearkitekturen ikke stilling til hvordan komponenterne og operationerne skal realiseres. Det afgørende er, at komponenterne spiller en veldefineret rolle i arkitekturen og at snitflader er veldefinerede. Om komponenterne så er centrale eller distribueret ud på flere parter, hvilke teknologier de baserere sig på og om snitflader realiseres v.h.a. web services eller andre teknologier, er denne teknologi-neutrale referencearkitektur uvedkommende.

3.6.1.1 Stamdata

Stamdata komponenten realiserer følgende operationer:

- Hent CPR-oplysninger
- Opret erstatnings-CPR-nummer
- Sammenknyt erstatnings-CPR-nummer til CPR-nummer
- Sammenknyt erstatnings-CPR-nummer til udenlandsk ID

- Opret/vedligehold/slet organisatorisk enhed
- Opret/vedligehold/slet relationer mellem organisatoriske enheder
- Søg organisatorisk enhed

Hvad	Beskrivelse
Kort beskrivelse	Forretningstjenesten henter relevante stamdata til brug for registrering af personer og organisationer. Ligeledes giver tjenesten adgang til at oprette et erstatnings-CPR nummer, som evt. kan knyttes til et dansk CPR-nummer på et senere tidspunkt eller kan knyttes til et udenlandsk ID.
Understøtter processer	
Afhængigheder	

3.6.1.6 Autentifikation

Autentifikationskomponenten realiserer følgende operationer:

- Check gyldighed af akkreditiver
- Identificer person ud fra akkreditiver

Hvad	Beskrivelse
Kort beskrivelse	
Understøtter processer	Styring af adgang til patientoplysninger (adgangskontrol)
Afhængigheder	

3.6.1.7 Autorisation

Autorisationskomponenten realiserer følgende operationer:

- Opret/vedligehold/slet roller/arbejdsfunktioner
- Tildel/vedligehold/slet rettigheder på baggrund af arbejdsfunktion
- Check arbejdsfunktion

Hvad	Beskrivelse
Kort beskrivelse	Komponenten muliggør registrering af roller/arbejdsfunktioner og de dertil hørende rettigheder, som kan anvendes ved adgang til fælles nationale tjenester og kommunikation på tværs i sundhedsvæsenet. I relation hertil skal de enkelte it-løsninger blot fastlægge, hvilke adgangsrettigheder, der skal knyttes til de enkelte roller/arbejdsfunktioner
Understøtter processer	Administration af ansættelsesforhold og arbejdsfunktion Styring af adgang til patientoplysninger (adgangskontrol)
Afhængigheder	Integration med lokal brugeradministration

3.6.1.5 Delegering

Delegeringskomponenten realiserer følgende operationer:

- Opret/vedligehold/slet delegeret arbejdsfunktion
- Tildel/vedligehold/slet rettigheder på baggrund af arbejdsfunktion

Hvad	Beskrivelse
Kort beskrivelse	Forretningstjenesten gør det muligt at registrere, at en sundhedsperson har delegeret en opgave til en anden person eller gruppe af personer (medhjælp). Ved delegering skal der kunne angives, hvilke systemmæssige rettigheder, medhjælpen skal have (ud over de rettigheder, vedkommende har i kraft af sin normale arbejdsfunktion) for at kunne udføre den delegerede opgave.
Understøtter processer	Forespørgsel på patientoplysninger Delegering af arbejdsopgaver / arbejdsfunktion Styring af adgang til patientoplysninger (adgangskontrol)
Afhængigheder	Integration fra lokale it-løsninger til forretningstjenesten

3.6.1.8. Behandlingsrelation

Behandlingsrelationskomponenten realiserer følgende operationer:

- Valider behandlingsrelation

Hvad	Beskrivelse
Kort beskrivelse	Forretningstjenesten gør det muligt på baggrund af udtræk fra autoriserede kilder at beskrive evidens for behandlingsrelation mellem en patient og en behandler/behandlingssted. Dette bruges f.eks. ved opslag på nationale tjenester (f.eks. FMK). Servicen returnerer svar, der er klassificeret i forhold til styrken af evidens for relationerne.
Understøtter processer	Styring af adgang til patientoplysninger (adgangskontrol)
Afhængigheder	

Komponenten benytter sig af dataudtræk fra forskellige kilder til at finde evidens for behandlingsrelationer mellem en patient og en behandler/behandlingssted.

3.6.1.2 Samtykke

Samtykkekomponenten realiserer følgende operationer:

- Opret, vedligehold og slet samtykke
- Validér positivt samtykke
- Validér negativt samtykke

Beskrivelse af komponenten er angivet i følgende tabel:

Hvad	Beskrivelse
Kort beskrivelse	Samtykkekomponenten indeholder alle borgerens samtykkeoplysninger. Borgeren selv, en befuldmægtiget eller en sundhedsperson på vegne af borgeren kan oprette et positivt eller et negativt samtykke. I forbindelse med opslag på nationale tjenester sikrer samtykkekomponenten, at borgerens samtykkeoplysninger anvendes til at validere brugerens adgang til data.
Understøtter processer	Administration af samtykkeoplysninger Styring af adgang til patientoplysninger (adgangskontrol)
Afhængigheder	Der skal etableres interfaces mellem samtykkekomponenten og de enkelte it-løsninger. Løsningen vil ikke være fuldt dækkende, før alle it-systemer kan anvende komponentens informationer

3.6.1.3. Fuldmagt

Fuldmagtskomponenten realiserer følgende operationer:

- Opret, vedligehold og slet fuldmagt
- Check fuldmagt

Hvad	Beskrivelse
Kort beskrivelse	Forretningstjenesten gør det muligt for borgeren at give en anden person ret til at agere på vedkommendes vegne. I første omgang giver den digitale tjeneste adgang til, at den befuldmægtigede kan tilgå on-line tjenester på vegne af borgeren.
Understøtter processer	Administration af fuldmagtsoplysninger Styring af adgang til patientoplysninger (adgangskontrol)
Afhængigheder	

Fuldmagtskomponenten udvikles af Digitaliseringsstyrelsen som en fællesoffentlig tjeneste.

3.6.1.10. Værdispring

Værdispringskomponenten realiserer følgende operationer:

- Registrer anvendelse af værdispring
- Registrer opfølgning på værdispring

Hvad	Beskrivelse
Kort beskrivelse	Forretningstjenesten skal sikre, at man elektronisk kan registrere og følge op på en bruger, der har tilgået data, som de ikke med deres almindelige adgangsrettigheder må tilgå.
Understøtter processer	Forespørgsel på patientoplysninger
Afhængigheder	

3.6.1.9. Opfølgning

Komponenten realiserer følgende operationer:

- Opsaml logoplysninger fra tilknyttede kilder
- Vis logoplysninger
- Valider behandlingsrelation løbende
- Send information om manglende behandlingsrelation til dataansvarlig

Hvad	Beskrivelse
Kort beskrivelse	Hvis det ikke er muligt at finde evidens for en behandlingsrelation på et tilstrækkeligt højt niveau på det tidspunkt, hvor der foretages opslag i en national tjeneste, kan informationer om opslaget overføres til opfølgningskomponenten, som på baggrund af opslag i autoritative kilder (f.eks. LPR og sygesikringsregisteret) kan validere, at der eksisterede en behandlingsrelation på det tidspunkt, opslaget blev foretaget.
Understøtter processer	Logning af adgang til patientoplysninger Opfølgning på adgang til patientoplysninger
Afhængigheder	

4 Teknisk arkitektur

Denne referencearkitektur er en grundlæggende referencearkitektur, der skal bringes i anvendelse på tværs af forskellige teknologier og anvendelsesscenarier. Da referencearkitekturen således er tænkt teknologineutral, er det begrænset, hvor meget teknisk arkitektur, der er at beskrive.

Afsnittet afgrænser sig til at beskrive information, der benyttes til adgangsstyring m.m., herunder hvilke kilder, der er (eller foreslås) autoritative i forhold til denne information, samt identificerer behov for fastlæggelse af nationale standarder, der medvirker til en mere ensartet sikkerhedshåndtering.

4.1 Kilder til styringsinformation

Kilde	**Information**
Nets / DanID. Certificate Authority (CA)	OCES certifikater og deres gyldighed (herunder LRA-certifikater)
CPR registret	Identiteten af fysiske personer og stamdata på disse, eks. navne, bopæl, civilstand, statsborgerskab og meget andet.
Sundhedsstyrelsens autorisationsregister	Sundhedsfaglige autorisationer, oplysninger om uddannelse.
Sundhedsvæsenets Organisationsregister - SOR	Identiteten af organisatoriske enheder indenfor sundhedsvæsenet og stamdata på disse.
Samtykkeregistret (etableret med NPI)	Borgerens samtykkeoplysninger.
Lokale Identity Management systemer, Sundhedsstyrelsens elektroniske brugerstyring (SEB)	Personers tilknytning til organisation (eks. ansættelser) herunder hvilke arbejdsfunktioner de udfører
Brugersystem	Oplysninger om bruger session, herunder system-, bruger og patientkontekst samt oplysninger om formål med indhentelse af oplysninger samt begrundelser for anvendelse af værdispringsregel.

4.2 Forslag til standarder

Område	Forslag til fastsættelse standard
Krav der skal overholdes i forbindelse med forskellige sikkerhedsniveauer	Liberty Identity Assurance Framework v. 1.1
Beskrivelse af arbejdsfunktioner til brug for tildeling af systemmæssige rettigheder	Intet konkret forslag, men behov for fastsættelse af en national klassifikation.
Beskrivelse af begrundelser for anvendelse af værdispringsregel	Hvis disse er få og relativ statiske bør de indarbejdes i fremtidig revision af denne referencearkitektur – ellers bør der fastlægges en national klassifikation.

Bilag A: Samlet begrebsmodel

[Leveres af begrebsarbejdet E2012]

Bilag B: Supplerende begreber

Begreb	Beskrivelse
aktuel behandling	Er en patients igangværende kontakt til en sundhedsperson eller en sundhedsorganisation.
Akkreditiver	Et akkreditiv er en attest, der verificerer, at en ressource eller person er den hævdede. **A**kkreditivets rigtighed godtgøres af kontrolløren i forbindelse med autenticitetssikring. Akkreditiver er bundet til det individ, de er udstedt og anvendes til autentificering eller kan være gældende for et individ, der på et givet tidspunkt er ihændehaver af dem.
Audit	Analyse og gennemgang af et system med henblik på sikkerhed og funktionalitet, herunder analyse af brugeres adfærd
autenticitet	Egenskab, der beskriver, om noget er, hvad det giver sig ud for at være (om det er autentisk/ægte). Gennem autenticitetssikring/autentifikation sikres, at en ressource eller person er den påståede.
Autentifikation	Autentifikation er den handling, hvor en brugers unikke identitet verificeres ved brug af en autentifikationsteknik. Autentifikationen vil typisk være baseret på fremvisning af eller bevis for ihændehavelse af et akkreditiv.
Autorisation	Autorisation er den handling, hvor en brugers adgangsrettighed til funktion til funktioner eller data i et informationssystem styres
autoriseret bruger	En autoriseret bruger er en bruger, der har fået tildelt adgangsrettigheder til funktioner eller data i et informationssystem
begrænsende sikringsforanstaltning	sikringsforanstaltning der har til formål hindre udbredelse af skade efter et sikkerhedsbrud
behandlingsenhed	En behandlingsenhed er en sundhedsproducerende enhed, hvor der ved at knytte en relation mellem patient og sundhedsperson afgrænses adgang til sundhedsoplysninger i it-systemer. Begrebet har ingen genografisk afgrænsning. En sundhedsproducerende enhed danner rammen for de sundhedsprofessionelles sundhedsaktiviteter
behandlingsrelation	En behandlingsrelation er relationen mellem en sundhedsprofessionel og en patient/borger, som eksisterer, så længe den sundhedsprofessionelle er involveret i patientens aktuelle behandling. Behandlingsrelationen anvendes til at afgøre, om den sundhedsprofessionelle må få adgang til patientens oplysninger
delegering	Delegering er den handling, hvor en sundhedsperson overdrager retten til at udøve sundhedsfaglig virksomhed på sine vegne til en anden. Denne form for delegation følger af bekendtgørelsen vedr. delegering af sundhedsfaglig

	virksomhed[22]. Hvis en sundhedsperson overdrager retten til at indhente patientrelateret information på sine vegne til en anden, er dette reguleret via Sundhedslovens[23] §42a, der indeholder særlige regler om benyttelse af medhjælp ved informationsindsamling. I begge tilfælde er den person, der delegerer opgaven, ansvarlig for instruktion af og kontrol med den medarbejder, til hvem opgaven er delegeret.
forebyggende sikringsforanstaltning	sikringsforanstaltning der har til formål at forhindre sikkerhedsbrud
forsinkende sikringsforanstaltning	sikringsforanstaltning der har til formål at udsætte tidspunktet for hvornår skaden indtræffer
fortrolighed	Egenskab ved informationssystem der medfører, at kun bestemte brugere har adgang til bestemte data eller bestemt information
forældremyndighed	Forældres ret og pligt til at drage omsorg for barnet og kan træffe afgørelse om dets personlige forhold ud fra barnets interesse og behov
fuldmagt	Tilladelse, som en person giver til en anden person, sådan at denne bliver umiddelbart berettiget og forpligtet overfor tredjemand ved handlinger, som den befuldmægtigde foretager i fuldmagtsgiverens navn og indenfor fuldmagtens grænser
fysisk sikringsforanstaltning	teknisk sikringsforanstaltning der benytter fysiske midler
integritet	Egenskab ved et informationsaktiv, der sikrer dettes nøjagtighed og fuldstændighed. Integritet sikrer fx kommunikation, således at en serviceudbyder og en serviceaftager er garanteret, at beskederne ikke ændres mellem afsender og modtager uden at én af parterne opdager det.
kompenserende sikreingsforanstaltning	sikringsforanstaltning der erstatter en anden sikringsforanstaltning Kommentar: Hvis fx funktionsadskillelse til minimering af risikoen for misbrug af systemer ikke kan gennemføres, kan en kompenserende sikringsforanstaltning være overvågning, logning el. lign.
logisk sikringsforanstaltning	teknisk sikringsforanstaltning der benytter logiske midler Kommentar: Ved logiske midler forstås fænomener, der udspiller sig i digitale informationssystemers kredsløb.
”negativt samtykke”	Egenskab, der giver patienten mulighed for at frabede sig, at en bestemt sundhedsperson indhenter informationen i et informationssystem. En patient kan også vælge at underlægge en patientrelateret information et generelt negativt samtykke. I så fald gælder det negative samtykke alle sundhedspersoner.
opklarende sikringsforanstaltning	sikringsforanstaltning der har til formål at opdage og belyse sikkerhedsbrud
organisatorisk sikringsforanstaltning	sikringsforanstaltning der benytter organisatoriske midler

[22] https://www.retsinformation.dk/forms/R0710.aspx?id=129042

[23] Se eventuelt www.retsinformation.dk/forms/r0710.aspx?id=130455

	Kommentar: 1. Ved organisatoriske midler forstås alt, hvad der har med en organisations medlemmer at gøre, fx - relationer mellem medlemmerne - arbejdsgange og rutiner - forskrifter (politikker, strategier, instrukser, vejledninger osv.) - kompetencer - virksomhedskultur - ledelsesbeslutninger
Privacy (”privatlivets fred”)	egenskab ved data, information eller informationssystem der beskytter potentielt personhenførbar information mod at komme i forkerte hænder
samtykke	egenskab ved patientrelateret information, der giver en person mulighed for at give en bestemt sundhedsperson eller sundhedsorganisation adgang til at indhente information om personen selv eller om en person, som man er værge for eller en person under 15 år, som man har forældremyndigheden for. Samtykke er reguleret gennem Persondatalovens § 3, nr. 8, hvor der står: ”8) Den registreredes samtykke: Enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling”. I sundhedslovens §41 vedrørende videregivelse af digitale informationer og §42a vedrørende indhentning af digitale informationer er der fastsat nærmere regler for, hvornår patientens samtykke er påkrævet.
sikringsforanstaltning	foranstaltning der har til formål at øge informationssikkerhed
sundhedsaktivitet (sundhedsfaglig opgave)	Sundhedsrelateret aktivitet, der er rettet mod én patient
sundhedsperson	sundhedsaktør der er autoriseret i henhold til særlig lovgivning til at varetage sundhedsfaglige opgaver, og personer, der handler på disses ansvar
sundhedsorganisation	En organisation, der danner ramme for sundhedsprofessionelles sundhedsaktiviteter.
teknisk sikringsforanstaltning	sikringsforanstaltning der benytter tekniske midler Kommentar: Ved tekniske midler forstås faciliteter, udstyr og fysiske indretninger, fx - bygninger og deres indretning - maskiner - it-udstyr (både hardware og software)
tilgængelighed	egenskab ved service der sikrer, at servicen er til rådighed for en bruger i henhold til fastlagte rammer

uafviselighed	egenskab ved information der gør det muligt at bevise, at en given bruger har udført en given handling på et givet tidspunkt
Udbedrende sikringsforanstaltning	sikringsforanstaltning der har til formål at afbøde skader efter sikkerhedsbrud

Bilag C: Fællesoffentlige it-arkitekturprincipper

STRATEGI	FORRETNING	TEKNIK
Forretningsbehov bør drive og definere løsningerne.	Borgere og virksomheder bør sættes i centrum.	It-arkitekturen bør via åbenhed styrke konkurrence og innovation.
Informationssikkerhed fra start til slut.	Processer bør optimeres i forbindelse med digitalisering.	Basér løsninger på løst koblede komponenter.
Brug den fællesoffentlige metoderamme for it-arkitektur.	Data og services bør genbruges.	Løsninger bør være fleksible.
		Udnyt mulighederne ved anskaffelser.

Kilde: IT- og telestyrelsen, **http://digitaliser.dk/resource/286019**

Bilag D: Referencer

[behandlingsrelation]	"Behandlingsrelations service - Definitioner, scenarier og vejledning til brug", NSI, version 1.09, december 2011.	Kan rekvireres ved henvendelse til NSI
[ITST]	"Vejledning vedrørende niveauer af autenticitetssikring", ITST	http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-brugerstyring/filer-til-standarder-for-brugerstyring/ Horing.B.st.niv.autenticitetssikring.v5.pdf
[ITST-OIOIDWS]	"Identitetsbaserede webservices og personlige data", version 0.8 UDKAST	https://www.borger.dk/Lovgivning/Hoeringsportalen/dl.aspx?hpid=19124
[LIAF]	"Liberty Identity Assurance Framework", v. 1.1	http://www.projectliberty.org/
[NBS 06]	"Et begrebssystem for informationssikkerhed - Rapport fra arbejdsgruppe nbs06 under Det Nationale Begrebsråd for Sundhedsvæsenet", Maj 2006	http://begrebsbasen.sst.dk/informationssikkerhed/nbs06_textrapp_20060609.pdf
[NIST 800-63]	"NIST Electronic Authentication Guideline", v. 1.0.2 April 2006	http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
[NIST 800-95]	"Guide to Secure Web Services", National Institute of Standards and Technology	http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

	(NIST), USA. August 2007	
[OIOEA_BP]	OIO Referencearkitektur – best practice anbefalinger"	http://ea.oio.dk/referencearkitektur/best-practice-anbefalinger/
[SDSD-AUTH]	"Vurdering af autentifikations-strategier for nationale tjenester i sundheds-sektoren", SDSD	Kan rekvireres ved henvendelse til NSI
[SDSD-Analyserapport]	"Behandlingsrelation, nødvendighed, samtykke og værdispring - Rapport fra analyseprojektet vedr. informationssikkerhed", SDSD, 30. nov. 2009.	Kan rekvireres ved henvendelse til NSI
[SikModeller]	"Nye digitale sikkerhedsmodeller – et diskussionsoplæg", It- og Telestyrelsen, januar 2011	http://www.google.dk/url?sa=t&rct=j&q=nye%20sikkerhedsmodeller&source=web&cd=1&ved=0CD4QFjAA&url=http%3A%2F%2Fdigitaliser.dk%2Fresource%2F781482%2Fartefact%2FNye%2Bdigitale%2Bsikkerhedsmodeller.pdf&ei=nUkzUNTFPOrR0QXPi4CgBg&usg=AFQjCNHJ7_SWxIyLiFMtwdp1wIQFUIkx6Q
[Sikkerhedsarkitektur]	Digital Sundhed – Sikkerhedsarkitektur. Kapitlerne: Indledning, Strategi, Forretning, Information, Applikation og Referencemateriale. SDSD, nov. 2010	Kan rekvireres ved henvendelse til NSI
[STD_RA]	"Standarder og referencearkitekturer vedr. sundheds-it området", version 1.0,	http://www.ssi.dk/Sundhedsdataogit/National%20Sundheds-it/~/media/Indhold/DK%20-%20dansk/Sundhedsdata%20og%20it/National%20Sundheds-it/Standardisering/Rapport_standarder_og%20_referencearkitekturer.ashx

	NSI, september 2011.	
[SundPrincip2009]	”Arkitekturprincipper for Sundhedsområdet – en ramme for udformning af fremtidens nationale it-arkitektur for sundhedsvæsenet”, SDSD, juni 2009	http://digitaliser.dk/resource/661376
LIAF-HEALTH	Oversigt over aktiviteter indenfor sundhedssektoren i Liberty-regi	http://www.projectliberty.org/liberty/adoption/healthcare