2023

Referencearkitektur for informationssikkerhed

Cyber- og informationssikkerhedsovervejelser i forbindelse med anskaffelse og udvikling af IT-systemer til sundhedssektoren.

SUNDHEDSDATA-
STYRELSEN

Udgiver	Sundhedsdatastyrelsen Ørestads Boulevard 5 2300 København S Sundhedsdatastyrelsens hjemmeside kontakt@sundhedsdata.dk
Ansvarlig institution	Arkitekturarbejdsgruppen under Sundhedsdatastyrelsens initiativ 2.6 fra Cyber- og informationssikkerhedsstrategien 2018-2022
Design	Sundhedsdatastyrelsen
Copyright	Sundhedsdatastyrelsen
Version	Godkendelsesversion 2.0
Versionsdato	20. september 2023
Web-adresse	www.sundhedsdata.dk
Titel	Referencearkitektur for informationssikkerhed

Revisionshistorik

Dato	Revision	Kommentar
19-02-2021	Udkast 0.1	Til kommentering i arbejdsgruppen
26-02-2021	Udkast 0.2	Indarbejdet kommentarer og rettelser fra Pia Jespersen
02-03-2021	Udkast 0.3	Indarbejdet kommentarer og rettelser jura v.1
03-03-2021	Udkast 0.4	Kommentarer og rettelser arbejdsgruppemøde 3/3
03-03-2021	Udkast 0.5	Indarbejdet kommentarer og rettelser jura
20-04-2021	Udkast 0.6	Indarbejdet kommentarer og rettelser fra jura
05-07-2021	Udkast 0.7	Jura kommentarer indarbejdet, tilrettet byggeblok afsnit så det passer med målbillede for infrastruktur, lagt i format template etc.
05-08-2021	Udkast 0.8	Flowdiagrammer indarbejdet i tekst og bilag
20-09-2022	Udkast 0.9	Afsnit om byggeblokke tilrettet af EAD. Klargøring til RUSA.
03-01-2023	Udkast 0.91	SRNI: Review efter kommentarer fra RUSA
10-01-2023	Høringsversion 01	
	Høringsversion 02	Revision efter modtagne høringssvar
	Høringsversion 02b	Rettet, men uden rettelsesmarkeringer
19-09-2023	Godkendelsesversion 2.0	Endelige rettelser til godkendelse på Cyberstyregruppemøde den 4. oktober 2023.

Arkitekturarbejdsgruppens medlemmer i forløbet

Pia Jespersen, Sundhedsdatastyrelsen
Christa Wulff Sarby, Sundhedsdatastyrelsen
Helle Mørch, Sundhedsdatastyrelsen
Dan Bjørnboe, Kommunernes Landsforening
Emil Lobe Suenson, Medicoindustrien
Esben Andreas Dalsgaard, Sundhedsdatastyrelsen
Hans Henrik Bøttger, Region Midt
Henning Olsen, Herning Kommune
Kim B. Larsen, Systematic
Kjeld Gandrup, Compugroup
Kurt Hansen, Strand og Donslund
Morten Mølgaard Pedersen, Region Syddanmark
Peder Illum, Medcom
Rasmus Halkjær Iversen, Kombit
Thomas Celinder, Region Hovedstaden
Thomas Lund Eriksen, NNIT
Søren Nielsen, Sundhedsdatastyrelsen

Endvidere juridisk rådgivning ved
Anahita Khatam-Lashgari, Sundhedsdatastyrelsen
Sigrun Gyrtrup, Sundhedsdatastyrelsen

Indhold

1 Resumé

It-anvendelsen i sundhedsvæsenet flytter sig fra den enkelte parts anvendelse af egne data til anvendelse af data opsamlet ved forskellige parter i og uden for sundhedsvæsenet.

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 og sikre det rigtige sikkerhedsniveau, der hvor data anvendes.

Referencearkitekturen fungerer som fælles pejlemærke, der medvirker til at sikkerhedsmodeller udvikler sig i samme retning.

Referencearkitekturen beskriver de vigtigste socioøkonomiske tendenser, der skal håndteres af nuværende og fremtidige løsninger. Dette omfatter i stor grad borgerens inddragelse og borgerens egne sundhedsdata. Af sikkerhedsmæssige og teknologiske tendenser bemærkes især øget niveau af cybertrusler, øget brug af mobile enheder og ikke mindst IOT-enheder, der skal integreres i løsningerne.

Referencearkitekturen opstiller en fælles vision, fælles værdier og fælles principper.

Visionen tegner et billede, hvor det sikres:

> ***At den fortsatte bevægelse mod en mere helhedsorienteret indsats, hvor hospitaler, kommunale sundhedstilbud, praksissektor og andre offentlige og private aktører i hele sundhedsvæsenet kan samarbejde i et integreret netværk om og med borgeren i centrum. Strategiens overordnede sigte er at understøtte sundhedsaktører i at løfte deres ansvar for at skabe sammenhæng på tværs af de enkelte kontakter. Flere opgaver kan med digitalisering løses tæt på borgeren i et nært og sammenhængende sundhedsvæsen, der ser på det hele menneske og ikke kun på den enkelte diagnose.***

Referencearkitekturen foreslår, at

- der arbejdes efter sikkerhedsmodeller, der såvel tillader fælles sikkerhedsløsninger ved betroet tredjepart som modeller baseret på føderationer.
- at sikkerhedsmodeller er attribut-baseret, og at sikkerheden håndhæves der, hvor data anvendes.
- at der adgangsstyres ud fra standardiserede oplysninger om borgere, sundhedspersoner, organisatoriske enheder, ansættelsesforhold, arbejdsfunktioner, autenticitetsstyrke (sikkerhed for fastslået identitet af brugere og systemer), styrke for evidens af behandlingsrelation, samtykke, fuldmagter, delegeringer og begrundelser for brug af værdispringsregel m.v.

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

Referencearkitekturen peger på et sæt arkitekturbyggeblokke, der anses som værende centrale for sikkerhedsmodellerne, og som ved projekter og anskaffelser bør vurderes i forhold til sikkerhedsmodel for den specifikke løsning. Referencearkitekturen angiver en række løsningsbyggeblokke, som kan anvendes i de enkelte løsninger.

Referencearkitekturen peger også på relevante standarder og metoder for arbejdet med informationssikkerhed generelt og for sikkerhedsmodeller.

2 Indledning

2.1 Revision

Denne Referencearkitektur for informationssikkerhed 2.0, gældende for det danske sundhedsvæsen, er udformet henover efterår og vinter 2020-2021.

Det tilsigtes at holde en form for referencearkitektur eller bibliotek ved lige. Det påhviler initiativ 2.6 i Sundhedssektorens strategi for cyber og Informationssikkerhed 2023- 2025, at finde en form der tilgodeser behovet på en måde, der understøtter den dynamik, der er på sikkerhedsområdet i sundhedssektoren.

2.2 Hvad er referencearkitektur?

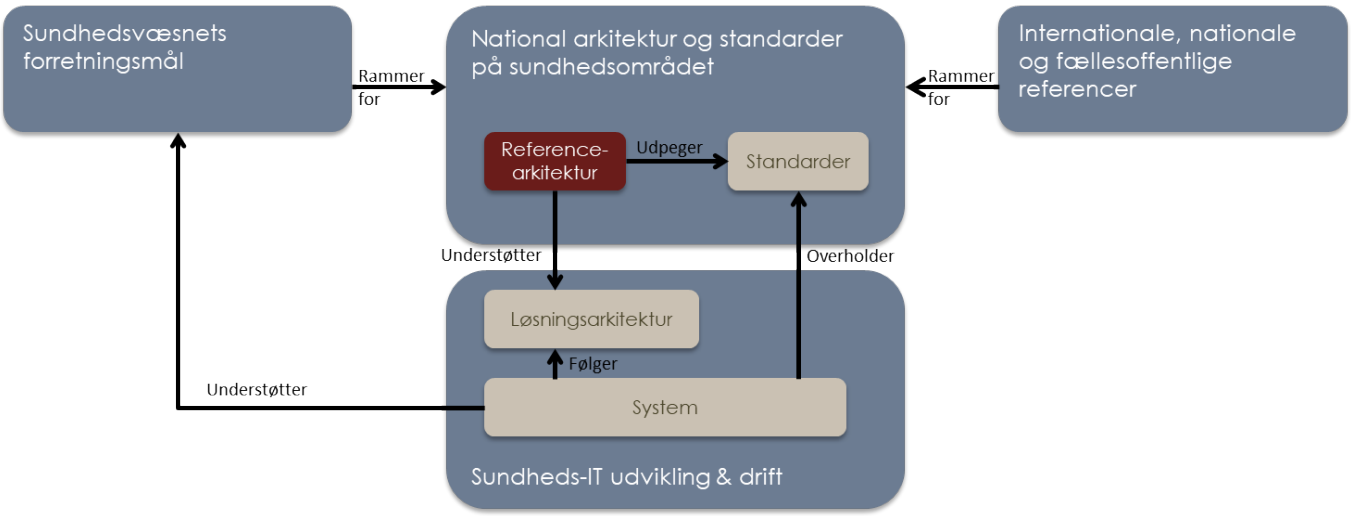
FDA, Fællesoffentlig Digital Arkitektur, beskriver det således: *"En referencearkitektur beskriver, hvordan løsninger skal bygges inden for et specifikt område, med henblik på at flere anvender samme arkitektur. Referencearkitekturerne beskriver vision, mål og principper, udpeger de vigtigste arkitekturbyggeblokke og kan anvendes til at pege på løsningsbyggeblokke og områder for fælles standarder og fælles løsninger herunder særligt fælles infrastrukturkomponenter"*

I rapporten "Standarder og referencearkitekturer vedr. sundheds-it-området" tages der udgangspunkt i IT- og Telestyrelsens definition:

- *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, ud over 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."*

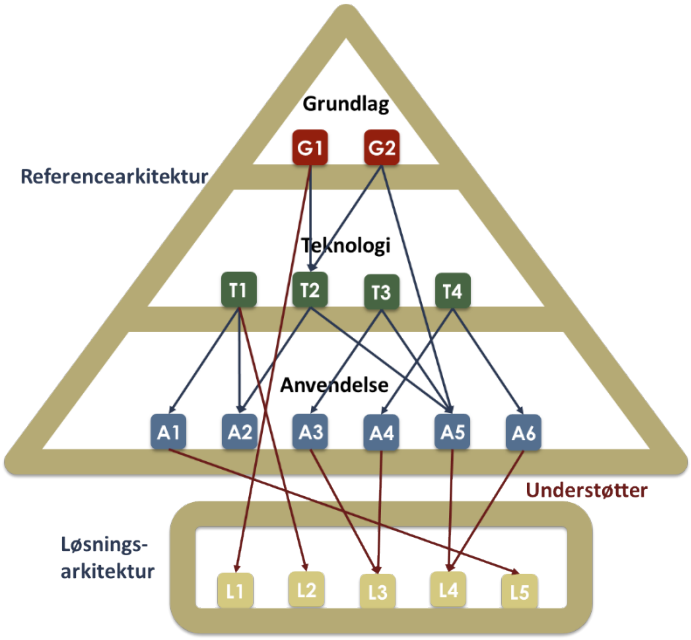
En referencearkitektur dækker således et afgrænset område, hvor der på det strategiske niveau fastlægger forretningsmæssige mål og beskriver ønskede egenskaber for løsninger på området. Her fastlægges også de overordnede principper for løsninger. Løsningselementer og processer beskrives og på baggrund af dette, identificeres de områder, der kan gøres til genstand for standardisering.

Nedenstående figur illustrerer sammenhængen mellem referencearkitekturer og standarder. Figuren viser endvidere at forretningsmål for sundhedsvæsenet samt internationale og nationale standarder definerer rammer for den enkelte referencearkitektur.



Figur 1 Arkitektur og standarder på sundhedsområdet

Inden for sundhedsdomænet arbejdes der med 3 typer referencearkitekturer:



Figur 2 Sammenhæng mellem forskellige typer arkitektur

Figur 3 Sammenhæng mellem forskellige typer arkitektur

Grundlæggende referencearkitekturer er fundamentet for de fleste løsninger på tværs af anvendelse og teknologier. Et eksempel på en grundlæggende referencearkitektur kan f.eks. være en referencearkitektur for informationssikkerhed.

Teknologiske referencearkitekturer understøtter de anvendelsesrettede og de grundlæggende områder. En referencearkitektur for webservices tilhører eksempelvis denne gruppe.

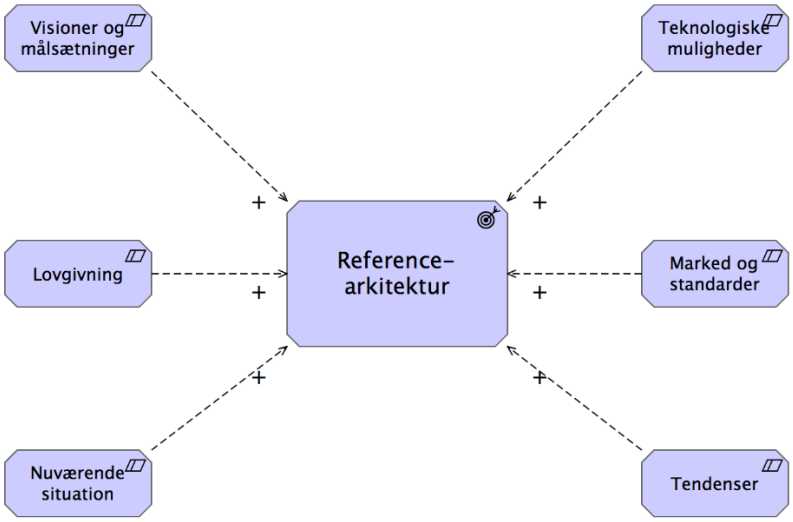
Anvendelsesorienterede referencearkitekturer understøtter prioriterede forretningsmæssige målsætninger. En referencearkitektur for deling af dokumenter og billeder tilhører eksempelvis denne gruppe.

Pyramiden illustrerer det forhold, at der vil være relativt få grundlæggende referencearkitekturer, lidt flere teknologiske og flest anvendelsesmæssige. Hvad der ikke fremgår af figuren er, at der naturligvis er flest arkitekturer, der beskriver de specifikke løsninger.

Denne referencearkitektur er af typen Grundlæggende referencearkitektur.

2.3 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 og formulere en fælles vision og fælles principper for den videre udvikling. Nærværende referencearkitektur beskæftiger sig med digital behandling af digitale oplysninger, og er således ikke møntet på håndtering af papirbårne oplysninger.



Figur 4 Referencearkitekturen påvirkes af omgivelserne

Referencearkitekturen 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 oplysninger. Der er tale om en referencearkitektur, der skal være med til at skabe fælles rammer om de it-løsninger, som udvikles og anvendes, herunder samspil med fælles offentlige tiltag og løsninger som for eksempel NSIS og realisering af denne.

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 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.

2.4 Afgrænsning

I et landskab med stadig stigende fokus på beskyttelse af individdata og et stort ønske fra myndigheder og forskere om at dele sundhedsdata, vil denne referencearkitektur for informationssikkerhed koncentrere sig om behandling af individbaserede data. Altså den primære benyttelse af patientdata i behandlingsøjemed, men også borgerens ret og ønske om at have indsigt i og kontrol over egne oplysninger

Begreber som de-identificering, anonymisering, pseudonymisering og syntetisering af data berøres ganske kort, men en egentlig behandling af emnet bør henvises til en selvstændig referencearkitektur.

2.5 Referencearkitekturens centrale begreber

Referencearkitekturens centrale begreber tager udgangspunkt i Sundhedsvæsenets begrebsdatabase (NBS)[1]. De centrale begreber er suppleret i forhold til NSIS-definitioner, for at referencearkitekturens begreber er i overensstemmelse med NSIS-begreber.

NBS sætter lighedstegn mellem information og oplysninger, men databegrebet er ikke defineret. Data betragtes her som en rå samling af materiale, der sammenstilles, så det det giver en logisk mening og bliver til oplysninger. De er en gennemgående konsekvent brug af ordet ”oplysning”, bortset fra når det er mere generelt brugt at vælge ”information” f.eks. i informationssikkerhed.

I forhold til det oprindelige begrebsarbejde fra 2006, hvor informationssikkerhed blev betragtet som bestående af 3 ”dele”: Fortrolighed, integritet og tilgængelighed, 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 at data er korrekte og fuldstændige, og at der ikke er foretaget uautoriseret ændringer af data
Uafviselighed	Egenskab ved oplysninger 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

[1] https://sundhedsdatastyrelsen.dk/nbs

I diskussioner om informationssikkerhed i sundhedsvæsenet har det ofte været aspektet fortrolighed, der har været fokuseret på. Den øgede fokus på gennemførelse af strukturerede risikovurderinger og det stigende pres fra ondsindede aktører har medført, at der nu foretages en mere balanceret afvejning af behovet for at tilgodese alle relevante aspekter af informationssikkerhed.

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

En sikkerhedsrisiko er en potentiel hændelse, der vurderes at kunne indtræde med en vis sandsynlighed, og som vil have en uønsket negativ påvirkning af forretningens it-aktiver. Jo større sandsynligheden er for at hændelsen indtræder, og jo større konsekvensen er for forretningen, desto 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 centrale begreber i NSIS [NSIS Version 2.0.1] er:

Identitet (elektronisk)	En digital persona repræsenteret ved et sæt af attributter, som fx kan repræsentere en fysisk person (privat- identitet), en juridisk enhed (virksomhedsidentitet), eller en fysisk person, der er associeret med en juridisk enhed (fx erhvervsidentitet). En Identitet kan rumme personidentifikationsdata men kan også være pseudonym.
Entitet	En fysisk person eller juridisk enhed, som ønsker adgang til en online tjeneste gennem Autentifikation med Elektroniske Identifikationsmidler. En Entitet kan have flere Elektroniske Identiteter – fx kan en fysisk person både have en privatidentitet og flere erhvervsidentiteter.
Sikringsniveau	Graden af tillid til en autentificeret Identitet (på engelsk "Level of Assurance") og ofte benævnt autenticitets-Sikringsniveau.
Elektronisk Identifikationsmiddel	Et middel som en Entitet får udstedt til brug for on- line Autentifikation. Midlet kan både være fysisk og virtuelt, og skal være under Entitetens kontrol. Et samlet Elektronisk Identifikationsmiddel består af ét eller flere elementer, der hver især er et enkelt elektronisk Identifikationsmiddel, som anvendes i kombination med henblik på at tilfredsstille kravene på et højere Sikringsniveau, end der kan opnås isoleret med et enkelt Elektronisk Identifikationsmiddel.

De dele af begrebssystemet, der er relevante for denne referencearkitektur beskrives nærmere i afsnit 4.2. Der er her dels tale om ret generiske begreber, der ikke er specifikke for informationssikkerhed inden for sundhedsdomænet, og dels begreber der knytter sig til Sundhedslovens bestemmelser om adgang til sundhedsdata (f.eks. indhentning, videregivelse, samtykke, aktuel behandling, værdispring, mm.).

2.6 Formålet med en referencearkitektur for Informationssikkerhed

Referencearkitekturen er overordnet set begrundet af sundhedsvæsnets forretningsmål. Den skal udgøre en arkitekturmæssig ramme for, hvordan man skal indrette løsninger, så de kan "tale sammen" og udveksle følsomme personoplysninger på en sikker og ensartet måde. Den skal medvirke til at danne rammerne for konkrete løsningsarkitekturer og byggeblokke og fungere som fælles pejlemærke for udviklingen af it-systemer til sundhedssektoren.

Referencearkitekturen skal også bidrage til standardisering af området. Herunder, at der udpeges 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.

Formålet med referencearkitektur for informationssikkerhed er derudover:

- At opsamle, fastlægge og konkretisere eksisterende viden, beslutninger, begreber, modeller og processer omkring informationssikkerhed i kontekst af sundhedsvæsnet og dermed bidrage 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.
- At give sundhedsvæsnets parter en ramme, der bidrager til at bygge løsninger, der både lever op til gældende lovgivningskrav dels er forberedt på fremtiden.

2.7 Anvendelse

Referencearkitekturen skal anvendes i forbindelse med kravspecificering af systemer og ved indgåelse af aftaler med leverandører af it-løsninger til sundhedssektoren.

Referencearkitekturen udgør den generelle ramme for it-løsninger til sundhedssektoren i forhold til informationssikkerhed.

Det er tanken at referencearkitekturen skal anvendes som guide og inspiration til arbejdet med at specificere og udvikle det danske sundhedsvæsen hen mod de fastlagte mål og strategier.

Referencearkitekturen har ikke svar på alt, og der opfordres til at man supplerer indholdet med egne erfaringer og andre relevante målbilleder og referencearkitekturer. Det er dog vigtigt at man altid tager højde for ændringer i trusler, infrastruktur, tendenser, miljø og andre parametre, der kan have indflydelse på arkitekturen.

Såfremt referencearkitekturen ikke er konsistent i forhold til andre referencearkitekturer, standarder, målbilleder eller et projekts behov, vil Sundhedsdatastyrelsen gå i dialog med parterne, så der i samarbejde kan foretages de vurderinger og valg, der er nødvendige for at skabe konsistens.

2.8 Målgruppe

Referencearkitekturen er udformet, så den kan benyttes af en lang række interessenter:

- Chefer, ledere og andre med rollen som systemejer eller systemansvarlig inden for organisationer, der skal gennemføre anskaffelser eller større ændringer af sundheds-it-løsninger.
- Organisationer, der designer it-løsninger til sundhedsvæsnet. Dette blandt andet i form af fastlæggelse af fælles sikkerhedsmodeller og referencer til nationale og internationale standarder, principper og lovgivning. Målgruppen er således også leverandører af it-løsninger, særligt deres arkitekter og udviklere.
- Organisationer, der lovgiver omkring informationssikkerhed samt fører tilsyn med at reglerne på området overholdes.
- Endelig omfatter målgruppen personer og organisationer, der udarbejder øvrige referencearkitekturer.

2.9 Læsevejledning

Referencer og links i teksten skal anvendes med forbehold for efterfølgende ændringer af lovtekst og placering af links.

2.10 Tilblivelsesproces

Det har været et bærende princip i arbejdet med referencearkitektur i sundhedsvæsenet at der skal bygges videre på det brede fundament af viden, erfaringer og resultater, som 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. I september 2013 udkom Referencearkitektur for Informationssikkerhed Version 1.0 fra National Sundheds It.

Med **National strategi for cyber- og informationssikkerhed 2018-2021** igangsattes 6 decentrale strategier for 6 udvalgte samfundskritiske sektorer, heriblandt sundhedssektoren.

Som følge af dette kom sundhedssektorens strategi 2019-2022: ”**En styrket, fælles indsats for cyber- og informationssikkerhed”.** I denne er der udpeget 17 initiativer, der i flere tilfælde består af flere del-initiativer.

Et af initiativerne (2.6) omhandler udbygning af sektorens sikkerhedsarkitektur og i forbindelse med det, hedder det bl.a.:

På tværs af sundhedssektoren skal der arbejdes ensartet med it-sikkerhedsmæssige krav, fx vedr. databeskyttelse gennem design og i forbindelse med videreudvikling af eksisterende systemer eller nyanskaffelser. For at sikre et passende og ensartet højt niveau af databeskyttelse gennem design og standardindstillinger skal sektoren lægge sig fast på et fælles sæt af metodikker og standarder, der gælder for hele sektoren. DCIS får som grundlag herfor til opgave at opdatere den samlede sikkerhedsarkitektur for sektoren inkl. fastlæggelse af standarder og udarbejdelse af værktøjer og vejledninger.

Som en del af udmøntningen af dette initiativ er det valgt, at den eksisterende Referencearkitektur for Informationssikkerhed, Version 1.0. skal revideres.

I forbindelse med arbejdet med revisionen er der afholdt et antal arkitekturworkshops med deltagere fra flere interessenter blandt sundhedsvæsenets parter og leverandører.

3 Strategiarkitektur

3.1 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.

Sikkerhed er i stor grad implementeret ved at sikre netværksperimeteren, og selv om der er flere forbedrings-initiativer i gang, er det en lang, sej og dyr kamp. Der findes centrale løsninger inden for sundhedssektoren, men disse er traditionelt beskyttet på en lignende måde. Denne situation er udfordret gennem en række krav og ønsker. Disse er blandt andet større sammenhæng mellem løsninger og stadig større åbenhed mod og udveksling af data med ikke sikrede miljøer, fx indhentning af data direkte hos borgeren. Alle forhold som stiller krav om en mere differentieret sikring, større anvendelse af trust, mere sikre identiteter og øget fokus på datakvalitet.

Det nuværende sikkerhedsmæssige niveau i sundhedsvæsenet er kun i begrænset omfang understøttet af fælles begreber og en fælles ramme for informationssikkerhed. Specielt set i forhold til planlagte og igangværende initiativer til at ændre den samlede sikkerheds- og informationsarkitektur.

Der findes fælles sikkerhedsløsninger for sundhedssektoren, for eksempel løsningerne på Den Nationale Serviceplatform (NSP), men der er også en forståelsesmæssig erkendelse af behovet for bredere løsninger - både for at kunne udveksle data med flere parter, herunder parter uden for sundhedssektoren, og for at imødegå det ændrede trusselbillede, der bl.a. er afledt af både interne og eksterne trusler. Det kan være alt fra data fra IOT-enheder til cybersikkerhed generelt.

Single sign-on er i større eller mindre grad implementeret i de forskellige organisationer inden for sundhedssektoren. Udbredelsen er i høj grad styret af, i hvilken grad de enkelte systemer, der indgår i den samlede systemportefølje, understøtter single sign-on direkte eller tilbyder mulighed for gennem tredjepartmoduler at indgå i single sign-on set up.

På tværs af sundhedsvæsenets parter er det generelt meget begrænset, hvad der er sket af tiltag for at etablere fælles løsninger. Lovgivning og aftaler mellem parterne om at følge fælles standarder (som eksempelvis ISO 2700x) og fælles vejledninger har skabt en vis ensretning, men denne er sket på et så overordnet niveau at der reelt ikke er tale om et fælles sikkerhedsniveau og ensartet sikkerhedshåndtering sundhedsvæsenets parter imellem.

Udveksling af patientoplysninger mellem sundhedsvæsenets parter sker hovedsageligt ved, at der sendes beskeder fra et system til et andet (på et givet tidspunkt bestemt af afsendersystemet). Det er afsendersystemet, der har ansvar for at sikre, at oplysningerne må videregives. Modtagersystemet lagrer herefter de indkomne oplysninger lokalt og adgangen til disse oplysninger styres af den af modtagersystemet anvendte sikkerhedsløsning. Typisk er det sådan at sikkerheden ikke følger data, men styres lokalt.

Tilgængeligheden af data er høj for dem, der skal anvende data, når data lagres lokalt i modtagersystemet. Omvendt kan det være svært at sikre aktualitet, korrekthed og integritet af data, når data distribueres til

flere systemer. Det er afsendersystemet, som skal holde styr på, hvilke systemer, der har modtaget hvilke data og sende rettelser til disse. Desuden skal modtagersystemet kunne modtage og håndtere opdateringerne.

Der er et stadig stigende behov for integration af medico-løsninger og mindre lokale løsninger. De er arkitekturmæssigt typisk bygget til at blive driftet i "isolerede" miljøer eller er ofte bygget på ældre teknologier/platforme. Det medfører øgede udfordringer med at skabe et konsistent og sammenhængende sikkerhedsniveau.

Risikobilledet ændres ved etablering af sådanne systemintegrationer. Det enkelte system giver nu ikke bare adgang til egne (lokale) data, men kan principielt være indgang til indhentning af andre data registreret om den enkelte patient. Det er derfor nødvendigt at revurdere, om de eksisterende sikringsforanstaltninger er tilstrækkelige.

Øget samarbejde og deling af data gør, at ansvarsforhold bliver mere komplekse. Den dataansvarlige organisation er altid ansvarlig for at sikre, at kun autoriserede personer får adgang til de nødvendige patientdata. Men hvor det tidligere kun var medarbejdere i egen organisation, der kunne få adgang til data, er det nu ofte også medarbejdere fra andre organisationer, der skal kunne få adgang. For at gøre det muligt for den enkelte dataansvarlige at opnå en tilstrækkelig sikkerhed for autorisationen af disse eksterne medarbejdere, skal der etableres et tillidsforhold til samarbejdsparterne, så den enkelte dataansvarlige kan give andre organisationers medarbejdere adgang, under forudsætning af, at den anden organisation kan garantere, at de har autentificeret og autoriseret deres brugere behørigt.

Referencearkitektur for brugerstyring[2] behandler problemstillingen, og regionerne har allerede samarbejder baseret på fødererede løsninger.

Dette skaber dog ikke altid den nødvendige overensstemmelse. De forskellige lokale systemer håndterer for eksempel adgangsforholdene ret forskelligt, alt efter hvilke paradigmer og regelsæt der har været herskende, da de blev udtænkt. Der findes i dag ikke en standardiseret måde til at validere brugeradgange og foretage sikkerhedsmæssige kontroller.

Så længe adgangen til data er baseret på forskelligartede sikkerhedshåndtering i anvendersystemerne, vil sikkerheden ikke være højere end den til enhver tid svageste sikkerhedshåndtering blandt anvendersystemerne. Brydes sikkerheden i det svageste system, er der risiko for at dette kan bruges til at skaffe sig adgang til fortrolige og følsomme persondata nationalt.

Opsummerende, er den nuværende situation kendetegnet ved følgende:

- Der er ikke implementeret et fælles nationalt, dokumenteret sikrings- og sikkerhedsniveau.
- Sundhedspersoner hos forskellige parter har ikke nødvendigvis samme adgang til data, selvom de løser samme opgave.
- Patienten kan ikke være sikker på, at alle relevante oplysninger registreret om vedkommende er tilgængelige, hvor de skal bruges.

[2] https://arkitektur.digst.dk/node/123

- Patienten har ikke samme tekniske 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 meget forskellige sikkerhedsmodeller.
- Der er kun få fælles løsninger, der understøtter dataudveksling i højere grad og interoperabilitet mellem systemer.

3.2 Tendenser

3.2.1 Overordnede socioøkonomiske tendenser

Øget og stadig stigende fokus på privatlivsbeskyttelse: Databeskyttelsesforordningen trådte i kraft 25. maj 2018 og medførte skærpet opmærksomhed på hele databeskyttelsesområdet. Samtidig har indførslen resulteret i øget opmærksomhed omkring den dataansvarliges rolle og forpligtelser. Databeskyttelsesforordningen har ikke influeret direkte på sundhedsloven.

Systemlandskabet ændres: Skarpe grænser nedbrydes, og der etableres mere eller mindre integrerede organisatoriske og tekniske landskaber med stadigt mere flydende og dynamiske grænseflader. De veldefinerede tekniske landskaber, hvor der er sikkerhedsmæssigt kontrol med alle enheder, erstattes af fødererede landskaber, der i langt højere grad baseres på begrundet tillid. Der indgår enheder og snitflader, der er potentielt usikre, men som på grund af fleksibilitet og tilgængelighed skal indgå i det samlede landskab, fx gamle u-supporterede men nødvendige systemer, der skal indgå sammen med nye integrerede løsninger. Heraf følgende risici og konsekvenser, der har direkte indvirkning på tilgængelighed, integritet og fortrolighed og skal imødegås af både organisatoriske og tekniske kontroller.

Borgerne bør inddrages endnu mere: Borgerne inddrages i større omfang i egen behandling og i kommunikation med sundhedsvæsenet. Dette sker ofte gennem kanaler, der ikke er de samme som de primært anvendte af sundhedsvæsenet. Specielt Covid-19-pandemien i 2020/2021 har gjort det tydeligt, hvor mange henvendelser, der kan klares med IT-tekniske hjælpemidler. Før pandemien blev der arbejdet meget på forbedring i forhold til håndtering af kroniske sygdomme ved brug af dataopsamling fra medicotekniske enheder i hjemmet og kommunikation via mobile enheder. Under pandemien blev dette arbejde øget, og andre internetbaserede kommunikationsformer blev hastigt taget i brug. Når sundhedsvæsnet modtager og bruger data fra borgerne eller udstyr, der bruges af borgerne, opstår der nye risici. Det er endvidere vigtigt at skabe sig et overblik over lovgivningen i forhold til eventuelle ansvarsproblematikker, når borgerne involveres aktivt i egen behandling og opsamling af data, eksempelvis via medicinsk udstyr eller hvis der benyttes usikre kommunikationsformer.

Borgerne leverer egne sundhedsdata: Ud over de autoriserede telemedicinske løsninger, der benyttes mere og mere i behandling af specielt kroniske lidelser, opsamler borgerne til stadighed større og større mængder sundhedsdata gennem egne enheder, f.eks. smartphones, smart-watches og lignende elektronisk udstyr, hvis data måske forventes at kunne anvendes af sundhedsvæsenet i behandlingssituationer. Brugen af uautoriseret udstyr medfører dog øget risiko for fejl i datagrundlaget. Tilliden til sikkerheden på udstyret, netværket og kilden for disse data er af afgørende betydning for, hvordan disse data kan benyttes. Ukritisk

brug af fejlbehæftede eller manipulerede data kan have fatale følger, og sundhedspersoner skal være opmærksomme på at validere data, inden de benytter dem som input i behandlingsøjemed.

Internationalisering: I takt med den øgede digitalisering af sundhedssektoren, således også i resten af verden, opstår der mulighed og behov for samarbejder på tværs af nationer. Som effekt deraf vokser udbuddet af systemer og digitale enheder. Sundhedsvæsenets parter må derfor orientere sig om internationale standarder og være klar til at kunne integrere med udenlandske parter. GDPR- og eIDAS-forordningerne er eksempler på europæiske standarder, som skal fremme borgere og virksomheders muligheder for at anvende elektroniske tjenester på tværs af EU's indre grænser, og der arbejdes blandt andet på en Europæisk forordning for sundhedsdata (EHDS), der skal give større bevægelsesfrihed for borgere og data, samt på et direktiv om cyber-og informationssikkerhedskrav til udvalgte samfundsvigtige sektorer.

Covid-19 pandemien, der startede sidst i 2019, satte sundhedsvæsenets it-systemer under pres. Den viste at der, på trods af beredskabs øvelser og risikovurderinger, ikke var kapacitet til at håndtere et stigende pres på den eksisterende infrastruktur, og at der ikke var sikkerhedssystemer og beskyttet infrastruktur til rådighed for de nødvendige supportsystemer. Eksempelvis tidsbestilling til Corona-test, selve testprogrammet og efterfølgende vaccinationsprogram, hvor mange midlertidigt ansatte havde et behov for adgang til persondata, som ikke umiddelbart kunne håndteres af de eksisterende metoder.

3.2.2 Sikkerhedsmæssige tendenser

Cybertrusler: Risikoen for at blive ramt af en form for cyberangreb er stor, og cyberkriminelle, herunder statsstøttede aktører, bliver stadig mere målrettede og sofistikerede i deres metoder. Det afføder store krav til robusthed, fleksibilitet og vedligeholdelse af sektorens systemlandskab for til stadighed at kunne afværge trusler og håndtere sårbarheder. Der udgives jævnligt risikobilleder og trusselsvurderinger både nationalt og i forhold til kritiske sektorer såsom sundhedssektoren. Desuden er der kommet flere internationale samarbejder og netværk, hvor myndigheder og virksomheder kan udveksle oplysninger og værktøjer relateret til trusler, sårbarheder og aktuelle angreb.

Øget afhængighed af IT: Sundhedsvæsenet oplever en stadig stigende afhængighed af IT-systemer og datakommunikationsservices. Der deles data mellem sundhedsvæsenets aktører, der oprettes centrale nationale sundhedsdatabaser, og borgerne har i mange tilfælde adgang til deres data via internet og mobile apps. Den danske datakommunikationsinfrastruktur er en kritisk faktor for det moderne sundhedsvæsen, men tilgængeligheden er udfordret af forskellige former for cybertrusler. Disse trusler forstærkes af ikke tidssvarende infrastruktur, der især kan give problemer ved større byggeprojekter, f.eks. supersygehusene. Med den øgede afhængighed fører også en stigende sårbarhed over for nedbrud, uanset om det skyldes fejl i hardware eller software, eller om det skyldes ondsindede handlinger. Det medfører også et behov for øget fokus på rettidig omhu.

Fortroligheden og integriteten er truet, dels på internettet, hvor krypteringsalgoritmer brydes, men også på lejede data-forbindelser, faste kredsløb og farvede eller sorte fibre, der kan aflyttes. Det stiller krav til øget kryptering af både interne og eksterne dataforbindelser eller datastrømme samt løbende vedligeholdelse af krypteringsalgoritmer og certifikater.

Medicoteknisk udstyr kobles på de centrale netværk og indgår efterhånden på linje med andet IT-udstyr, der skal kunne kommunikere med hinanden og tilgås alle steder fra. Det giver en række udfordringer, da den teknologiske levetid for selve udstyret ofte er længere end for det tilkoblede IT-udstyr og de anvendte operativsystemer. Hermed opstår en række sårbarheder, der er meget dyre eller direkte umulige at komme af med.

Mobile enheder: I takt med at aktørerne i sundhedsvæsenet i større og større grad deler data med hinanden og med borgerne, opstår der også et krav om at have data tilgængelige til alle tider og på alle typer enheder. Både klinikere og borgere forventer at kunne tilgå mobilversioner af sundhedssystemerne fra smartphones og tablets. Det medfører en del sikkerhedsudfordringer, idet disse enheder er vanskelige at sikre, nemme at miste, og kan indeholde følsomme oplysninger.

IOT: En anden form for enheder er netværksforbundne enheder med specifik funktionalitet. De betegnes IOT-enheder og indgår i konceptet kaldet "Internet Of Things". Disse er typisk udviklet til et givent formål, f.eks.:

- elektrisk pære, der kan fjernstyres fra telefonen med hensyn til farve og lysstyrke,
- fjernstyret kaffemaskine
- robotstøvsuger, der kan startes og administreres fra telefonen
- udstyr til hjemmemåling og rapportering af ekg
- apparater til hjemmemåling og rapportering af blodtryk og puls
- mobil enhed, der kan overvåge og dosere insulin

Føderationer: Der er en igangværende bevægelse mod at organisationer indgår i føderationer og i større udstrækning baserer sig på trustrammeværk. Dette understøttes af standardiseringstiltag og dansk profilering af internationale standarder. Digitaliseringsstyrelsen har i 2020 udgivet en revideret version af referencearkitektur for brugerstyring[3] og Sundhedsdatastyrelsen har udgivet et målbillede for sammenhængende brugerstyring[4]. MitID- og NemLog-in3-initiativerne ændrer den danske digitale identitetsinfrastruktur fra at være en centraliseret infrastruktur til at være en distribueret sikkerhedsarkitektur med flere aktive parter, som i høj grad er baseret på trust mellem de forskellige aktører.

AI og robotics: AI og robotics er i hastig fremdrift og drives i stor grad af teknisk udvikling men åbner en række sikkerhedsmæssige problemstillinger omkring data, datakvalitet og dataansvar, som skal adresseres. For eksempel kan anvendelse af AI i behandlingsmæssig beslutningsstøtte medføre personskade, hvis der ikke er tilstrækkelig kontrol og validering. Digitaliseringsstyrelsen har udgivet en vejledning: "Tiltag til at sikre brugen af kunstig intelligens"[5]

---

[3] https://arkitektur.digst.dk/sites/default/files/Referencearkitektur%20for%20brugerstyring%20version%201_1_FINAL.pdf

[4] https://dksund.sharepoint.com/sites/Mlbilledefortillidstjenesterogtillidsrelationer/Delte%20dokumenter/M%C3%A5lbillede%20for%20sammenh%C3%A6ngende%20brugerstyring/M%C3%A5lbillede_for_sammenh%C3%A6ngende_brugerstyring-v1.1.1.pdf#search=m%C3%A5lbillede%20for%20sammenh%C3%A6ngende%20brugerstyring

[5] https://sikkerdigital.dk/media/11401/vejledning-tiltag-til-at-sikre-brugen-af-kunstig-intelligens-2020.pdf

3.3 Vision

Den store overskrift for strategi for digital sundhed 2018 - 2024 er:

Ét sikkert og sammenhængende sundhedsnetværk for alle.

Og en del af indledningen til strategien udtrykker netop en vision:

> **Strategien skal sikre den fortsatte bevægelse mod en mere helhedsorienteret indsats, hvor hospitaler, kommunale sundhedstilbud, praksissektor og andre offentlige og private aktører i hele sundhedsvæsenet kan samarbejde i et integreret netværk om og med borgeren i centrum. Strategiens overordnede sigte er at understøtte sundhedsaktører i at løfte deres ansvar for at skabe sammenhæng på tværs af de enkelte kontakter. Flere opgaver kan med digitalisering løses tæt på borgeren i et nært og sammenhængende sundhedsvæsen, der ser på det hele menneske og ikke kun på den enkelte diagnose.**

"Nationale mål for sundhedsvæsenet" defineres af én tydelig overligger: Bedre sammenhæng, kvalitet og geografisk lighed i sundhedsvæsenet. Og for de otte mål, som tilsammen skal løfte overliggeren, er digitalisering på visse områder en vigtig brik – og på andre områder den afgørende driver for forandring. Udviklingen af et sundhedsvæsen med bedre kvalitet, geografisk lighed og øget sammenhæng på tværs af enheder, fag, specialister og andre aktører kræver, at der fortsat investeres i den digitale infrastruktur, så der kan skabes flow i de forløb, borgeren indgår i. Derfor spiller digital udvikling en afgørende rolle, når det kommer til at videreudvikle vores sundhedsvæsen som ét reelt sammenhængende netværk.

Informationssikkerhed er en grundlæggende forudsætning for at sundhedsvæsenet kan fortsætte den igangværende digitalisering på tværs af sundhedsområdet. Men nationale og internationale standarder skal også være på plads, for at vi kan opnå de ønskede tværgående gevinster og nå helt ud til borgerne med tillidsvækkende løsninger, der er både let anvendelige, tilgængelige, troværdige og sikre. I det ligger også, at vi skal sikre både data og funktionalitet, så det er robust over for de konstant stigende og foranderlige trusler fra personer og organisationer med ondsindede hensigter.

3.4 Forretningsmæssigt målbillede

Hvor visionen udpeger de langsigtede og overordnede mål for området, så er det forretningsmæssige målbillede udtryk for, hvad man forventer at kunne opnå inden for de næste 3-5 år.

Det kan ikke forventes at alle tekniske, organisatoriske eller semantiske barrierer for det digitale samarbejde på tværs af sundhedsvæsenet kan adresseres inden for denne tidshorisont. Dette afspejler sig i, at målbilledet både omhandler kortsigtede gevinster såvel som en styrkelse af arbejdet med at sammentænke de digitale løsninger og bygger på en fælles digital infrastruktur, der kobler IT-systemerne sammen.

Forudsætningen herfor er, at der specificeres og udvikles et sæt fælles byggeblokke, der er åbne og leverandøruafhængige og dermed understøtter en bred og fleksibel anvendelse.

Et af de væsentligste formål med referencearkitekturen er derfor at danne rammen for fastlæggelse af standarder for arbejdet hen mod et sikkert og sammenhængende sundhedsnetværk for alle, som det er udtrykt i strategien for digital sundhed 2018-2022[6]

3.5 Referencearkitekturens værdiskabelse

Værdiskabelsen for referencearkitekturen for informationssikkerhed sker gennem anvendelse af den i alle projekter og opgaver i sundhedssektoren. De enkelte afsnit og emner i referencearkitekturen bidrager hver med værdielementer for informationssikkerheden.

Referencearkitekturen for informationssikkerhed skal danne grundlag for udvikling af sikkerhedsmodeller, der dels sikrer sikkerhedsmæssig sammenhæng og interoperabilitet på tværs af føderationer, dels gør det enklere og billigere at etablere nye fælles it-løsninger med et tilstrækkeligt sikkerhedsniveau.

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.
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 nødvendige oplysninger til understøttelse af behandlingen i primær og sekundær sektor. Borgernes retsstilling sikres bedst gennem ensartede principper for hvilke personer, der har adgang til patienternes data og hvorledes samtykker kan afgives, samt i relation til hvem og med hvilken afgrænsning af data.
Ensartede sikkerhedskrav til løsninger	Gør det lettere for leverandører at udvikle sammenhængende løsninger med genbrugelige sikkerhedskomponenter. Forenkler opgaven med at kravspecificere individuelle og sammenhængende løsninger.

[6] https://sundhedsdatastyrelsen.dk/-/media/sds/filer/strategi-og-projekter/strategi-digital-sundhed/strategi-for-digital-sundhed-2018_2022.pdf

Fælles forståelse og rammer	Der skabes et bedre grundlag for samarbejde på tværs af offentlige myndigheder, således at myndighederne arbejder sammen om standarder og løsninger, der ligger i forlængelse af arbejdet med informationssikkerhed.
Genbrug og anvendelse af fælles komponenter	Hurtigere og billigere udvikling af løsninger. Nye informationskilder "tilkobles" hurtigere og mere omkostningseffektivt den samlede mængde af tilgængelige oplysninger.
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. Bedre interoperabilitet
Referencearkitekturens operationalisering af gældende lovgivning	Der skal bruges mindre tid og færre ressourcer på at sikre, at it-løsninger lever op til persondatalovens og sundhedslovens krav.
Genbrug af modeller og byggeblokke	Gør det lettere at dokumentere overholdelse af lovkrav overfor de relevante myndigheder (f.eks. Datatilsynet) og revision
Standardisering af og genbrug af registreringer	Letter administration af brugere og rettigheder

4 Forretningsarkitektur

4.1 Principper

4.1.1 Baggrund

Alt arkitekturarbejde bør orientere sig om de retningslinjer, regler og lover, der eksisterer på området. En del af disse kan udtrykkes i principper. Vi har valgt at medtage de principper, det danske datatilsyn har udformet for at hjælpe den dataansvarlige med at overholde databeskyttelsesforordningens krav.

Arkitekturprincipper skal udgøre en oversættelse imellem forretningsdomænet og teknikdomænet. De bruges i den daglige styring af arbejdet med at udforme de it-systemer og komponenter, som skal hjælpe forretningen med at realisere sine strategiske målsætninger. Det skal med andre ord være muligt med dette sæt af principper i hånden at beslutte sig for, hvilken af flere alternative løsninger, der i en given situation er den bedste. Listen er baseret på listen over principper der er medtaget i dokumentet "Arkitekturprincipper for sundhedsområdet[7]"

4.1.2 Databeskyttelsesretlige principper

Databeskyttelsesforordningens artikel 5 indeholder seks grundlæggende principper som dataansvarlige altid skal overholde, og som derfor også har relevans i forbindelse med referencearkitekturen:

1. **Lovlighed, rimelighed og gennemsigtighed**: Behandlingen skal overholde databeskyttelsesreglerne og være gennemsigtig
2. **Formålsbegrænsning**: Ved indsamling skal det være klart hvilke saglige formål, oplysningerne skal anvendes til. Senere behandling må ikke være uforenelig med disse formål
3. **Dataminimering**: Behandling, herunder opbevaring af oplysninger, skal begrænses til det, der er nødvendigt for at opfylde formålet
4. **Rigtighed**: Oplysninger skal ajourføres, og urigtige oplysninger skal slettes eller berigtiges
5. **Opbevaringsbegrænsning**: Når det ikke længere er nødvendigt at behandle oplysningerne, skal de anonymiseres eller slettes
6. **Integritet og fortrolighed**: Oplysninger må ikke komme til uvedkommendes kendskab, gå tabt eller blive beskadiget

[7] https://sundhedsdatastyrelsen.dk/-/media/sds/filer/rammer-og-retningslinjer/referenceaktitektur-og-it-standarder/referencearkitektur/arkitekturprincipper_version-2,-d-,0.pdf

4.1.3 Referencearkitekturens principper

Nedstående er de principper vi har valgt at tage med i denne referencearkitektur.

Principper for forretningsarkitektur
F2: Internationale, nationale og lokale initiativer skal koordineres med henblik på genbrug af såvel nye som allerede etablerede løsningselementer, standarder og infrastruktur
F3: Fælles løsninger skal respektere, at samarbejdet sker mellem uafhængige juridiske enheder, som kan have egne regler, retningslinjer og processer
F6: Løsninger, der produktionssættes, bør baseres på komponenter, der er driftsmodnede og har gode referencer fra andre anvendere/projekter
Principper for informationsarkitektur
I1: Ved deling af information fastlægges entydigt ansvar
I2: Deling af struktureret information forudsætter fælles begrebsforståelse
I4: Information opsamles én gang og genanvendes i alle relevante sammenhænge i overensstemmelse med regler for visning og anvendelse
I5: Effektive foranstaltninger forebygger risici fremfor at afhjælpe dem.
I6: Databeskyttelse implementeres som standardindstilling
I7: Databeskyttelse designes ind i systemers arkitektur fra starten.
Principper for applikationsarkitektur
A2: Overvej opsplitning af store, komplekse systemer i mindre, simplere komponenter, der kan udvides på længere sigt.
A3: Applikationer og komponenter skal kunne indgå i et nationalt økosystem for sundhedsvæsenet.
A4: Passende databeskyttelse skal afpasse funktionaliteten, så både den ønskede funktionalitet og den nødvendige sikkerhed understøttes.
A5: Det sikreste sted at beskytte data er ved kilden.
Principper for teknisk arkitektur
T1: Anvend fælles infrastrukturkomponenter til effektivt at sikre et ensartet og højt sikkerhedsniveau i kommunikation mellem parter

T2: Teknisk interoperabilitet opnås gennem anvendelse af udbredte, åbne standarder
T3: Uafhængighed af leverandører styrkes ved anvendelse af bredt understøttede teknologier
T4: Non-funktionelle krav indtænkes fra starten
T5: Den nationale infrastruktur er standardiseret og ansvaret for at integrere hertil ligger lokalt
T6: Driftsmæssig kontinuitet af komponenter og services, som indgår i den nationale infrastruktur, skal sikres
T7: Optimale sikringsforanstaltninger måles og forbedres løbende for at sikre kvalitet og effektivitet

Principperne uddybes nærmere i afsnit 5.1(Appendiks)

Endvidere har Digitaliseringsstyrelsen udgivet et sæt fælles arkitekturprincipper.[8]

4.2 Begreber

4.2.1 Referencearkitekturens begreber

Sundhedsvæsenet arbejder ud fra et væld af ord og begreber, hvis betydning og indbyrdes forhold, af hensyn til patienter, ansatte, processer etc., skal være helt tydelige. Begrebsforvirring kan være årsag til mange misforståelser. Derfor opbygges der ofte begrebsmodeller for at sikre en ensartet opfattelse af betydningen af et givet ord eller udtryk.

4.2.2 Hvad er en begrebsmodel?

En begrebsmodel beskriver begreber ved hjælp af deres karakteristiske træk og deres indbyrdes relationer. Begrebsmodellen 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 begrebsmodel 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.

[8] https://arkitektur.digst.dk/principper-og-regler

- Dialogforbedring mellem fagekspert og it-udvikler gennem entydigt og veldefineret grundlag.

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

4.2.3 Kilder og afgrænsning

Der eksisterer en række kilder, der på forskellig vis beskæftiger sig med begrebsmodeller eller centrale begreber inden for informationssikkerhed. Nedenfor gennemgås udvalgte kilder, der er fundet relevante i forhold til nærværende referencearkitektur.

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

NBS har i 2006 udarbejdet et terminologisk begrebssystem for informationssikkerhed [NBS][9]. Da arbejdet er gennemført i 2006, er indholdet her vurderet i forhold til aktualitet for informationssikkerhed med den konklusion, at det indholdsmæssigt stadig er validt. Samtidig udgør den et samlet bud på en begrebsmodel for informationssikkerhed. Endvidere er begreber herfra inkluderet i Sundhedsvæsenets begrebsbase (NBS).

Vejledning om it-risikostyring og -vurdering, Digitaliseringsstyrelsen, februar 2015

Dette arbejde fokuserer på en del af en samlet begrebsmodel, nemlig den del, der beskriver sikkerhedsrisici samt vurdering og styring af disse. Om end et af formålene med vejledningen er at introducere væsentlige begreber og terminologi inden for risikovurdering, indeholder vejledningen ikke egentlige definitioner og terminologiske begrebsmodeller men refererer til ISO 27001 og ISO 27005.

National Standard for Identiteters Sikringsniveauer (NSIS)[10]

Formålet med NSIS er at skabe rammer for tillid til digitale identiteter samt digitale ID-tjenester og definerer nødvendige begreber for, at en tjenesteudbyder kan definere kravene til ønsket sikringsniveau for brugerne baseret på en risikovurdering.

Referencearkitektur for brugerstyring[11]

Referencearkitektur for brugerstyring beskriver arkitektur for administration og kontrol af brugere, identifikationsmidler og adgang til forretningstjenester og omfatter en terminologisk begrebsmodel med tilhørende definition af begreber.

[9] https://sundhedsdatastyrelsen.dk/nbs
[10] https://digst.dk/it-loesninger/standarder/nsis/
[11] https://arkitektur.digst.dk/referencearkitekturer/brugerstyring/referencearkitektur-brugerstyring

4.2.4 Princip for afgrænsning

Sigtet for nærværende arbejde er ikke at skabe en begrebsmodel for informationssikkerhed "fra bunden". Modellen er baseret på eksisterende arbejde i det omfang, det har været muligt. Kun relevante dele af eksisterende arbejde er uddraget med henblik på at tjene referencearkitekturens formål.

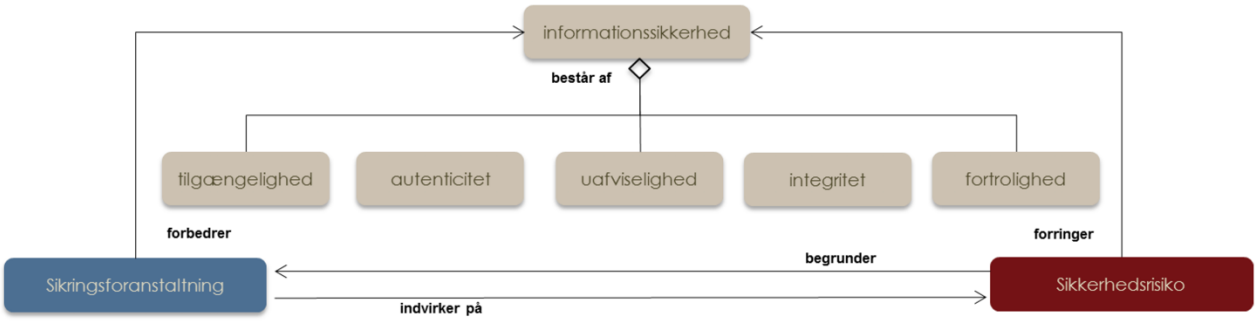
Med andre ord fastlægges her kun betydningen af centrale begreber, som er relevante for formålet med nærværende referencearkitektur. I det omfang det har været nødvendigt, er modellen udbygget eller tilrettet i forhold til de eksisterende modeller, der tages udgangspunkt i.

På en del områder kan det være vanskeligt at lave en præcis afgrænsning, da sikkerhedsområdet løbende får større og større betydning.

Der henvises derfor endvidere til Sundhedsdatastyrelsens generelle standarder og referencearkitekturer.[12]

Begrebsmodellen for informationssikkerhed

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



Figur 5: Begrebsmodel for informationssikkerhed på øverste niveau

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

[12] https://sundhedsdatastyrelsen.dk/da/rammer-og-retningslinjer/om-referencearkitektur-og-standarder/referencearkitekturer

Figur 6 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 6 - 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.

Sondringen 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 kan 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

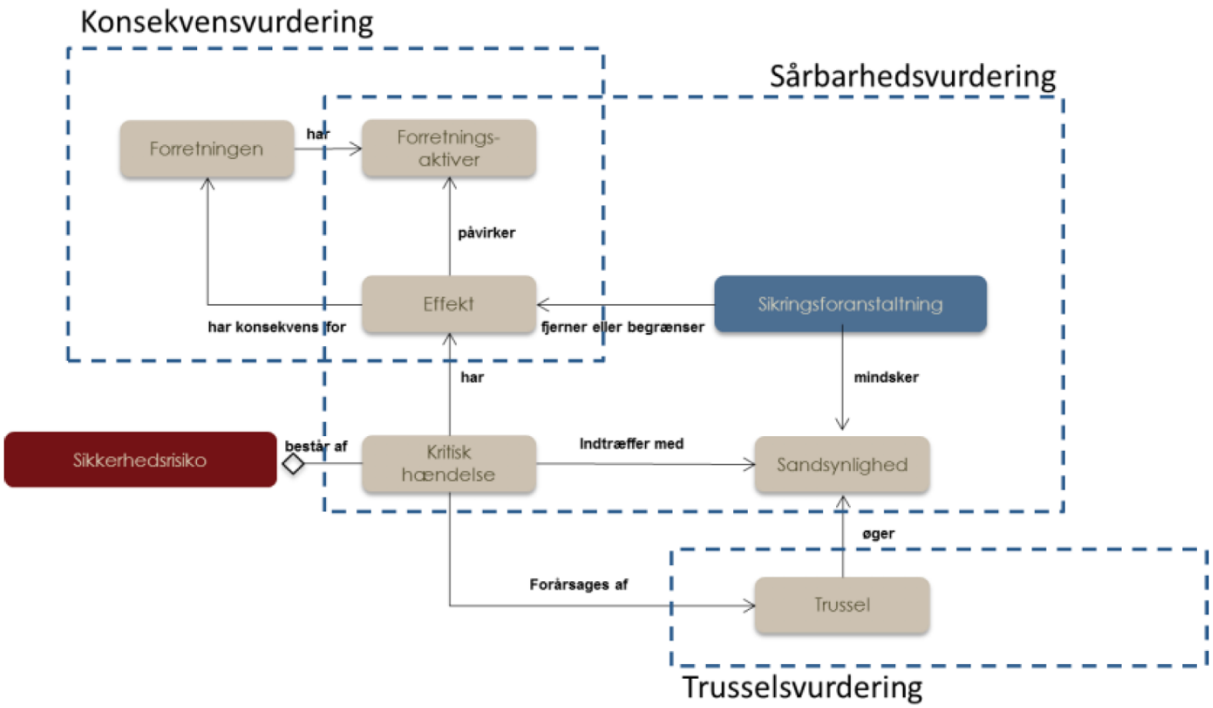
- Herunder revision

Disse begreber er endnu ikke indarbejdet i modellen.

Indtil nu har fokus været på den ene side af informationssikkerhed (sikringsforanstaltningerne). Skal den anden side vurderes (sikkerhedsrisici), kan der tages udgangspunkt i Digitaliseringsstyrelsens "Vejledning til risikostyring inden for informationssikkerhed"[13]. Denne baseres på ISO 27005 og ISO 31000.

Vejledningen beskriver risikovurdering som bestående af konsekvensvurdering, trusselsvurdering og sårbarhedsvurdering. Konsekvensvurderingen er med til at kortlægge, hvad sikkerhedsbrud inden for 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 7:



Figur 7 - Begreber, som indgår i risikovurdering

[13] https://sikkerdigital.dk/media/12268/vejledning-til-risikostyring-inden-for-informationssikkerhed-2020.pdf

Ved trusselsvurderingen anbefales det at tage udgangspunkt i ISO 27005 herunder 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 for nærværende ikke indarbejdet i modellen.

I næste afsnit uddybes betydningen af en række begreber, idet de anvendes i beskrivelser af forretningsprocesser. Begreberne vil senere blive indarbejdet i den samlede begrebsmodel. En række af begreberne med definition er vedlagt som Bilag B – Begreber.

4.3 Forretningsprocesser vedr. Informationssikkerhed

Kortlægning af forretningsprocesser i sundhedsvæsenet vil kunne bidrage til at vurdere, hvilke processer der er mest kritiske for understøttelse af patientbehandlingen og dermed bidrage til at klarlægge, om de eksisterende sikringstiltag er tilstrækkelige eller bør suppleres.

Der findes i dag ikke en central og autoritativ oversigt over forretningsprocesser i sundhedsvæsenet, og nedenstående liste er et forsøg på at klarlægge de processer, der er mest almindelige og hyppigt forekommende.

Nærværende kapitel er stort set arvet fra første version af referencearkitekturen. Andre initiativer i strategien har til opgave at klarlægge de samfundskritiske processer og disses understøttende systemer og den tilhørende infrastruktur, så det vil være hensigtsmæssigt at tage dette kapitel op til revision i en senere udgave af dokumentet.

4.3.1 Den Kliniske brugers processer

- Forespørgsel på patientoplysninger (indhentning af personoplysninger)
- Kommunikation med andre parter (videregivelse af personoplysninger)
- Inddatering af patientdata
- Ind-skanning
- Manuel inddatering af data
- Kontrol af måledata
- Delegering af arbejdsopgaver / arbejdsfunktion
- Indberetning af data til forskning og kvalitetssikring

4.3.2 Automatisk processer

- Automatisk Indhentning af måledata
- Automatisk kontrol af måledata

4.3.3 Borgerens/patientens processer

- Registrering af egne oplysninger
- Involvering i egen behandling
- Involvering i behandlingens planlægning
- Adgang til logoplysninger (MinLog)
- Adgang til en pårørendes oplysninger
- Administration af samtykkeoplysninger
- Administration af fuldmagtsoplysninger
- Hjemmemonitorering
- Borgeren kommer med egne målte data

4.3.4 Administratorernes processer

- Administration af akkreditiver
- Administration af arbejdsfunktioner (inkl. delegering)
- Administration af systemspecifikke rettigheder
- Administration af organisationsoplysninger
- Administration af brugere med ansættelsesforhold og arbejdsfunktioner

4.3.5 Governance-processer

- Styring af adgang til patientoplysninger (adgangskontrol)
- Logning af adgangen til patientoplysninger
- Opfølgning på adgangen til patientoplysninger
- Opfølgning og kontrol i forhold til kvalitetssikring og afregning
- Ledelsesinformation
- Beredskabs planlægning

4.4 Lovgivning og sikkerhed i forbindelse med processer

Lovgivning og sikkerhed i forbindelse med processer hvor sundhedspersoner indhenter patientoplysninger

Når processerne skal konkretiseres, er der mange regelsæt som den dataansvarlige skal orientere sig i forhold til. Hvis der er tale om sundhedspersoners (eller disses medhjælps) indhentning og videregivelse af oplysninger i og fra patientjournaler, er dette særligt reguleret i sundhedsloven. Samtidig findes der regler om den konkrete journalføring i medfør af autorisationsloven, der skal overholdes. Der kan tillige findes regler om indhentning af oplysninger fra andre parter i medfør af fx servicelov samt retssikkerhedslov. Hertil kommer, at den enkelte medarbejder er underlagt den almindelige ledelsesret. Således kan en indhentning af oplysninger i en patientjournal eller fra andre parter være omfattet af flere forskellige særlove på samme tid. Alle særlove er samtidig reguleret på en måde, hvorpå de er i overensstemmelse med reglerne i databeskyttelsesloven og -forordningen, da disse regler altid vil gælde for behandling af personoplysninger.

Dette afsnit indeholder et eksempel på et beslutningstræ, der viser hvilke spørgsmål, der skal tages stilling til og hvilken lovgivning, der regulerer de forskellige situationer. Eksemplet er taget fra "Målbillede for samtykke og frabedelse i forbindelse med databehandling på sundhedsområdet."[14]

Specielt "Bilag 2"[15] til denne der gennemgår 7 scenarier for videregivelse og indhentning af sundhedsoplysninger i det danske sundhedsvæsen.

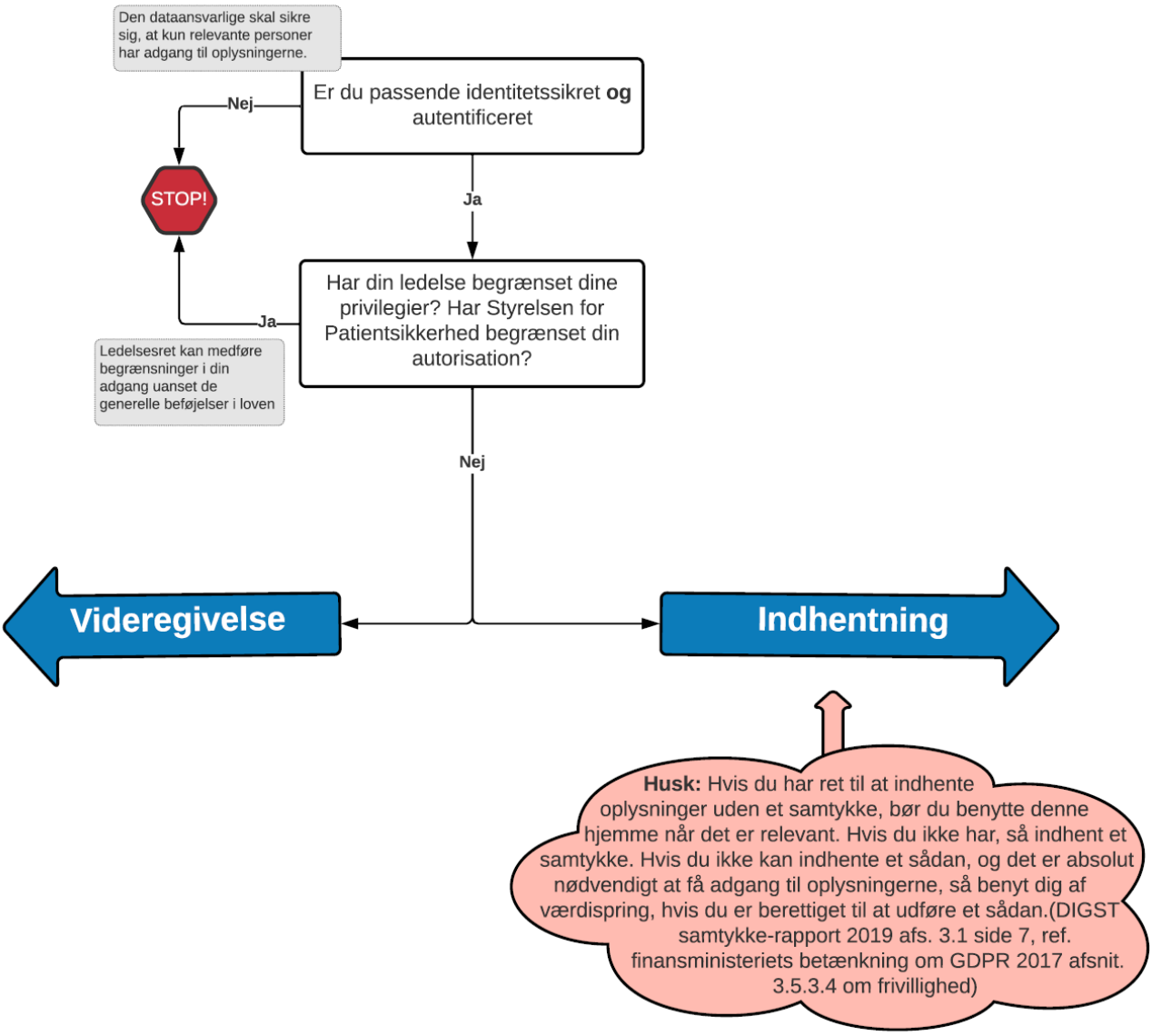
Figurerne fra bilaget er medtaget her som Bilag C - Videregivelse og indhentning.

Gennemgangen er foretaget med udgangspunkt i den lovgivning der var gældende i juni 2021. Der tages forbehold for senere ændringer.

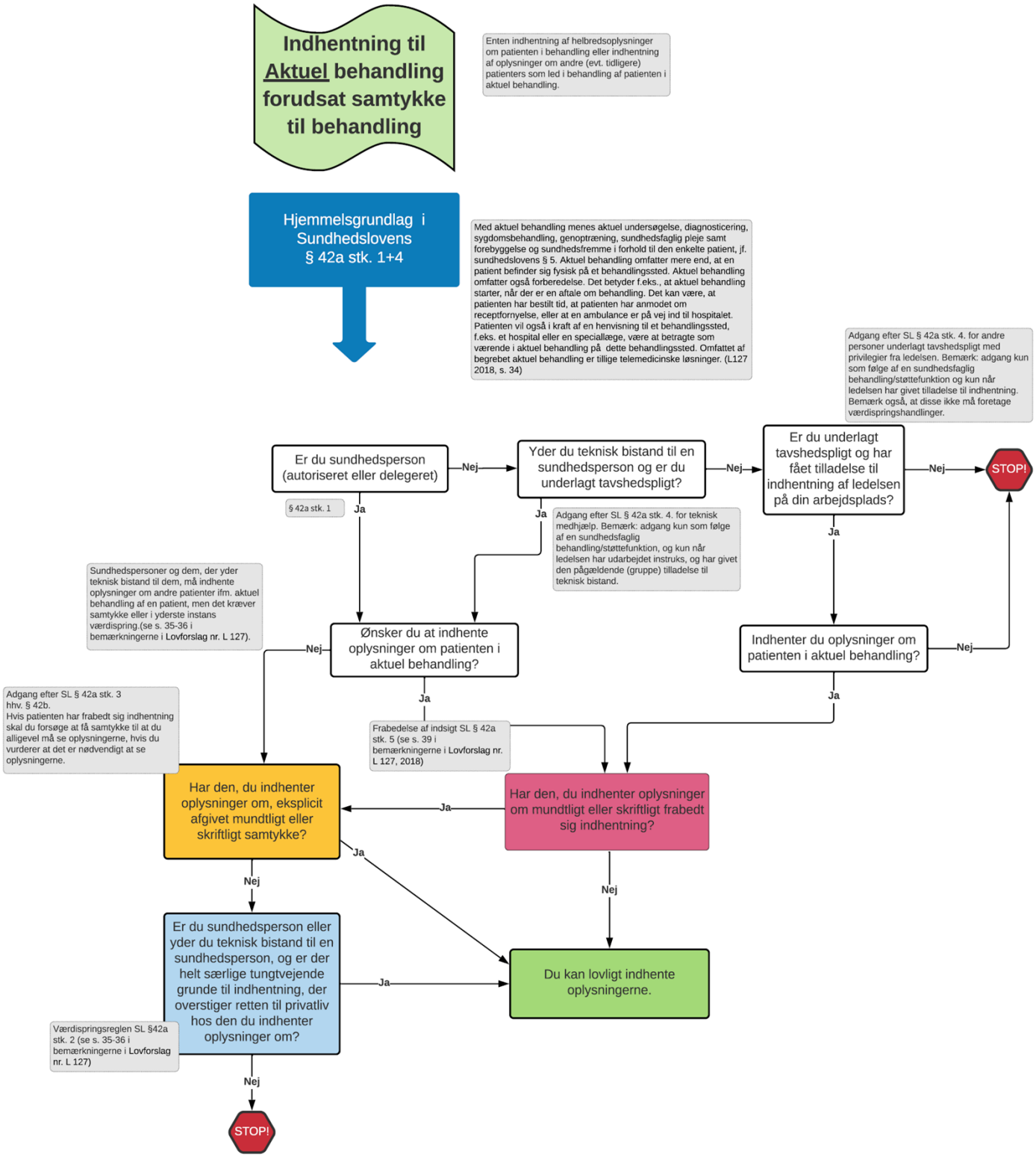
Gennemgangen starter med en validering af personen, da enhver adgang til sundhedsdata kræver at personen er behørigt autentificeret og autoriseret af de relevante parter.

I det efterfølgende gennemgås reglerne for indhentning af personlige sundhedsdata i forbindelse med aktuel behandling.

[14] https://sundhedsdatastyrelsen.dk/-/media/sds/filer/rammer-og-retningslinjer/referenceaktitektur-og-it-standarder/referencearkitektur/maalbillede_samtykke_frabedelse.pdf
[15] https://sundhedsdatastyrelsen.dk/-/media/sds/filer/rammer-og-retningslinjer/referenceaktitektur-og-it-standarder/referencearkitektur/bilag2_samtykke_frabedelse.pdf



Figur 8 Validering af person



Figur 9 Indhentning af elektroniske helbredsoplysninger i forbindelse med behandling af patienter

Figuren viser, at dét at afgøre om en person må få adgang til at indhente sundhedsoplysninger er komplekst. Netop dét kan let give anledning til fejl og forskelligartet implementering af lovgivningen i IT-systemerne.

I ovenstående figur vises et eksempel på, hvordan dele af sundhedslovens §42 a kan implementeres.

I eksemplet har en klinisk bruger behov for at indhente oplysninger om en given patient til aktuel behandling. Brugerens identitet verificeres, og herefter sikres det, at brugeren er autoriseret til at indhente oplysningerne, enten fordi vedkommende har en sundhedsfaglig autorisation eller fordi der er tale om en bruger, der har tavshedspligt og ledelsens tilladelse til at tilgå oplysningerne. Hvis opslaget er nødvendigt for den aktuelle behandling, kan opslaget foretages, medmindre patienten har frabedt sig indhentning af oplysninger.

Der findes mange variationer, og forholdende vedrørende adgang til og indhentning af oplysninger i patientjournaler er komplekse.

Referencearkitekturen er vedlagt en omfattende oversigt, som er vedlagt som bilag C, hvor følgende syv scenarier gennemgås:

- Indhentning til aktuel behandling (forudsat samtykke til behandling)
- Indhentning fra fælles medicinkort
- Indhentning i forbindelse med behandling (ikke aktuel/igangværende)
- Indhentning til andre formål end behandling
- Videregivelse i forbindelse med behandling
- Videregivelse til andre formål end behandling
- Videregivelse til forskning og statistik

4.5 Arkitekturbyggeblokke i referencearkitekturen

4.5.1 Overblik

Med udgangspunkt i begrebsmodellen og de beskrevne processer er det muligt at udpege de arkitekturbyggeblokke, der bør indgå i sikkerhedsarkitekturen.

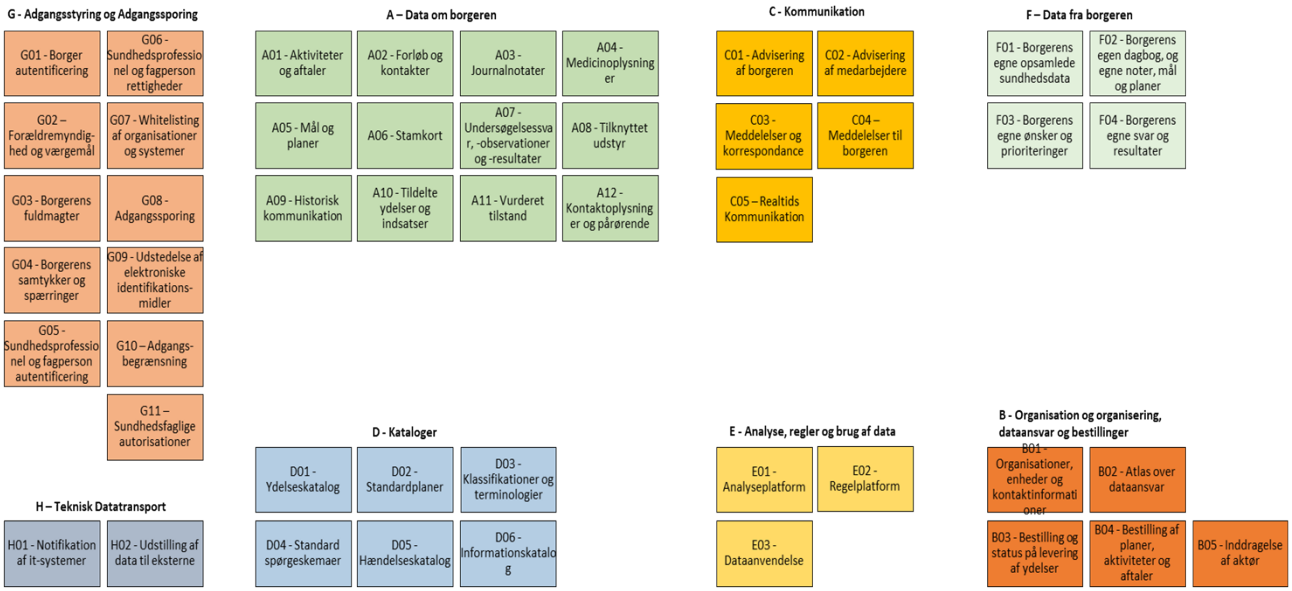
En byggeblok er et afgrænset element i en arkitektur eller en løsning, der kan genbruges. Der arbejdes jf. den fællesoffentlige digitale arkitektur (FDA) med to typer af byggeblokke; arkitekturbyggeblokke og løsningsbyggeblokke[16]. En arkitekturbyggeblok er en abstrakt men veldefineret delmængde af arkitekturmodellen, hvor der logisk set kun findes én af hver arkitekturbyggeblok. En løsningsbyggeblok modsvarer en arkitekturbyggeblok, men er konkret fysisk realisering (kode etc.) og kan anvendes i implementerede løsninger. Der kan samtidig være flere løsningsbyggeblokke for en arkitekturbyggeblok, dvs. flere realiseringer af samme arkitekturbyggeblok. Referencearkitekturen beskriver alene arkitekturbyggeblokke, og der tages ligeledes ikke stilling til, hvordan byggeblokke skal realiseres i løsningsbyggeblokke, fx hvilke komponenter, der skal etableres, hvilke teknologier disse baseres på, om disse er centrale eller lokale eller distribuerede ud over flere lokationer og hvem der har ejerskab til dem.

[16] https://arkitektur.digst.dk/rammearkitektur/arkitekturmodel-og-byggeblokke

Afledt af Strategi for Digital Sundhed 2018-2022 er der opstillet et målbillede for fælles infrastruktur på sundhedsområdet. I denne forbindelse er der identificeret et antal arkitekturbyggeblokke, der samlet danner det opstillede målbillede. I skrivende stund er der alene sket en identifikation af byggeblokkene, men det er hensigten, at arkitekturbyggeblokke bliver løbende defineret og dokumenteret, bl.a. gennem input fra referencearkitekturer, projekter og andre opgaver.

Nedenstående beskrivelse af arkitekturbyggeblokke er referencearkitekturens input til definition og dokumentation af de arkitekturbyggeblokke i infrastruktur-målbilledet, der vedrører informationssikkerhed. Det er målet, at når arkitekturbyggeblokkene er entydigt defineret og fuldt dokumenteret, vil beskrivelsen i referencearkitekturen blive erstattet med en reference til byggeblokken i målbilledet for fælles infrastruktur.

Referencearkitekturen peger også på 4 kandidater til nye arkitekturbyggeblokke i målbilledet. Der gives tilsvarende input til definition af disse.



Figur 10: Arkitekturbyggeblokke i målbillede for fælles infrastruktur

Nedenfor beskrives overvejelser vedr. det centrale indhold af arkitekturbyggeblokkene. Efterfølgende præciseres hvilke operationer, det er nødvendigt, at arkitekturbyggeblokkene skal realisere for at kunne understøtte de beskrevne processer.

4.5.2 De enkelte arkitekturbyggeblokke

4.5.2.1 Stamkort (A06)

Stamdata er data, der er forholdsvis statiske. Stamkort er her et register med relevante "statiske" oplysninger om borgere. Stamkort som begreb benyttes flere steder udenfor sundhedsvæsenet og kan have en anden betydning.

4.5.2.1.1 Lovgrundlag

I henhold til et af de grundlæggende principper i databeskyttelsesretten, herunder databeskyttelsesforordningens artikel 5, stk. 1, litra f, skal persondata behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende oplysninger.

Oplysninger, der ikke er omfattet af databeskyttelsesforordningen, fordi det ikke er personoplysninger, er også vigtige, f.eks. oplysninger om organisationer i Sundhedsvæsnet Organisations Register (SOR). Dertil kommer andre oplysninger, der kan benyttes i forbindelse med håndhævelse af sikkerheden. Eksempelvis kan oplysninger knyttet til lægemidler være med til at sikre, at forsøgsmedicin kun ordineres af personer, der er godkendt hertil (medvirker til en stærk adgangskontrol).

4.5.2.1.2 Operationalisering

Der er behov for at kunne identificere personer entydigt på tværs af sundhedsvæsnets parter. Det gælder såvel sundhedspersoner som borgere. CPR-registret er det eneste underliggende "registersystem", der i dag kan sikre entydig identifikation og som rummer de grundlæggende identiteter, der er behov for. Grundlæggende stamoplysninger om de enkelte personer hentes fra CPR-registret, men der vil ofte, ud over de rene identitetsoplysninger, være behov for andre oplysninger f.eks. kontaktoplysninger og pårørende (se byggeblok Kontaktoplysning og pårørende, afsnit 4.5.2.2).

I 2019 blev der lavet en pilotafprøvning af en "Fælles Stamkort"-løsning, for at afdække anvendeligheden af et sådant. Afprøvningen var en del af programmet "Et Samlet Patientoverblik", hvor forskellige parter på sundhedsområdet var samlet for at definere og pilotafprøve fælles digitale løsninger. I Fælles Stamkort hentes personoplysninger fra CPR-registret, der er relevante at kende for behandlingssteder, herunder sundhedspersoner. Samtidig er det muligt for borgere at indtaste oplysninger om nærmeste pårørende og deres kontaktoplysninger, oplysninger om sprog m.v. Evalueringsrapporten[17] er tilgængelig og viser en positiv effekt ved deling af de valgte oplysninger. Denne referencearkitektur finder, at erfaringerne fra dette fælles pilotafprøvningsprojekt og den videre implementering bør indvirke på definitionen af den fælles arkitekturbyggeblok.

[17] https://sundhedsdatastyrelsen.dk/-/media/sds/filer/strategi-og-projekter/patientoverblik/evaluering_pilotafproevningen_samlet_patientoverblik.pdf?la=da

4.5.2.2 Kontaktoplysninger og pårørende (A12)

Ud over de rene identitetsoplysninger (jf. byggeblokken A06 ovenfor), vil behandlingssteder ofte have behov for også at have oplysninger om bl.a. pårørende, kontaktmuligheder og eventuelle personlige hensyn (tolkebistand, transport etc.), mv.

4.5.2.2.1 Lovgrundlag

Kontaktoplysninger og oplysninger om pårørende er underlagt de samme databeskyttelsesretlige forhold som oplysninger om patient i Stamkort byggeblokken. Dvs. at jf. databeskyttelsesforordningens artikel 5, stk. 1, litra f, skal data behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende oplysninger. Samtidig er oplysninger i Fælles Stamkort omfattet af reglerne om den fælles digitale infrastruktur i sundhedslovens § 193 b og medfølgende bekendtgørelse

4.5.2.2.2 Operationalisering

Igen peger referencearkitekturen på erfaringerne med pilotafprøvning af det "fælles stamkort". Her fandt man det relevant for behandlingssteder at dele kontaktoplysninger, midlertidig adresse, sygesikringsgruppe og foretrukne kommunikationssprog samt kontaktoplysninger på borgerens pårørende – navne, adresser, telefonnumre samt oplysninger om egen læge. Oplysningerne kom primært fra patientens egen indtastning på sundhed.dk samt fra CPR-registeret og sygesikringssystemerne.

4.5.2.3 Organisationer, enheder og kontaktinformationer (B01)

Der er endvidere behov for at kunne identificere organisatoriske enheder entydigt på tværs af parter. Det er af afgørende betydning for sikkerhedsløsningerne at benytte den samme entydige identifikation af organisatoriske enheder. Organisatoriske oplysninger benyttes såvel i samtykke/spærring, behandlingsrelations tjek, ved tildeling af roller og rettigheder, white listing af adgang til løsninger fra organisationer, forskellige typer logning og borgervisning af oplysninger om hvem, der har set data (MinLog). Og det hjælper ikke, at borgeren eksempelvis frabeder sig adgang til oplysninger opsamlet af en given organisation, hvis disse oplysninger er registreret under forskellige organisatoriske identiteter (og hvor det ikke er muligt at oversætte mellem forskellige identiteter).

4.5.2.3.1 Lovgrundlag

Denne byggeblok har ikke ophæng i noget lovgrundlag.

4.5.2.3.2 Operationalisering

SOR er det eneste organisationsregister på sundhedsområdet, der kan dække alle typer organisatoriske enheder. SOR rummer alle organisatoriske enheder, der udøver behandling i henhold til sundhedsloven (der er en aftalemæssig forpligtelse for parterne til at lade sig oprette heri, således at der kan føres tilsyn med behandlingen). Stamoplysninger om de enkelte organisatoriske enheder hentes fra SOR. Denne referencearkitektur finder, at erfaringerne med etablering og brug af SOR og oplysninger herfra (bl.a. til nationale sikkerhedsservices) bør indvirke på definitionen af den fælles arkitekturbyggeblok.

4.5.2.4 Borgerautentificering (G01)

Ved autentifikation forstås godtgørelsen af ægtheden af noget, fx en persons, en computers eller et digitalt objekts identitet. Denne byggeblok beskriver sikringen af (EU-)borgeres identitet.

4.5.2.4.1 Lovgrundlag

Den europæiske eIDAS[18] forordning om eID og tillidstjenester blev vedtaget af EU-landene den 17. september 2014. eIDAS-forordningen skal fremme borgere og virksomheders muligheder for at anvende elektroniske tjenester på tværs af EU's indre grænser. Forordningen pålægger således også Danmark at anerkende eID for borgere og virksomheder fra andre europæiske medlemslande i danske selvbetjeningsløsninger. I forlængelse heraf, er der vedtaget lov vedr. anvendelse af dansk eID, se lov om MitID og Nemlogin[19].

4.5.2.4.2 Operationalisering

National Standard for Identiteters Sikringsniveauer (NSIS[20]), har til formål at skabe rammer for tillid til digitale identiteter samt digitale ID-tjenester. NSIS tager afsæt i internationale standarder og rammeværk med henblik på at sikre interoperabilitet, videndeling, certificering, akkreditering og understøttelse af det indre marked, herunder væsentligst [eIDAS]-forordningen[21], den tilhørende gennemførselsforordning 2015/1502[22] om "Levels of Assurance" (LOA) og [ISO 29115]. Udover NSIS-standarden med normative krav findes også en særskilt vejledning til standarden[23], som uddyber kravene gennem forklaringer og eksempler, samt revisionsinstrukser, som benyttes ved anmeldelse.

NSIS bliver standarden for MitID og NemLog-in3.

Sundhedsområdet ønsker at være en del af den fællesoffentlige MitID-løsning, hvor borgeren udstyres med MitID identifikationsmidler i henhold til fælles processer og hvor autentifikation sker af MitID-infrastrukturen. Borgeren kan med andre ord benytte samme identifikationsmidler til at få adgang til tjenester på sundhedsområdet som kan benyttes i forhold til mange andre offentlige og private tjenester. Den nationale sikkerhedsinfrastruktur på sundhedsområdet formidler adgang til autentifikation i MitID-infrastrukturen og modtager autentifikationsbeviser fra denne.

4.5.2.5 Borgerens fuldmagter (G03)

En borger kan give en anden person ret til at handle på sine vegne. En fuldmagt dækker typisk et enkelt område og sætter den anden person i stand til at agere med samme rettigheder i stedet for fuldmagtsgiveren/borgeren. På sundhedsområdet findes der flere former for fuldmagter – nogle giver ret til at handle på fuldmagtsgivers vegne i alle forhold, andre er ensbetydende med, at en fuldmagtshaver kan se med i fuldmagtsgivers oplysninger.

---

[19] https://www.retsinformation.dk/eli/lta/2021/783
[20] https://digst.dk/it-loesninger/nemlog-in/det-kommende-nemlog-in/vejledninger-og-standarder/nsis-standarden/
[21] https://digst.dk/it-loesninger/nemid/om-loesningen/samarbejde/eidas/
[22] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32015R1502
[23] https://digst.dk/media/28115/vejledning-til-national-standard-for-identiteters-sikringsniveauer-nsis-version-23.pdf

4.5.2.5.1 Lovgrundlag

Fuldmagter i dansk ret er et ganske særligt aftaleforhold, der som udgangspunkt indtil 2017 udelukkende var reguleret i aftalelovens kapitel II. Aftaler om fuldmagt kan typisk ikke indgås vedrørende personlige forhold.

På den baggrund indførtes lovregulering i forhold til fremtidsfuldmagter, således at det blev muligt for borgere på forhånd at give en anden person fuldmagt til at varetage borgerens personlige (eller økonomiske) forhold, hvis borgeren ikke længere selv har evne til det pga. sygdom, svækket mental funktion eller lignende. Således træder en fremtidsfuldmagt først i kraft under visse omstændigheder og sætter fuldmagtshaveren i stand til at give tilkendegivelser i forbindelse med behandling, mv. Ordningen vedrørende fremtidsfuldmagter er et frivilligt og privat alternativ til en almindelig fuldmagt og det offentligt fastsatte værgemål. I et behandlingstestamente er det muligt for borgeren på forhånd at tage stilling til ophør af livsforlængende behandling m.v. For at et behandlingstestamente træder i kraft, er der lovfastsatte betingelser, som skal gøre sig gældende, herunder hvis borgeren bliver uafvendeligt døende, eller hvis borgeren ligger hjælpeløs hen pga. sygdom, ulykke mv., eller hvis de fysiske konsekvenser af borgerens sygdom eller behandling er meget alvorlige og lidelsesfulde.

Således kan en fremtidsfuldmagt træde i kraft før et behandlingstestamente og kan supplere i den forstand, at borgeren selv på forhånd kan vælge den, der skal varetage vedkommendes private interesser.

4.5.2.5.2 Operationalisering

Der eksisterer en fællesoffentlig fuldmagtsløsning[24] "Digital Fuldmagt", hvor borgere kan give andre personer fuldmagt til en række digitale selvbetjeningsløsninger. Borgerens administration af Digital Fuldmagt løsningen er tilgængelig via borger.dk. Konceptet er pt. tænkt snævert; der er fokus på adgangsstyring i portalløsninger og ikke til de bagvedliggende løsninger.

En del sundhedsløsninger er oprettet i systemet. Af eksempler kan nævnes: handle i Fælles Medicinkort (via Medicinkortet-appen) og se Laboratoriesvar (via Sundhed.dk). Dokumentation for sundhedsvæsenets del af løsningen kan findes på NSPOP[25]. Der arbejdes løbende på at forbedre løsningen og udbrede den til flere løsninger. Digitaliseringsstyrelsen administrerer løsningen. Der er brug for yderligere dialog for at sikre en fællesoffentlig løsning, der funderes på et bredere og mere dækkende koncept.

4.5.2.6 Borgerens samtykke og mulighed for spærring (G04)

I dette dokument dækker samtykke over en accept af en sundhedsfaglig behandling eller behandling af persondata. Spærring dækker over muligheden for at kunne spærre for at andre kan se ens persondata.

4.5.2.6.1 Lovgrundlag

Inden for sundhedsvæsnet er samtykkereglerne reguleret forskelligt, alt efter hvilken lov forholdet er omfattet af.

Udgangspunktet er, at behandling af oplysninger, der sker i forbindelse med den sundhedsfaglige behandling af borgeren, er omfattet af sundhedsloven, herunder de samtykkekrav, som findes i sundhedsloven og dertil hørende bekendtgørelse. Sundhedslovens kapitel 5 indeholder regler om informeret samtykke til behandling

[24] https://digst.dk/it-loesninger/digital-fuldmagt/anvendelse/
[25] https://www.nspop.dk/pages/releaseview.action?pageId=102395910

og selvbestemmelsesretten. Kapitel 9 i sundhedsloven omhandler behandlingen af personoplysninger, herunder det forudsatte samtykke til indhentning af oplysninger i forbindelse med aktuel behandling, muligheden for at frabede sig at oplysninger indhentes, samtykke til videregivelse af oplysninger i behandlingsøjemed og til andre formål end behandling, samt borgerens ret til at frabede sig videregivelse.

Såfremt forholdet ikke er omfattet sundhedslovgivningen eller anden særlov, gælder databeskyttelsesforordningens bestemmelser om samtykke, herunder definitionen i artikel 4, nr. 11 samt betingelserne for samtykke i artikel 7.

4.5.2.6.2 Operationalisering

Borgerne har ifølge sundhedsloven ret til at frabede sig, at deres sundhedsoplysninger indhentes, samtidig har borgeren ret til at nægte at oplysninger videregives fra en sundhedsperson til en anden, eller at oplysningerne videregives mellem sektorer. Retten omfatter dog ikke en ret til at oplysningerne ikke deles teknisk. Hvis en borger ønsker teknisk at understøtte retten til at nægte videregivelse eller frabede sig indhentning, er det i visse tilfælde muligt at angive en spærring for adgangen til borgerens sundhedsoplysninger. Sundhedsdatastyrelsen driver en national service "Min Spærring", der kan administreres af borgere på sundhed.dk. Servicen kører på NSP og har effekt for tilmeldte nationale løsninger og kan gøres tilgængelig på andre anvendersystemer, som f.eks. "Min Læge" app'en.

I mange systemer håndteres borgerens tilkendegivelser vedrørende nægtelse af videregivelse eller frabedelse af indhentning dog i fritekstfelter og understøtter ikke integration til den nationale service.

Som udgangspunkt har en sundhedsperson behov for at kunne orientere sig om borgerens sygdomshistorik eller andre relevante oplysninger for at kunne behandle vedkommende. Derfor er det også vigtigt at sundhedspersonen kan se, at der er oplysninger, der er blevet filtreret fra som følge af frabedelser. Sundhedspersonen kan i Sundhedsdatastyrelsens løsninger og på Sundhed.dk se, at der er filtreret oplysninger fra og kan på den baggrund gå i dialog med borgeren om, hvorvidt oplysningerne måske kan være nødvendige for, at borgeren kan få den bedste behandling. Sundhedspersonen kan undtagelsesvist se i de spærrede oplysninger uden borgerens samtykke, hvis sundhedspersonen vurderer, at 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. Sundhedsloven §42a stk. 2[26]

Afgrænsningen af hvad der samlet kan frabedes indsigt i skal altid holdes på et niveau, der er meningsfuldt for borgeren. Eksempelvis kan det dreje sig om alle data vedrørende et givet sygdomsforløb, en kontakt med sygehusvæsenet eller et besøg ved en sundhedsfaglig. Afgrænsningen skal endvidere være meningsfuld systemteknisk. Hvis borgeren ønsker at spærre for alle oplysninger vedrørende et givet sygdoms-/behandlingsforløb, forudsætter det at alle systemer, der rummer oplysninger om/fra dette forløb kan identificeres – uanset hvilket system de registreres i. Dette er ikke muligt i dag.

[26] https://www.elov.dk/sundhedsloven/paragraf/42a/

4.5.2.7 Sundhedsprofessionel og fagperson autentificering (G05)

Ved autentificering forstås godtgørelsen af ægtheden af noget, her en fagpersons identitet.

4.5.2.7.1 Lovgrundlag

Lov om MitID og NemLogin[27], National Standard for Identiteters Sikringsniveau (NSIS)[28] og for internationalt brug, eIDAS forordningen[29].

4.5.2.7.2 Operationalisering

Lov om MitID og NemLogin.
§ 6. Når offentlige myndigheder og offentligretlige organer anvender digitale selvbetjeningsløsninger til at udføre en myndighedsopgave, skal de sikre, at privatpersoner og erhvervsbrugere med MitID gives adgang til selvbetjeningsløsningen, hvis adgangen kræver sikker autentifikation.

Et fælles krav i sundhedssektoren er større og større sikkerhed for at det anvendte identifikationsmiddel rent faktisk er udstedt til den sundhedsprofessionelle eller fagperson, der er i besiddelse af det, uden at selve autentifikationsprocessen bliver unødig kompleks. Teknologier som multifaktor autentifikation, hardwarekryptonøgler, mobile apps og biometriske enheder er teknologier, der kan understøtte dette.

En problemstilling, der er særligt aktuel i et højt digitaliseret sundhedsvæsen er, at de mange systemer ikke alle benytter samme autentifikation, samt at der benyttes mange fælles nationale systemer på tværs af væsenet. En måde at håndtere det på er ved at benytte en såkaldt føderationsmodel, hvor parterne indretter deres løsninger indenfor fælles rammer og hvor der derfor er tillid til disse løsninger fra forskellige parter. Den nationale infrastruktur på sundhedsområdet vil fremover ikke etablere en fælles autentifikationsservice, men fungere som videreformidler, så brugere med fællesoffentlige identifikationsmidler autentificeres af fællesoffentlige tjenester og brugere med lokale identifikationsmidler autentificeres af den organisation, der har udstyret den pågældende bruger med det lokale identifikationsmiddel.

Løsningerne baseres på National Standard for Identiteters Sikringsniveauer (NSIS[30]), der har til formål at skabe rammer for tillid til digitale Identiteter samt digitale ID-tjenester. NSIS tager afsæt i internationale standarder og rammeværk med henblik på at sikre interoperabilitet, videndeling, certificering, akkreditering og understøttelse af det indre marked, herunder væsentligst [eIDAS]-forordningen[31], den tilhørende gennemførselsforordning 2015/1502 om "Levels of Assurance" [LOA]), referencearkitektur for brugerstyring [REFARK][32] og [ISO 29115]. Udover NSIS-standarden med normative krav findes også en særskilt vejledning til standarden [VEJL], som uddyber kravene gennem forklaringer og eksempler, samt revisionsinstrukser, som benyttes ved anmeldelse.

Der er udarbejdet et målbillede for sammenhængende brugerstyring på sundhedsområdet, der konkretiserer ovenstående.[33]

---

[27] https://www.retsinformation.dk/api/pdf/222704
[28] https://digst.dk/media/28382/national-standard-for-identiteters-sikringsniveauer-nsis-version-202a-final.pdf
[29] https://digst.dk/it-loesninger/nemid/om-loesningen/samarbejde/eidas/
[30] https://digst.dk/it-loesninger/nemlog-in/det-kommende-nemlog-in/vejledninger-og-standarder/nsis-standarden/
[31] https://digst.dk/it-loesninger/nemid/om-loesningen/samarbejde/eidas/
[32] https://arkitektur.digst.dk/rammearkitektur/referencearkitekturer/referencearkitektur-brugerstyring
[33] https://www.nspop.dk/download/attachments/131139562/M%C3%A5lbillede_for_sammenh%C3%A6ngende_brugerstyring-v1.1.1.pdf?version=1&modificationDate=1620374214178&api=v2

4.5.2.8 Sundhedsprofessionel og fagperson rettigheder (G06)

Ved rettighed forstås her en godkendelse eller tilladelse til at udføre en given handling, der er veldefineret.

4.5.2.8.1 Lovgrundlag

Ifølge persondataforordningens artikel 5 skal personoplysninger behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret behandling, under anvendelse af passende tekniske eller organisatoriske foranstaltninger. Konsekvensen af dette er, at den dataansvarlige skal sikre autorisationen af de personer, der kan behandle persondata under dennes ansvar. Overholdelse af dette skal kunne påvises.

Et område, der tit forveksles med egentlig delegation i sundhedsretlig forstand er brug af teknisk bistand i forbindelse med indhentning af elektroniske helbredsoplysninger m.v. i forbindelse med behandling af patienter og tildeling af relevante rettigheder hertil.

Her er der ikke tale om en egentlig delegation, men om lovligheden af, at andre personer f.eks. laver opslag i patientjournalen på vegne af en autoriseret sundhedsperson. Dette i overensstemmelse med sundhedslovens § 42 a, stk. 4[34].

Eksempler på dette kan være lægesekretæren, der administrerer lægens kalender og gør klar til næste patient eller SOSU-assistenterne på sengeafsnittet, der passer de indlagte patenter og i den forbindelse har behov for at kunne slå visse oplysninger op i EPJ-systemet.

4.5.2.8.2 Operationalisering

Rettigheder tildelt på grund af jobfunktion benyttes typisk til at give adgang til systemer, data, funktionaliteter eller fysiske områder. Tildeling af denne type rettigheder styres typisk af en adgangspolitik, og i den forbindelse kan der være mange forskellige ting, der skal tages hensyn til. Rettigheder kan tildeles individuelt og manuelt, eller man kan vælge at lade rettighedstildelingen styre af forskellige forhold, som for eksempel fysisk arbejdssted, organisatorisk placering, jobfunktion, titel, sundhedsfaglig uddannelse og andre attributter. Brug af attributter er en af forudsætningerne for at opnå en effektiv og sikret fødereret adgangsmodel, og må forventes at blive den fremherskende teknik.

Brugerstyringsområdet er beskrevet og behandlet i den fælles offentlige "Referencearkitektur for brugerstyring[35]" fra 2020. Et vigtigt princip i denne forbindelse er, at rettighederne bør være de samme, uafhængigt af metode og adgangsvej således at adgangen til data er uafhængig af disse.

Der er også udarbejdet et målbillede for sammenhængende brugerstyring på sundhedsområdet. Denne lægger op til at brugerroller og rettigheder administreres af brugerens organisation – enten i nationale løsninger (brugerkataloger) eller i lokale (fødereret tilgang).

34 henvis til sundhedsloven
35 https://arkitektur.digst.dk/rammearkitektur/referencearkitekturer/referencearkitektur-brugerstyring

4.5.2.9 Adgangssporing (G08)

Registrering af hvilke personer eller processer, der har foretaget hvilke behandlinger af persondata, med angivelse af hvornår det er sket. Samt en vis kontrol af om alle regler og love er overholdt.

4.5.2.9.1 Lovgrundlag

Det følger dog af de grundlæggende principper samt artikel 5, stk. 2, hvorefter den dataansvarlige er ansvarlig for at kunne påvise, at stk. 1 overholdes (»ansvarlighed«). Det følger derudover eksplicit af øvrige bestemmelser i forordningen om behandlingssikkerhed, herunder artikel 24, 25 og 32.

Specifikke krav til logning kan findes i sundhedslovens § 42 c, Bekendtgørelse om pligt til at registrere logoplysninger og indsigt i logoplysninger (retsinformation.dk) og Bekendtgørelse om ændring af bekendtgørelse om pligt til at registrere logoplysninger og indsigt i logoplysninger (retsinformation.dk) fastsætter nærmere regler om private og offentlige dataansvarliges pligt til at registrere oplysninger om, hvem der har foretaget opslag i elektroniske systemer inden for sundhedsvæsenet (logning), samt om loggens indhold, opbevaring og sletning. Endvidere findes der i sundhedslovens § 157 om Det Fælles Medicinkort samt § 193 b om den fælles digitale infrastruktur bestemmelser om loggens indhold.

4.5.2.9.2 Operationalisering

Som nævnt ovenfor er der krav til logning i sundhedsloven

For mange af de løsninger, hvor personoplysninger deles på tværs af sundhedsvæsnet gennem nationale løsninger, er der et "krav" om at borgeren har indsigt i en forståelig oversigt over logningsoplysninger. Dette gælder bl.a. for Sundhedsdatastyrelsens fælles digitale infrastruktur[36]. Sundhed.dk blev etableret i persondatalovens gyldighedsperiode og skulle derfor godkendes af Datatilsynet. I godkendelsen er oprettelsen af Sundhed.dk betinget af, at der gives de registrerede adgang til en oversigt over logoplysninger.

Ved operationalisering af G08 bør der tages stilling til om de nationale, regionale, kommunale og private aktører kan dækkes af samme løsningsbyggeblokke eller der kræves adskilte byggeblokke. MinLog er i øjeblikket etableret på det nationale niveau.

4.5.2.10 Sundhedsfaglige autorisationer (G11)

Autorisationsregisteret, der føres af Styrelsen for Patientsikkerhed, indeholder oplysninger om autoriserede sundhedspersoner, herunder autorisationsform, autorisationsstatus m.v.

Den sundhedsfaglige autorisation må ikke sammenblandes med den informationssikkerhedsmæssige tekniske 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 om sundhedsprofessionel og fagperson rettighed). Omvendt kan fratagelse eller indskrænkning af en sundhedsfaglig autorisation betyde, at sundhedspersonen mister

36 Bekendtgørelse nr. 1101 af 29. juni 2020 om drift m.v. af den fælles digitale infrastruktur

retten til at udøve en bestemt sundhedsfaglig virksomhed, som kan være ensbetydende med, at de systemmæssige rettigheder i deres tekniske autorisation skal begrænses.

4.5.2.10.1 Lovgrundlag

Autorisation af sundhedspersoner er reguleret i lov om autorisation af sundhedspersoner og om sundhedsfaglig virksomhed[37]. (Autorisationsloven)

4.5.2.10.2 Operationalisering

Autorisationsregisteret er et offentligt register, der føres af Styrelsen for Patientsikkerhed.
Sundhedsfaglige autorisationer administreres af Styrelsen for Patientsikkerhed (STPS. Der findes 19 forskellige sundhedsfaglige autorisationer i Danmark. Formålet med den sundhedsfaglige autorisation er at styrke patientsikkerheden og fremme kvaliteten af sundhedsvæsenets ydelser.
STPS har udfærdiget et dokument om rettigheder og pligter ved autorisation[38], som også beskriver delegationssituationerne.

4.5.2.11 Delegation (Kandidat til ny byggeblok)

Visse sundhedsfaglige opgaver er forbeholdt læger[39]. En læge kan dog delegere dele af sin forbeholdte virksomhed til en anden person, også kaldet en medhjælp. Delegation af lægeforbeholdt virksomhed giver mulighed for en god og effektiv arbejdsfordeling i almen praksis, men stiller også krav til både læger og praksispersonale. Delegation kan almindeligvis - og uden for det sundhedsretlige område – have en anden og bredere anvendelse. Delegation er kandidat, som arkitekturbyggeblok i målbillede for fælles infrastruktur inden for G-adgangsstyring og adgangssporing.

4.5.2.11.1 Lovgrundlag

Delegation sker, når en sundhedsperson, der er autoriseret til at varetage et forbeholdt virksomhedsområde i henhold til lov om autorisation af sundhedspersoner og om sundhedsfaglig virksomhed (autorisationsloven), vælger at delegere nogle af sine sundhedsfaglige opgaver til en anden person. Dette i overensstemmelse med autorisationsloven samt medfølgende vejledninger hertil[40].

Af bestemmelserne fremgår det hvilke opgaver, der ikke kan delegeres.

Når en sundhedsperson, f.eks. en læge, vælger at delegere opgaver til en anden person, drejer det sig om selve arbejdsopgaven og ikke om den systemmæssige adgang til IT-systemerne. At det kan være nødvendigt, at denne anden person også får systemmæssig adgang for at kunne udføre opgaven, er en følge af denne delegation.

---

[37] https://www.retsinformation.dk/eli/lta/2009/1219

[38] https://stps.dk/da/udgivelser/2019/rettigheder-og-pligter-ved-autorisation/~/media/903C05D44CB84B7DA5774AFBFE43B1FD.ashx

[39] https://stps.dk/da/udgivelser/2023/vaerd-at-vide-om-delegation-af-forbeholdt-virksomhed-og-skriftlige-instrukser-i-almen-praksis/~/media/4E01E0F37D0A4EA7B3C87F85F81AF0D2

[40] LBK nr 731 af 08/07/2019 § 17 Vejledning om autoriserede sundhedspersoners benyttelse af medhjælp VEJ nr 115 af 11/12/2009

https://www.retsinformation.dk/Forms/R0710.aspx?id=129064
Denne vejledning knytter sig til §17 i autorisationsloven og til Bekendtgørelse 1219 af 11/12 2009
https://www.retsinformation.dk/Forms/R0710.aspx?id=129042

Eksempler på delegation af forbeholdt virksomhed kan være sygeplejersken, der foretager vaccinationer på vegne af den praktiserende læge, eller hospitalet, der anvender en udenlandsk virksomhed til at vurdere røntgenbilleder.

4.5.2.11.2 Operationalisering

Da det kan være vanskeligt at håndtere de forskellige situationer er operationalisering af en delegation meget afhængig af den kontekst, der er tale om. Fælles er det dog at ansvarsfordelingen skal være klar. Samtidig er den dataansvarlige forpligtet til at følge op på og sikre, at tekniske autorisationer og delegationer i sundhedsretlig forstand er korrekte eksempelvis ved fratrædelse m.v.

- Det bør overvejes at fastlægge konceptet i et målbillede for brugerrettighedsstyring.
- Se også her STPS' dokument om rettigheder og pligter ved autorisation[41]

4.5.2.12 Behandlingsrelation (Kandidat til ny byggeblok)

En behandlingsrelation eksisterer, når en borger er i aktuel behandling hos en sundhedsperson/behandler. Behandlingsrelation er kandidat som arkitekturbyggeblok i målbillede for fælles infrastruktur inden for G-Adgangsstyring og adgangssporing.

4.5.2.12.1 Lovgrundlag

Sundhedslovens § 5 omhandler, hvad der efter sundhedslovens bestemmelser er omfattet af begrebet behandling. Reglerne for indhentning og videregivelse af oplysninger, f.eks. i forbindelse med aktuel behandling af patient/borgere, fremgår af lovens kapitel 9. Som udgangspunkt kræver indhentning af oplysninger om en patient at patienten er i "aktuel behandling". Således skal der være en behandlingsmæssig relation mellem patient og sundhedsperson/behandler. Undtagelsesvis kan en sundhedsperson indhente oplysninger om andre patienter til brug for den aktuelle behandling af en konkret patient.

Derudover er der indført regler om indhentning af oplysninger vedrørende en gruppe af patienter til brug for såkaldt behandlingsstøtte jf. sundhedslovens § 42 a, stk. 6. Der er endnu ikke udformet en bekendtgørelse, der beskriver forudsætningerne herfor

4.5.2.12.2 Operationalisering

Elektroniske registreringer i forskellige systemer og registre kan anvendes til teknisk at indikere, om der eksisterer en behandlingsrelation mellem en sundhedsfaglig og en patient i aktuel behandling. Hvis eksempelvis et sygehus har henvist en patient til behandling ved privat praktiserende speciallæge, og en sådan speciallæge har hentet den pågældende henvisning (kan verificeres ud fra registreringer i henvisningsformidlingsløsningen), vil der være en høj evidens for, at den privat praktiserende speciallæge har den pågældende patient i behandling.

Sundhedsdatastyrelsen har udviklet en behandlingsrelationsservice, og dokumentationen beskriver tydeligt hvilke overvejelser, der er gjort og hvilke løsninger, der er valgt i dette tilfælde.

[41]https://stps.dk/da/udgivelser/2019/rettigheder-og-pligter-ved-autorisation/~/media/903C05D44CB84B7DA5774AFBFE43B1FD.ashx

Der henvises derfor til denne[42].

4.5.2.13 Værdispring (Kandidat til ny byggeblok)

Med værdispring menes, at hensynet til hemmeligholdelse viger for hensynet til andre væsentlige interesser. Det kan enten være hensynet til patienten selv, andre patienter, samfundet m.v. Der skal være tale om en væsentlig forskel i værdien af hemmeligholdelse og disse andre væsentlige hensyn.

Værdispring er kandidat som arkitekturbyggeblok i målbillede for fælles infrastruktur inden for G-Adgangsstyring og Adgangssporing.

4.5.2.13.1 Lovgrundlag

Hvis en borger har frabedt sig indhentning eller videregivelse af oplysninger – både teknisk og mundtligt - i forbindelse med behandling, findes der undtagelser i sundhedsloven, der gør det muligt for sundhedspersonale under visse konkrete forudsætninger at indhente og eventuelt videregive oplysninger på trods heraf. Som ovenfor anført kaldes det værdispring. Således kan værdispring alene foretages, såfremt det vurderes konkret, at det er nødvendigt til berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, herunder en patient, der ikke selv kan varetage sine interesser, sundhedspersonen eller andre. Da der er tale om en undtagelsesregel, skal der meget til, før det kan ske.

Værdispringsreglen for indhentning findes i sundhedslovens § 42 a, stk. 2, for videregivelse til behandling findes den i § 41, stk. 2, nr. 1. Hvis der undtagelsesvist skal videregives til andre formål, findes værdispringsreglen i § 43, stk. 2, nr. 2.

4.5.2.13.2 Operationalisering

Værdispring er med til at sikre, at en sundhedsperson ikke kommer i en situation, hvor vedkommende ikke kan få adgang til vigtige oplysninger om patienten og dermed sættes ude af stand til at kunne behandle patienten. Værdispringsreglen er dog ikke til for at omgå patientens ønsker eller eksisterende sikkerhedsløsninger. I visse tilfælde vil patientens frabedelse være ensbetydende med, at den sundhedsfaglige behandling ikke er mulig Patienten kan ikke modsætte sig, at der indhentes eller videregives, hvis der er tale om forhold der er egnet til at varetage sundhedspersonens eller andres interesser.

Værdispringsreglen er ikke ensbetydende med, at der kan ses bort fra krav om tekniske sikkerhedsforanstaltninger, der regulerer brugernes adgang. Disse adgangskrav skal netop sikre en mulighed for at overskride de normalt gældende adgangsrettigheder, hvis der er behov herfor.

[42] https://www.nspop.dk/display/public/web/Behandlingsrelationsservice+%28BRS%29+-+Leverancebeskrivelse

Som udgangspunkt bør den enkelte løsning som minimum leve op til følgende godkendte[43] 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.

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 anvendelse

Værdispring skal være brugerens aktive beslutning og ikke blot 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.

4.5.2.14 Validitet (Kandidat til ny byggeblok)

Byggeblok, der understøtter kontrol af datas er korrekthed og/eller troværdighed, samt mulighed for sletning eller berigtigelse af ukorrekte data.

Kandidat til arkitekturbyggeblok i "målbillede for fælles infrastruktur" indenfor grupperingen F-Data fra borgeren.

4.5.2.14.1 Lovgrundlag

I forbindelse med sundhedsfaglig behandling er det som udgangspunkt den autoriserede sundhedsperson, der i henhold til autorisationsloven og dertil hørende journalføringsbekendtgørelse har en række

[43] Godkendt af Informationssikkerhedsrådet i regi af Digital Sundhed i 2010.

forpligtigelser, herunder blandt andet til at journalføre og validere de oplysninger, der er om borgeren. Sundhedspersonen kan dog alene tilføje korrigerede oplysninger til journalen men aldrig slette én gang registrerede data med undtagelse af åbenlyse fejl. Årsagen til at data ikke må slettes er, at andre sundhedspersoner eller sundhedspersonen selv kan have reageret på de ikke valide oplysninger. Såfremt oplysningerne efterfølgende slettes, kan det ikke dokumenteres, på hvilket grundlag sundhedspersonen har handlet. Patientsikkerhedsmæssigt har det også den fordel at klinikere ikke kan dække over eventuelle fejlbehandlinger ved at fjerne beviserne i journalen.

Udover ovenstående følger det af databeskyttelsesforordningens artikel 5, stk. 1, litra d, at personoplysninger skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»rigtighed«). Derudover fremgår det af databeskyttelsesforordningens artikel 5, stk. 1, litra f, at personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

4.5.2.14.2 Operationalisering

Idet data i sundhedsvæsnet kommer fra flere parter, herunder sundhedspersoner og evt. borgeren selv, kan der til tider opstå tvivl om, hvem der har ansvar for data og hvem man skal gå til, hvis man vil have slettet eller berigtiget oplysninger. Det kunne således være ønskeligt med oplysninger om, hvor data stammer fra, evt. med eksplicit angivelse af dataansvar. Oplysninger om, hvor data stammer fra kan også være med til at stemple datakvaliteten.

Der kan eksempelvis være tale om data modtaget fra patientens mobiltelefon, egne måleapparater og cloud-baserede tjenester. Systemer som f.eks. Apples Sundhed app og Google Health bliver mere og mere udbredte, og både patienter og sundhedsvæsen ønsker at kunne benytte disse til at optimere behandling af og kommunikation med patienter og borgere. Der skal arbejdes mere med konceptet for styring af validitet/kvalitet.

4.6 Metoder

I dette afsnit beskrives arkitekturbyggeblokkene ud fra deres snitflader til omgivelserne (interfaces). Et interface beskriver en række metoder, som byggeblokken realiserer. Eksempelvis vil byggeblokken ”Borgerens samtykke og spærringer” stille et interface til rådighed med en række metoder, der skal gøre det muligt for den konkrete løsning at håndtere borgerens samtykker. Der tages som nævnt i referencearkitekturen ikke stilling til hvordan arkitekturbyggeblokke og metoderne skal realiseres. Det afgørende er, at arkitekturbyggeblokkene spiller en veldefineret rolle i arkitekturen og at snitflader er veldefinerede.

4.6.1 Stamkort (A06)

Stamdata byggeblokken realiserer følgende metoder:

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

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	

4.6.2 Kontaktoplysninger og pårørende (A12)

Byggeblokken realiserer følgende metoder:

- Opret/vedligehold/slet supplerende kontaktoplysninger
- Opret/vedligehold/slet pårørende med tilhørende kontaktoplysninger
- Søg kontaktoplysninger
- Søg pårørende

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	

4.6.3 Organisationer, enheder og kontaktinformationer (B01)

Byggeblokken realiserer følgende metoder:

- 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 organisationer.
Understøtter processer	Klar identifikation af organisationer og enheder på tværs af sundhedsvæsenet.
Afhængigheder	Adgang til SOR

4.6.4 Borgerautentificering (G01)

Autentifikationsbyggeblokken realiserer følgende metoder:

- Check gyldighed af borgerens akkreditiver f.eks. (MitID)
- Identificer person ud fra akkreditiver

For større indblik i denne byggeblok, kan der hentes inspiration i de eksisterende fælles tjenester, samt i referencearkitektur for brugerstyring [44]

Hvad	Beskrivelse
Kort beskrivelse	Validerer borgeren med henblik på at give adgang til personlige services i sundhedsvæsenet.
Understøtter processer	Styring af adgang til selvbetjeningsløsninger eller sundhedsdata.
Afhængigheder	Lokale, decentrale og centrale autentifikationstjenester

4.6.5 Borgerens fuldmagter (G03)

Løsningsbyggeblok for fuldmagtsbyggeblokken drives og udvikles af Digitaliseringsstyrelsen som en fællesoffentlig tjeneste.

Fuldmagtsbyggeblokken realiserer følgende metoder:

- Opret, vedligehold og slet fuldmagt
- Check fuldmagt

[44] https://arkitektur.digst.dk/referencearkitekturer/brugerstyring/referencearkitektur-brugerstyring

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 online tjenester på vegne af borgeren.
Understøtter processer	Administration af fuldmagtsoplysninger Styring af adgang til patientoplysninger (adgangskontrol)
Afhængigheder	

4.6.6 Borgerens samtykke og mulighed for spærring (G04)

Samtykke og spærringer-byggeblokken realiserer følgende metoder:

- Administrér samtykke registrering
- Validér samtykke
- Validér spærring

Det giver her mening at henvise til målbillede for digitalt samtykke og frabedelse[45]

Formålet med digitalisering af samtykker og frabedelser er primært at give borgere og medarbejdere overblik over relevante samtykker og frabedelser samt mulighed for at administrere disse til at sikre overholdelse af relevant lovgivning på området.

Beskrivelse af byggeblokken er angivet i følgende tabel:

Hvad	Beskrivelse
Kort beskrivelse	Samtykkebyggeblokken indeholder alle borgerens samtykkeoplysninger. Borgeren selv, en befuldmægtiget eller en sundhedsperson på vegne af borgeren kan oprette spærringer. I forbindelse med opslag på nationale tjenester sikrer samtykkebyggeblokken, at borgerens samtykkeoplysninger anvendes til at validere brugerens adgang til data.
Understøtter processer	Administration af samtykkeoplysninger Styring af adgang til patientoplysninger (adgangskontrol) ”Min Spærring” tilbyder i dag, at Borgere kan spærre for adgang til deres sundhedsdata: • for specifikke sundhedspersoner med autorisation • for data **fra** bestemte tidsperioder • for data **fra** bestemte tidsperioder med oprindelse i bestemte sundhedsorganisationer.

[45] https://digst.dk/media/27839/maalbillede-for-digitalt-samtykke-og-frabedelse-webtilgaengelig.pdf

Afhængigheder	Der skal etableres interfaces mellem samtykkebyggeblokken og de enkelte it-løsninger. Løsningen vil ikke være fuldt dækkende, før alle it-systemer kan anvende byggeblokkens informationer

4.6.7 Sundhedsprofessionel og fagperson autentificering (G05)

Autentifikationsbyggeblokken realiserer følgende metoder:

- Check gyldighed af akkreditiver
- Identificer person ud fra akkreditiver

Se også her referencearkitektur for brugerstyring[46]

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

4.6.8 Sundhedsperson og fagperson rettigheder (G06)

Byggeblokken realiserer følgende metoder:

- Opret/vedligehold/slet faglige brugeres rettigheder
- kontroller omfanget af systemmæssige autorisationer og rettigheder

Hvad	**Beskrivelse**
Kort beskrivelse	
Understøtter processer	Styring af adgang til fagsystemer
Afhængigheder	

[46] https://arkitektur.digst.dk/referencearkitekturer/brugerstyring/referencearkitektur-brugerstyring

4.6.9 Adgangssporing (G08)

Byggeblokken realiserer følgende metoder:

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

Nogle systemer benytter sig af Minlog-tjenesten på National Service Platform (NSP)[47]

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 oplysninger om opslaget overføres til opfølgningsbyggeblokken, 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	

4.6.10 Sundhedsfaglige autorisationer (G11)

Sundhedsfaglig autorisation udstedes af Styrelsen for Patientsikkerhed, og sundhedspersonen får denne i kraft af sin sundhedsfaglige uddannelse. Oplysninger om disse er tilgængelige i autorisationsregistret, og behandles ikke yderligere her.

Ved teknisk autorisation forstås tekniske adgange, der gives på grund af jobfunktion.

(Teknisk) Autorisationsbyggeblokken realiserer følgende metoder:

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

[47] https://www.nspop.dk/display/public/web/MinLog2+-+Design+og+Arkitektur+beskrivelse

Hvad	Beskrivelse
Kort beskrivelse	Byggeblokken 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

4.6.11 Delegation (Ny)

Delegationsbyggeblokken realiserer følgende metoder:

- Opret/vedligehold/slet delegeret 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 det være tydeligt hvilke opgaver det drejer sig om.
Understøtter processer	Delegation af arbejdsopgaver / arbejdsfunktion
Afhængigheder	

4.6.12 Behandlingsrelation (Ny)

Behandlingsrelations-byggeblokken realiserer følgende metoder:

- Valider behandlingsrelation

Se i øvrigt beskrivelsen af Behandlingsrelationsservice[48] som Sundhedsdatastyrelsen arbejder på.

[48] https://www.nspop.dk/display/public/web/Behandlingsrelationsservice+%28BRS%29+-+Leverancebeskrivelse

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	

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

4.6.13 Værdispring (Ny)

Værdisprings-byggeblokken realiserer følgende metoder:

- 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	

4.6.14 Validitet (Ny)

Byggeblokken realiserer følgende metoder:

- Metadata: Kvalificér kilden
- Tillid til kommunikation
- Registrér troværdigheden af informationskilden
- Valider modtagne data
- Klassificér validiteten af oplysningerne

Hvad	Beskrivelse
Kort beskrivelse	Modtagelse af data fra ikke autoriserede kilder eller ad usikre kanaler, kan være behæftet med stor usikkerhed, og skal enten markeres som værende ubekræftede eller behæftet med en vis upålidelighed. Dette uanset om det er sket ved automatisk dataoverførsel, eller registreret af borgerne selv. Alle den slags data bør valideres af kvalificeret sundhedspersonale inden det benyttes aktivt i behandlingssammenhænge.
Understøtter processer	Borgerens registrering af egne oplysninger Hjemmemonitorering Borgeren kommer med egne data
Afhængigheder	Integrationer til personlige "smarte sundhedsdata registrerende enheder", apps, og borgervendte grænseflader.

4.7 Teknisk

Dette afsnit beskriver, hvordan de forretningsmæssige processer, begreber og objekter, beskrevet i de forrige afsnit på overordnet niveau kan udmønte sig i mere konkrete løsninger. Referencearkitekturen er en grundlæggende referencearkitektur, der skal anvendes på tværs af forskellige teknologier og anvendelses- og løsningsscenarier. Derfor peges der ikke på specifikke teknologier eller løsninger. Afsnittet beskriver derimod mønstre og anbefalinger i forhold til teknologiske valg og angiver eksisterende standarder og specifikationer, der er i anvendelse i den offentlige sektor. Disse bør inddrages ved design af løsningsarkitektur og valg af teknologier. Endeligt suppleres med en oversigt over emner og punkter hvor der anbefales at udvikle nye standarder eller profilere eksisterende standarder inden for informationssikkerhed.

Specifikt vil det tekniske afsnit beskrive følgende områder på nedenstående punkter:

- Liste over eksisterende anbefalinger og standarder inden for risikomodellering.
- Løsningsmodeller for realisering af privacy-by-design og privacy-by-default, herunder anonymisering og pseudonymisering af data – bl.a. i forbindelse med anvendelse af data til forskning.
- Sikkerhed for modeller for system-til-borger rettede løsninger, der er aktualiseret igennem nationale og regionale strategier om telemedicinske løsninger for borgerne og disses adgang til egne data.
- Anbefaling til standardisering eller profilering - Liste over eksisterende standarder indenfor informationssikkerhed, der bør overvejes eller realiseres for løsninger i sundhedssektoren
- Liste over eksisterende løsningsbyggeblokke, der bør overvejes anvendt ved implementering af løsninger

4.7.1 Anbefalinger og standarder for risikomodellering

Risikovurdering og måling af risiko er svært, da det altid vil være en relativ størrelse, hvor der ikke findes et entydigt svar. Der nævnes her nogle standarder og metoder, der benyttes i det offentlige danske sundhedsvæsen, men der findes mange flere internationale standarder og rammeværker, der kan benyttes i forskellige sammenhænge.

For risikovurdering og risikomodellering peger referencearkitekturen på at ISO 27001 bør iagttages hertil og i forhold til en informationsstyringsarkitektur, at denne baseres på en defineret risikomodel fra ISO27005.

I forhold til risikostyring og cybersecurity, herunder trusselsbilledet herfor, peges på NIST800-53 som et muligt grundlag.

- Med hensyn til måling af risici, findes der metoder til at lave repeterbare vurderinger og målinger, f.eks. OWASPs Risk Rating Methodology[49]. Det anbefales at anvende denne eller lign. metoder for at få en standardiseret metodik og som nævnt, at den er repeterbar.

4.7.2 Secure-by-design og Secure-by-default

Før det detaljerede arbejde omkring fastlæggelse af en specifik model for hvordan arbejdet med Secure-by-Design og Secure-by-Default tænkes ind for en given løsning, skal der udarbejdes en risikovurdering[50]. Gerne jf. anbefalinger i afsnit 4.7.1, således at alle sikkerhedsmæssige aspekter tænkes ind fra start. Det er et krav i databeskyttelsesforordningen, at man forholder sig til begrebet "privacy by design and by default" allerede ved det indledende løsningsdesign og sørger for at det tænkes ind i hele produktets levetid. Det er dog vigtigt at alle risici er håndteret helt fra den spæde start til produktet er skrottet og hardwaren er destrueret forsvarligt.

- Et antal sikkerhedsmyndigheder fra flere steder i verden; FBI, NSA, CISA fra USA og lignende organisationer fra Australien, Canada, England, Tyskland og New Zealand har udgivet et dokument med anbefalinger og overvejelser til systemudvikling, indkøb og implementering med disse principper.
- Titlen er Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default 51 og det indeholder i slutningen en del links til nogle af de pågældende organisationers relevante øvrige dokumenter.
- Rådet for digital sikkerhed har udgivet 10 dataetiske principper, som kan indgå i en tjekliste for den enkelte databehandling.
- Tjeklisten kan benyttes af projekter og beslutningstagere, når det skal vurderes om et givent formål kan opnås uden at tilsidesætte individets privatlivsbeskyttelse – og dermed balancere hensigten/målet optimalt i forhold til de anvendte midler. Rådet for Digital Sikkerhed anbefaler, at alle 10 spørgsmål kan besvares med et JA, førend en konkret it-løsning iværksættes.

Emne	**Spørgsmål**
Nødvendighed	Er det umuligt at opfylde formålet med løsningen helt uden at indsamle personoplysninger eller med fuld anonymisering af data? (hvis nej, så vælg at redesigne løsningen)
Lovlighed	Er der fuld klarhed over hjemmelsgrundlaget? (er metoden lovlig pga. samtykke, legitime interesser, kontrakt eller særlov)

[49] https://owasp.org/www-community/OWASP_Risk_Rating_Methodology
[50] Se hertil de til enhver tid gældende retningslinjer og vejledninger på Datatilsynets hjemmeside www.datatilsynet.dk
[51] https://www.cisa.gov/sites/default/files/2023-06/principles_approaches_for_security-by-design-default_508c.pdf

Etisk design	Sikres individets rettigheder og principperne i GDPR gennem it-løsningens design? (forudbestemt formål, kun indsamling af nødvendige data, indsigt, oplysningspligt, kontrol over egne data, sletning m.v.)
Konsekvenser	Er der på forhånd taget stilling til, hvilke konsekvenser forslaget/løsningen kan have for de registrerede på kort og på lang sigt?
Valgfrihed	Er det valgfrit for den enkelte, hvorvidt data om vedkommende registreres eller ej?
Sikkerhed	Er der etableret en passende sikkerhed i og omkring systemet i tråd med de nødvendige og bedst tilgængelige tekniske og organisatoriske metoder?
Transparens	Er der gennemsigtighed i behandlingen, herunder ved brug af algoritmer og er der menneskelig kontrol med resultaternes rimelighed?
Respekt for menneskerettigheder	Er der sikkerhed for, at databehandlingen ikke er bias med risiko for diskriminering, marginalisering eller stigmatisering af individer?
Proportionalitet	Er der foretaget en proportionalitetsafvejning og dermed sikret, at individets rettigheder ikke undermineres ud fra en "målet helliger midlet" tankegang?
Ansvarlighed	Er der klarhed om ansvarsplacering, løbende tilsyn og klageadgang?

Skemaet herunder kategoriserer forskellige typer af data samt beskriver, hvilke krav der bør stilles til behandling af data. Uanset hvilke typer data man behandler, og hvordan de er beskyttet, skal metoder og beskyttelse hele tiden holdes opdateret, så en eventuel re-identifikation ikke er mulig.

Type af data	**Krav til brug af standarder og it-arkitektur i forbindelse med databehandling**
<u>Identificerbare data</u> Data hvor fx cpr. nr. fremgår koblet på ex sygdoms- og behandlingshistorie. Der kan være både identifikatorer og kvasi-identifikatorer, der gør data identificerbare. Identifikatorer er attributter, der unikt kan identificere individet fx cpr. nr. Kvasi-identifikatorer er attributter der i fællesskab kan identificere et individ, fx postnummer og fødselsdato.	• Principperne og kravene i særlovgivningen, databeskyttelsesloven og GDPR gælder fuldt ud. • Det anbefales, at data i denne form skal begrænses til databehandlinger, hvor der er brug for identifikation.
<u>Pseudonymiserede data</u> Identifikatorer og kvasi-identifikatorer erstattes med en anden og tilsyneladende, men tilfældig, værdi, hvorved det er	• Man kan pseudonomisere ved brug af automatiserede mapningstabeller. Herved kan man også opnå fysisk adskillelse af databaser. • Man kan kryptere identifikationsoplysninger med en hemmelig nøgle, hvorved man kan finde tilbage til de oprindelige identiteter.

vanskeligere at knytte datasættet til den registreredes originale identitet. Det er stadig muligt at udskille og sammenkoble enkeltpersoners identitet på tværs af datasæt.	Brugerne af datasættet kan så se den kodede værdi af identifikationsoplysningerne. • Databeskyttelsesloven og – forordningen finder stadig anvendelse i forhold til behandlingen af oplysninger. • Der skal stadig foretages logning
Anonymiserede data Her fjernes muligheden for at identificere data ved at fjerne identifikatorer og kvasi identifikatorer. Fx ved at generalisere adresser til områder eller fødselsdato til intervaller. På den måde kan data om den enkelte hverken udskilles af selve datasættet eller udledes ved sammenkobling med andre datasæt. Billedmateriale fx røntgenbilleder kan ikke anonymiseres, men man kan fjerne tilknyttede identifikatorer	• Da der er tale om data som er anonyme, er det ikke muligt at gendanne identitet fra data; men det forudsætter, at anonymiseringen sker således, at der skabes irreversibilitet. Det er derfor vigtigt, at ALLE datasæt, som er identitetsbærende, maskeres / forandres irreversibelt. • Anonymisering er ikke trivielt, og der har været eksempler, hvor anonymiseringen ikke har været stærk nok. Det kræver derfor grundighed og en vis viden at anonymisere data, samt evt. en risikovurdering. • Anonymisering skal benyttes, hvor det er muligt at fjerne personhenførbare data, samtidig med at det forskningsmæssige aspekt bevares.
Syntetiske data Et statistisk konstrueret datasæt, der bevarer karakteristika fra rigtige data, uden individer kan identificeres	• Konstruktion af syntetiske datasæt kræver adgang til ægte data med de ønskede karakteristika. De syntetiske data bliver skabt ved, at et originalt datasæt køres igennem et matematisk program, som lægger støj på datasættet på en måde, så de syntetiske data ikke kan henføres til konkrete personer og samtidig bibeholder en spredning og sammenhæng, som gør dem statistisk valide. • Der skal være hjemmel til at skabe de syntetiske datasæt, eftersom denne behandling vil være omfattet af særlovgivning, databeskyttelseslov og forordning. • Det vil ofte være muligt efterfølgende at dele og bearbejde syntetiske data i stedet for de rigtige datasæt så det test- og forskningsmæssige aspekt bevares, uden at persondatabeskyttelsen kompromitteres. Dette ud fra den betragtning, at ingen person må kunne identificeres efterfølgende.

4.7.3 Borgerrettede løsninger

- Borgerrettede digitale løsninger er et bredt felt, som bl.a. omfatter løsninger inden for patientbehandling, såsom hjemmemonitorering og systemer, der ofte er målrettet mobile enheder eller har klienter til flere platforme. Desuden er der en del kommunikationsløsninger og nationale borgerrettede platforme. Der kan nævnes smittestop, corona-pas, Min læge, Medicinkortet, MinSundhed og de services, der er tilgængelige på Sundhed.dk og borger.dk. Af mere lokale løsninger kan nævnes regionale kronikerløsninger, min sundhedsplatform og en række personlige løsninger til kontrol af blodsukker eller styring af høreapparater.
- Når der vælges design og teknologi til borgerrettede løsninger, skal den der etablerer løsningen være særligt omhyggelig med privacy by design og default, herunder risikovurdering og sikring, da borgerens udstyr som udgangspunkt må betragtes som kompromitteret.
- Det må i den forbindelse overvejes i hvor stor grad, der er behov for at opbevare data på borgerens enheder, eller disse kan fastholdes i den centrale infrastruktur.
- Ved udveksling af data er det vigtigt at oplysninger, der modtages fra borgere, behandles med passende kontroller i forhold til resultat af risikovurderingen. Her kan anvendelse af realiserede løsninger af valideringsbyggeblokken være aktuel at vurdere.
- Ved implementering af tekniske sikkerhedskontroller bør man som minimum orientere sig i det aktuelle trusselniveau udgivet af Center for Cybersikkerhed.

4.7.4 Driftsmæssige hensyn, regler og begrænsninger

I lyset af den senere tids hændelser med pandemi, forsyningsproblemer, krig og aggression er det blevet tydeligt at vi har opbygget nogle afhængigheder, som vi ikke længere kan basere vores samfund på. Samtidig er cyberkriminalitet særdeles lukrativt og omfattende. Vi kan således sjældent opretholde et præcist fjendebillede.

Blandt andet derfor kommer der til stadighed nye krav og hensyn. I øjeblikket er følgende blandt de særligt aktuelle på sikkerhedsområdet: Schrems II, NIS2 og tekniske minimumskrav for statslige myndigheder.

- NIS-direktivet er et EU-direktiv, der pålægger operatører af kritisk infrastruktur, f.eks. sundhed, energi, transport, vigtige udbydere af tjenester i informationssamfundet (e-handelsplatforme, sociale netværk o. lign.) og offentlige myndigheder at vedtage og implementere hensigtsmæssige foranstaltninger til styring af cybersikkerhedsrisici. Der vil blive ført tilsyn med overholdelsen af NIS-direktiverne. Der foreligger i skrivende stund en godkendt version af NIS2, men der skal være en national bearbejdning efterfølgende. Man bør orientere sig om indholdet af direktivet.
- Digitaliseringsstyrelsen m.fl. har udgivet et sæt tekniske minimumskrav for statslige myndigheder[52]. Der er her tale om nogle krav, der hører til sikkerhedsmæssig best practice og gælder alle myndighedens tjenester. Altså også dem, der driftes hos eksterne parter.

[52] https://sikkerdigital.dk/myndighed/tekniske-tiltag/tekniske-minimumskrav/tekniske-minimumskrav-2023

4.7.5 Henvisninger til eksempler på eksisterende standarder og vejledninger

Nedenstående er en liste over eksisterende standarder, forordninger, vejledninger og andet, som med fordel kan anvendes i arbejdet med udvikling og anskaffelse af systemer til sundhedssektoren:

Medicinsk udstyr: Lægemiddelstyrelsens definition af og krav til medicinsk udstyr

Lægemiddelstyrelsen er myndighed på området, som er omfattet af regler og krav fra EU og andre myndigheder. Man skal specielt være opmærksom på at definitionen rammer meget bredt, så også en del mobile apps og anden software havner under denne definition.

MDR: EU-forordning for medicinsk udstyr

IVDR: EU-forordning for medicinsk udstyr til in vitro diagnostik

HIPAA: Krav i forbindelse med samarbejde med eller eksport til USA (ENG)

Ønsker man at samarbejde med eller eksportere til USA, bør man kontrollere kravene i HIPAA for afklaring.

ISO27001/27002

Kan suppleres med ISO27799, hvor der er flere eksempler på sikkerhedskontroller, der kan implementeres for it-løsninger, der anvendes i sundhedsvæsenet

CIS-kontroller: Download CIS-kontroller her (ENG)

Dækker over en række håndgribelige og operationelle kontroller, som er udledt af mange års erfaring med bekæmpelse af cyberangreb.

SOC (Security Operations Centre): 10 strategier for opbygning af en SOC – af MITRE (ENG)

Publikationer fra ENISA: Europæiske publikationer, der dækker sundhedsområdet (ENG)

EU's organisation for Cybersikkerhed, ENISA, udgiver publikationer, som også dækker sundhedsområdet.

Pseudonymiseringsprincipper: Pseudonymiseringsprincipper for sundhedsdata (PDF)

4.7.6 Eksisterende løsningsbyggeblokke

Dette afsnit oplister og beskriver kort eksisterende løsningsbyggeblokke, der er en realisering af arkitekturbyggeblokke beskrevet i afsnit 4.5 samt øvrige løsningsbyggeblokke, der er relevante for informationssikkerhed ved implementering af løsninger.

Løsningsbyggeblok	**Kort beskrivelse**
Samtykkeservicen	Sundhedsdatastyrelsen har en samtykkeservice, der hedder "Min Spærring" og dokumentationen kan findes på nspop[53] Det forlyder at Digitaliseringsstyrelsen[54] arbejder på en samtykkeservice, men der er i skrivende stund ikke offentliggjort detaljerede referencer herom.
Fuldmagtservicen	Løsningsbyggeblok for fuldmagtsservicen drives og udvikles af Digitaliseringsstyrelsen som en fællesoffentlig tjeneste. Den er tilgængelig på Borger.dk
MinLog	MinLog modtager registreringer om adgang til borgeres data i de systemer, som registrerer logdata i MinLog. MinLog udstiller services til opslag, og der er webbrugerflader til borgeren på "sundhed.dk" og "fmk-online.dk", samt til borgeren og sundhedspersoner på "fmk-online.dk".
Behandlingsrelationsservice	Behandlingsrelationsservice
STS/autentifikation	STS/autentifikation
SEB	SEB
Fælles Stamkort - FSK	Formålet med Stamkortregistret er at give borgeren og relevante sundhedsfaglige aktører et fælles overblik over borgerens stamdata. Den kører i test på NSP. Den samler data fra CPR, ODR, TTS-BSR og SKR.

[53] https://www.nspop.dk/pages/viewpage.action?pageId=43544313
[54] https://digst.dk/media/22101/ny-bilag-3-statusredegoerelse-2019.pdf

5 Appendix

5.1 Uddybning af Principper

F2	**Internationale, nationale og lokale initiativer skal koordineres med henblik på genbrug af såvel nye som allerede etablerede løsningselementer, standarder og infrastruktur**
Beskrivelse	Sikkerheds udfordringer er universelle og grænseoverskridende. En tværgående koordinering hen over af landegrænser og sektorer om fælles initiativer, baseret på anerkendte standarder, styrker grundlaget for samarbejde om en fælles sikkerhedsopfattelse og indsats.
Rationale	Mange initiativer og politiske hensigtserklæringer handler om samarbejde og deling af data på tværs af landegrænser. En forudsætning for at dette kan opnås uden at kompromittere infrastruktur og data, er en tværgående koordinering af initiativerne. Sammenhæng kan skabes mere effektivt, målt såvel på lokale arbejdsprocessers effektivitet som på omkostninger til etablering af systemmæssige integrationer, når forskellige internationale og nationale initiativer koordineres og etableres efter samme standarder, centrale arkitekturprincipper og sikkerhedsparadigmer. › Lokale initiativer kan gennemføres mere effektivt under inddragelse af erfaringer fra eller ved samarbejde med andre lignende lokale initiativer i andre organisationer, hvor relevante standarder, forskningsresultater og internationale erfaringer inddrages. › Ved at sikre at danske standardiseringstiltag tager fornødent hensyn til internationalt standardiseringsarbejde bevares de størst mulige frihedsgrader i forhold til anvendelse af produkter udviklet på såvel det danske som det internationale marked i fuld konkurrence.
Implikationer	✓ Princippet indebærer en forpligtelse for alle parter i sundhedsvæsenet til at sikre overholdelse af standarder og koordinere med centrale funktioner. ✓ Alle parter skal være opmærksomme på deres ansvar, så sub-optimale løsninger eller varianter over allerede etablerede lignende løsninger ikke skabes med unødvendige udgifter og øgede sikkerhedsrisici til følge ✓ Etablering af en national infrastruktur og valg af anvendte standarder bidrager i væsentligt omfang til at sikre, at initiativer, som baseres på disse elementer optræder på en ensartet måde over for brugerne med et kendt og tilstrækkeligt sikkerhedsniveau.

F3	**Fælles løsninger skal respektere at samarbejdet sker mellem uafhængige juridiske enheder, som kan have egne regler, retningslinjer og processer**
Beskrivelse	Fælles løsningers succes afhænger af at man respekterer de involverede parters kontrol med eget miljø. Det er vigtigt at implementering af fælles løsninger ikke hindres af enkelte parters begrænsninger eller lokale politikker.
Rationale	Det er en forudsætning for at opbygge et sammenhængende sundhedsvæsen, at alle parter kan få adgang til relevante løsninger. Det kræver at de pågældende løsninger er udformet, så der er er taget højde for forskelligheder i parternes politikker, infrastruktur, strategier og governance. Dette i respekt for de registreredes rettigheder.
Implikationer	✓ Princippet medfører, at sundhedsvæsenets parter skal stille krav til deres systemleverandører om at overholde nationalt fastsatte vejledninger og sikkerhedsstandarder i overensstemmelse med denne referencearkitekturs anvisninger og inden for rammerne af gældende lovgivning. Der kan dog være markedsmæssige forhold, der begrunder konkrete afvigelser herfra. ✓ Dette fordrer, at de nationale rammer er formuleret tilstrækkeligt præcist, entydigt og operationelt og definerer et hensigtsmæssigt og tilstrækkeligt sikkerhedsniveau. ✓ Parterne bør endvidere afstå fra at stille krav til adgangsbegrænsende sikringsforanstaltninger i systemer, som ikke kan begrundes af nationalt fastsatte rammer (lovgivning, referencearkitekturer, standarder, vejledninger etc.). Eller – såfremt man indledningsvis vælger at basere sikkerhed på lokale rammer - at man er klar til at migrere til nationale rammer, når disse vurderes at være tilstrækkelige. ✓ Hvis de nationale rammer ikke findes tilstrækkelige er det vigtigt, at der arbejdes på at forbedre disse.

F6	**Løsninger, der produktionssættes, bør baseres på komponenter, der er driftsmodnede og har gode referencer fra andre anvendere/projekter**
Beskrivelse	Man skal, i det omfang det er muligt og hensigtsmæssigt, benytte løsninger og teknologier, der er gennemprøvede og tidssvarende, og som yder en tilstrækkelig beskyttelse af data og infrastruktur. Alle løsninger bør have en godkendt risikovurdering inden idriftsættelse.
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, og en efterfølgende vurdering af tilstrækkeligheden af de etablerede foranstaltninger. ✓ 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.

I1	**Ved deling af information fastlægges entydigt ansvar**
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 driftspartnere). Oplysninger kan ”videregives”. Hermed får den modtagende organisation dataansvaret for de oplysninger, den modtager og opbevarer. Hvis de videregivne oplysninger samtidig forbliver hos den afgivende organisation, vil denne stadig have dataansvaret for disse oplysninger, mens den modtagende organisation har et dataansvar for de oplysninger, som denne organisation har modtaget.
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 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.

I2	**Deling af struktureret information forudsætter fælles begrebsforståelse**
Beskrivelse	Der er behov for et stærkt fokus på, at grundlaget for kliniske, forskningsmæssige og administrative beslutninger er så entydigt som muligt. Princippet skal sikre, at den indholdsmæssige standardisering tilgodeses på lige fod med den tekniske standardisering, som en forudsætning for fuld interoperabilitet ved digital informationsdeling.
Rationale	› Man kan have tillid til validiteten af udvekslet information › Enighed om den semantiske sikkerhed for entydig betydning af modtaget information, medfører at modtager kan have fuld tillid til dennes informationsmæssige værdi, ikke mindst til sikkerhed for borgerne › Større effektivitet og kvalitet via genanvendelse af information › Semantisk entydighed er en forudsætning for realiseringen af de væsentligste forretningsmæssige målsætninger!
Implikationer	✓ Fælles klassifikationer og mapninger etableres o Parterne i sundhedsvæsenet baserer deres udveksling af information på klassifikationer og terminologier. Mapning mellem disse kan være nødvendig, men bør holdes på et minimum, da vedligeholdelse er ressourcekrævende. Derfor er der behov for fortsat udvikling og styring af disse områder nationalt ✓ Begrebsmodeller o En fælles grundlæggende forståelse af sundhedsvæsenets centrale begreber er af afgørende betydning. Hvert af disse begreber skal beskrives på en måde, der sikrer konsensus om en fælles betydning. Der er altså tale om behov for udvikling af en fælles terminologisk begrebsmodel for sundhedsvæsenet på et relativt højt abstraktionsniveau, som stadig tillader lokale implementeringer med større detaljeringsgrad, så længe den overordnede begrebsmodel overholdes.

I4	**Information opsamles én gang og genanvendes i alle relevante sammenhænge i overensstemmelse med regler for visning og anvendelse**

Beskrivelse	Det er af afgørende betydning for såvel kvalitet og sikkerhed som effektivitet, at relevant information er til rådighed og genanvendes, hvor der er muligt og hensigtsmæssigt. Patienter og borgere ønsker en service fra et mere sammenhængende sundhedsvæsen, hvor information flyder på tværs af organisatoriske grænser ligesom patienten selv gør det i et sammensat forløb, uden at information tabes undervejs. Medarbejdere i sundhedsvæsenet ønsker tilsvarende adgang til alt behandlingsrelevant information uanset hvor og hvornår den måtte være blevet tilvejebragt.
Rationale	Behandling sker på grundlag af al relevant information, som er indsamlet om patienten uanset hvor og hvornår, › Klinikernes tid anvendes effektivt, fordi information, som andre dele af sundhedsvæsenet allerede har tilvejebragt kan anvendes › Patienter oplever en bedre service både via kortere forløb, færre gentagne undersøgelser og en oplevelse af, at sygehistorien er kendt af alle organisatoriske enheder, som bidrager til behandlingen. › Kopiering og spredning af information gør det problematisk at sikre sporbarhed og validitet af disse, samtidig med at ønske om spærring er vanskeligt at overholde.
Implikationer	✓ Tilgængelighed af information på tværs af sundhedsvæsenet forudsætter etablering af fælles infrastruktur og fælles indholdsmæssige standarder, som tillader alle parter at anvende fælles data uanset hvor de findes.

I5	**Effektive foranstaltninger forebygger risici fremfor at afhjælpe dem**
Beskrivelse	Sikkerhed og sundhed har nogle fællestræk, idet det for begge er bedre at forebygge end at helbrede.
Rationale	Investeringer i proaktive tiltag kan ofte virke uoverskuelige, da man ikke har nogen sikkerhed for at man forhindrer netop de hændelser, der rammer en. Her benytter man sig af opdaterede risikovurderinger, efterretninger og sårbarhedsvurderinger for at sikre at foranstaltningerne følger med. Beredskabsplaner, genopbygningsplaner og tests er stadigt vigtige for at kunne håndtere situationer, hvor skaden er sket.
Implikationer	Forebyggelse skal implementeres på alle relevante niveauer i henhold til lovgivning, regelsæt og detaljerede risikovurderinger. Eksempelvis: ✓ Krypteret kommunikation ✓ Beskyttede linjer ✓ Krypterede databaser

	✓ Segmenterede netværk ✓ Administrativ funktionsadskillelse ✓ Teknisk funktionsadskillelse ✓ Code review ✓ Osv.

I6	**Ægte databeskyttelse implementeres som standardindstilling**
Beskrivelse	Databeskyttelse gennem standardindstillinger[55] betyder, at produkter allerede fra start er indstillet til at sikre en passende databeskyttelse. Dette gælder for fortroligheden, integriteten og tilgængeligheden. Samtidigt er det nødvendigt at sikre sig, at personlig information om en bruger kun bliver opbevaret, så længe som det er nødvendigt for at levere et produkt eller en service.
Rationale	Artikel 25 [56]i Databeskyttelsesforordningen stiller krav om gennemførelse af tiltag, så et givet systems standardindstillinger giver den sikkerhed der skal til for at beskytte de behandlede personoplysninger i tilstrækkelig grad. Kun ved at implementere disse indstillinger som standard, kan man sikre at persondata er passende beskyttet og ansvaret for eventuelle lempelser af sikkerhedsniveauet, påhviler den dataansvarlige.
Implikationer	Den dataansvarlige skal gennemføre passende tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles. Denne forpligtelse gælder den mængde personoplysninger, der indsamles, og omfanget af deres behandling samt deres opbevaringsperiode og tilgængelighed. Sådanne foranstaltninger skal navnlig gennem standardindstillinger sikre, at personoplysninger ikke uden den pågældende fysiske persons indgriben stilles til rådighed for et ubegrænset antal fysiske personer.

[55] https://www.datatilsynet.dk/Media/7/C/Behandlingssikkerhed%20og%20databeskyttelse%20gennem%20design%20og%20standardindstillinger%20(2).pdf

[56] https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.DAN&toc=OJ:L:2016:119:FULL#d1e3052-1-1

I7	**Effektiv databeskyttelse tænkes ind i systemers arkitektur fra starten.**
Beskrivelse	Beskyttelse af persondata og andre følsomme eller fortrolige oplysninger skal designes ind i digitaliseringen af databehandlinger og opbevaring allerede fra starten.
Rationale	Artikel 25[56] i Databeskyttelsesforordningen stiller krav om gennemførelse af tiltag, der sikrer at databeskyttelse bygges ind i produkterne fra starten. Det skal sikres, at virksomheden indarbejder databeskyttelse som en integreret del af virksomhedens krav til produkter, forretningsprocesser, værdikæde og produktlivscyklus. Lige fra produktionsfasen til produktet ikke længere skal anvendes.
Implikationer	Den dataansvarlige skal gennemføre, både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen, passende tekniske og organisatoriske foranstaltninger, såsom, men ikke begrænset til, pseudonymisering, dataminimering, segmentering, funktionsadskillelse og kryptering.

A2	**Overvej opsplitning af store, komplekse systemer i mindre, simplere komponenter, der kan udvides på længere sigt.**
Beskrivelse	Det er svært at garantere sikkerheden i store systemer med høj kompleksitet. Derfor kan det være både bedre og billigere at benytte sig af mindre, afgrænsede byggeblokke, der kan levere en veldefineret overskuelig funktionalitet med et veldefineret sikkerhedsniveau.
Rationale	Kompleksitet er sikkerheds fjende. Det er vigtigt at funktionalitet, dataflows og rettigheder er tydelige og gennemskuelige, for at man kan gennemføre en retvisende risikovurdering, og dermed sikre at systemer, infrastruktur og processer beskyttes i tilstrækkelig grad. Også ved krav om certificeringer, kan der være fordele ved at kunne udskille givne funktionaliteter.
Implikationer	› Bedre mulighed for at tilpasse, opgradere, patche og vedligeholde komponenterne › Bedre overblik over komponenterne og identificering af deres sårbarheder.

A3	**Applikationer og komponenter skal kunne indgå i et nationalt økosystem for sundhedsvæsenet.**
Beskrivelse	Det er derfor vigtigt, at applikationer og komponenter udformes på en måde, så de vil kunne indgå i og understøtte et eventuelt fremtidigt økosystem for sundhedsvæsenet.
Rationale	Udviklingen i systemlandskabet går mod brug af agile metoder, for hurtigt og fleksibelt at kunne levere løsninger, der understøtter forretningsbehovene, bl.a. ved genbrug af fælles løsningselementer. Det er derfor vigtigt, at applikationer og komponenter udformes på en måde, så de vil kunne indgå i og understøtte et fremtidigt økosystem for sundhedsvæsenet, med standardiserede sikkerhedsfeatures, kendte risikoprofiler, og nemmere vedligehold. › Hurtig udvikling af nye produkter. › Genbrug af fælles komponenter › Lette inddragelse af mange uafhængige leverandører
Implikationer	Der skal foretages risiko analyser før under og efter et udviklingsforløb og man skal, i hele produktets levetid, finde den gode balance mellem hensynet til databeskyttelse, cybersikkerhed, økonomi, lovoverholdelse og ønsket funktionalitet.

A4	**Passende databeskyttelse skal afpasse funktionaliteten, så både den ønskede funktionalitet og den nødvendige sikkerhed understøttes.**
Beskrivelse	Et modsætningsforhold mellem sikkerhed og funktionalitet i det færdige produkt, er skadeligt for udbyttet af den gevinst produktet burde give.
Rationale	Digitalisering foretages for at opnå gevinster, enten i kvalitet, produktivitet, hastighed, tilgængelig eller andet. Hvis dette sker på bekostning af sikkerheden, vil man få øgede omkostninger til eksterne sikkerhedstiltag, eller oprettelser efter sikkerhedshændelser. På den anden side vil en restriktiv sikkerhedsmodel, der hæmmer funktionaliteten, medføre at anvendere vil finde måder at omgå sikkerheden på.
Implikationer	Der skal foretages risiko analyser før under og efter et udviklingsforløb og man skal, i hele produktets levetid, finde den gode balance mellem hensynet til databeskyttelse, cybersikkerhed, økonomi, lovoverholdelse og ønsket funktionalitet.

A5	**Det sikreste sted at beskytte data er ved kilden.**
Beskrivelse	Informationer/data er det store omdrejningspunkt i de fleste af de løsninger der benyttes i sundhedssektoren. Det sted de beskyttes bedst er der hvor de opbevares.
Rationale	Hvis man beskytter data i opbevaringen, vil de have samme beskyttelse uanset hvilken vej og med hvilke midler man tilgår data. Og anvendere vil kunne tilgå data med de værktøjer og protokoller de foretrækker.
Implikationer	Data skal beskyttes på database niveau, hvis det overhovedet er muligt. Det indebærer at: ✓ rettighedsstyringen ligger på databaseniveau ✓ databasen er krypteret ✓ kommunikationen med database-serveren er krypteret ✓ adgangen til data sker gennem sikkerhedsforanstaltningerne på databasen

T1	**Anvend fælles infrastrukturkomponenter til effektivt at sikre et ensartet og højt sikkerhedsniveau i kommunikation mellem parter**
Beskrivelse	Med mindre gode grunde taler herfor, bør man benytte den allerede etablerede (og sikrede) infrastruktur til kommunikation mellem sundhedsvæsenets parter. Er der behov for yderligere sikring af infrastrukturen, vil en sådan komme alle parter, der benytter infrastrukturen til gode.
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 nationale infrastrukturkomponenter, tilstræbes det er parterne sikre på at operere indenfor nationalt fastsatte sikkerhedsmæssige rammer. Eksempelvis bør følgende nationale infrastrukturkomponenter indgå i overvejelserne, når kommunikationsløsninger etableres mellem parter på sundhedsområdet: › Sundhedsdatanettet (SDN) til generel sikring af kommunikation mellem parter. › MitID og NemLogin når den skal logges på web applikationer / browserløsninger. › Den nationale serviceplatform (NSP) og de sikkerhedskomponenter, der er etableret på denne, når der skal udstilles (web-) services til andre parter. › Den fællesoffentlige sundhedsportal (Sundhed.dk), når der skal anvendes fælles (web-)applikationer. › Det af MedCom etablerede videoknudepunkt, når der skal etableres videokonferencer mellem parterne.

Implikationer	Inden der etableres nye kanaler til kommunikation mellem sundhedsvæsenets parter, skal det overvejes, om eksisterende kanaler kan benyttes (evt. efter udbygning). Et eventuelt fravalg af eksisterende infrastrukturkomponenter skal kunne begrundes (følg-eller-forklar-princippet). Princippet fordrer, at de fælles infrastrukturløsninger er sikret på et tilstrækkeligt højt niveau, og at nationale infrastrukturløsninger skal være de første til at overholde nationale rammer.

T2	**Teknisk interoperabilitet opnås gennem anvendelse af udbredte, åbne standarder**
Beskrivelse	Princippet vedr. semantisk entydighed er kun den ene halvdel af løsningen på problemet at skabe sikker, klinisk meningsfuld, digital sammenhæng. Den anden del vedrører de tekniske forhold, som sikrer, at forskellige parters forskellige systemer reelt kan udveksle information med hinanden. Området er i høj grad præget af internationale og nationale standarders forsøg på at skabe et fundament, som sikrer at compliance også garanterer interoperabilitet. Teknisk standardisering er et væsentligt element i fremtidssikring af sundhedsvæsenets nutidige investeringer i komponenter til arkitekturen. Standardisering skal sikre at komponenter anskaffet i dag kan anvendes relativt problemfrit sammen med fremtidige komponenter.
Rationale	Direkte integration er mulig på basis af veletablerede standarder, som understøttes bredt af mange leverandører, til gavn for både sikkerhed, fleksibilitet og økonomi. › Mindre binding til enkelte leverandører opnås ved, at sundhedsvæsenets parter ved udbredt anvendelse af standarder ikke er bundne til bestemte leverandører af bestemte komponenter, men til hver en tid kan udskifte disse med andre, som overholder samme standarder med begrænsede konsekvenser › Øget konkurrence opnås ved at sundhedsvæsenet indkøber løsninger, som er baseret på udbredte standarder. Derved sikres det, at såvel danske som internationale leverandører har en interesse i at levere løsninger til sundhedsvæsenet og at disse kan anvendes internationalt.
Implikationer	Hvis der ikke findes relevante standarder, eller de der findes er utilstrækkelige, vil udvalgte parter, efter vurderet behov, bidrage aktivt til profilering eller (videre)udvikling af sådanne. Anvendelsen af standarder betyder både fordele og potentielle ulemper f.eks.; ✓ Nemmere dokumentation af compliance ✓ Princippet betyder, at man i almindelighed må give afkald på den totale fleksibilitet i forhold til udformning af løsninger, som man ellers har. ✓ Anvendelsen af lokale standarder prioriteres lavere end anvendelse af udbredte, internationale standarder.

T3	**Uafhængighed af leverandører styrkes ved anvendelse af bredt understøttede teknologier**
Beskrivelse	Anvendelse af udbredte åbne teknologier samt best practices inden for governance, sikkerhed, processer og metoder skal sikre, at it-arkitekturen bliver konstrueret ud fra sunde, anerkendte principper, så den er maksimalt fleksibel over for en fremtid, som vil være præget af, at ændringer i såvel teknologi og trusselsbillede som i sundhedsdomænet sker uforudsigeligt og konstant. Åbenhed skal således forstås bredt: › Fri adgang til leverandøruafhængig vedligeholdelse og videreudvikling af kildekode enten via en open source-konstruktion eller kundens ejerskab af rettighederne til kildekoden. › Krav stilles så flere leverandører kan overholde dem, fx ved at anvende åbne, internationale standarder frem for snævrere nationale › Dokumentation af kildekode m.v. udvikles med det formål, at al relevant information er tilgængelig for en evt. fremtidig tredjeparts overtagelse af vedligeholdelses- og driftsopgaven › Udviklingsprocesser, der anvendes internt såvel som eksternt, er åbne og gennemskuelige, så ejere af projekter og systemer har fuld indsigt i disse.
Rationale	› Komponenter, som etableres i overensstemmelse med princippet kan vedligeholdes både af leverandøren og af tredjemand efterfølgende › Komponenter kan udskiftes med alternative komponenter evt. fra andre leverandører efterhånden som nye, bedre alternativer markedsføres af såvel lokale som internationale leverandører › Når en arkitektur og komponenterne, som indgår i denne, er designet med åbenhed for øje ud fra etablerede og anerkendte kriterier for ”gode løsninger”, er sundhedsvæsenets investeringer sikret bedst muligt imod hastig forældelse og dennes følgevirkninger.
Implikationer	Der skal vælges et sæt af åbne standarder, som leverandører af komponenter til infrastrukturen kræves at overholde Nærværende arkitekturprincipper udmøntes i specifikke krav om leverandørers overholdelse af best practice, fx dokumentationsmæssigt, sikkerhedsmæssigt og arkitekturmæssigt. Der er typisk større omkostninger på kort sigt forbundet med overholdelse af et sæt af standarder sammenlignet med en situation, hvor leverandører tillades at anvende egne proprietære formater og arkitekturer. Kunden påtager sig et større ansvar for løsningernes udformning.

T4	**Non-funktionelle krav indtænkes fra starten**
Beskrivelse	Udviklingen medfører at såvel borgere som sundhedspersonale bliver stadig mere afhængige af IT-baserede sundhedstjenester. Der stilles derfor stadig større krav til disses non-funktionelle egenskaber, f.eks. evnen til at: › kunne håndtere mange samtidige brugere og transaktioner › opretholde en høj datasikkerhed › sikre høj tilgængelighed og god performance › understøtte nye teknologier › kunne videreudvikle eller ændre funktionaliteten. › overholde lokale og nationale lovgivninger, krav og standarder Dertil kommer af non-funktionelle krav ofte vil have implikationer for den grundlæggende arkitektur f.eks. fsva. skalerbarhed, robusthed og sikkerhed. Endelig vil visse non-funktionelle krav i praksis sjældent blive effektivt opretholdt, hvis de ikke opfyldes fra starten, dette gælder f.eks. krav til arkitekturbeskrivelser.
Rationale	› Vanskeligt nedbrydelige barrierer for de non-funktionelle krav kan uforvarende bygges ind, såfremt der ikke tages højde for dem fra begyndelsen › Skalerbarheden af en samlet arkitektur kan begrænses i mange forskellige dele af den og begrænsningerne kan udløses af forskellige typer af belastning mv. Det er derfor vigtigt, at alle dele af en kompleks arkitektur optimeres mhp. opnåelse af god skalerbarhed › Når arkitekturen er designet med god skalerbarhed for øje, kan man alene ved at tilføre yderligere hardware bringe den til at håndtere stigende belastninger uden yderligere investeringer i software. › Når arkitekturen er veldokumenteret vil ændringer lettere kunne implementeres › Sikkerheden styrkes når der er taget højde for den i det grundlæggende design.
Implikationer	For at sikre opfyldelsen af non-funktionelle krav samlet set i en distribueret arkitektur er det nødvendigt at stille krav til alle komponenter, som indgår i den samlede værdikæde. Der skal derfor ✓ Udarbejdes SLA'er for alle komponenter og lag i arkitekturen ud fra de samlede forventninger til fremtidig belastning ✓ Udarbejdes og anvendes principper for test ✓ Udarbejdes principper for Service Level Management, som sikrer at kvaliteten af services overvåges på en ensartet måde mhp. identifikation af problemer med Quality of Service (QoS).

T5	**Den nationale infrastruktur er standardiseret og integrationer hertil ligger lokalt**
Beskrivelse	Princippet fastlægger en ansvarsfordeling for en løbende konvergens af lokale systemer over tid. Dette opnås bl.a. ved, at den nationale infrastruktur baserer sig på udvalgte standarder. Dermed vil der opstå situationer, hvor lokale systemer, som ikke anvender samme standarder må tilpasse sig disse enten via udvikling (typisk på længere sigt) eller via mapning (typisk på kort til mellemlangt sigt).
Rationale	› En effektiv implementering af infrastrukturen › Dybt kendskab til de enkelte komponenters modeller og grænseflader bevares hos den part, der ejer dem og drifter dem › En klar ansvarsfordeling mellem den decentrale og den nationale infrastruktur. › En fælles sikkerhedsbaseline, der ikke er styret af lokale behov
Implikationer	› Lokale systemers tilpasning til infrastrukturen sker lokalt. › Infrastrukturen bygger ikke på viden om specifikke lokale løsninger, modeller eller protokoller › Værktøjer af generel karakter som støtter lokal anvendelse af infrastrukturen kan stilles til rådighed fra centralt hold, men skal konfigureres lokalt (fx ved implementering af mapninger imellem lokale og nationale klassifikationer eller modeller). › Det skal tilses at lokale suboptimeringer ikke kompromitterer den nationale infrastruktur.

T6	**Driftsmæssig kontinuitet af komponenter og services, som indgår i den nationale infrastruktur, skal sikres**
Beskrivelse	I den nationale sundheds-it-arkitektur anvender mange parter såvel centralt som decentralt driftede komponenter og services i tæt samspil med egne systemer og komponenter. Dermed øges afhængigheden af forhold uden for den enkelte parts egen kontrol. Det er derfor af stor vigtighed, at sådanne fælles komponenter og services dels › Udformes så de har en høj grad af driftsstabilitet, tilgængelighed og robusthed, dels › Opgraderes i mindst mulige skridt, så konsekvenser af evt. problemer minimeres.
Rationale	› Ved at mindske afhængighederne imellem fælles services mest muligt kan nye versioner idriftsættes isoleret fra andre services i vidt omfang, hvorved evt. problemer i enkelte nye services breder sig minimalt til andre › Ved at iagttage sunde principper for change management kan ændringer af den nationale konfiguration ske så kontrolleret som muligt.
Implikationer	› Best practice for service management skal iagttages › Best practice for design, udvikling og test af kritiske services iagttages.

T7	**Optimale sikringsforanstaltninger måles og forbedres løbende for at sikre kvalitet og effektivitet.**
Beskrivelse	I takt med at nye muligheder opstår, og/eller trusler ændrer sig eller skifter karakter, skal det overvejes om de aktuelle foranstaltninger med fordel kan udskiftes eller tilpasses for at matche det nødvendige sikkerhedsniveau.
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. Valgte sikkerhedsforanstaltninger skal løbende vurderes op mod de reviderede risikovurderinger og de faktisk oplevede forhold, for at sikre at effekten er tilstrækkelig og foranstaltningerne virker efter hensigten. Er der ikke overensstemmelse mellem forventningerne og resultatet, skal sikringsforanstaltningerne revurderes og ændres, så de stemmer overens med den effekt og det niveau der er valgt på baggrund af risikovurderingen.

6 Bilag A - Ønsker

Ønsker affødt af arbejdet med referencearkitekturen

- Tekniske retningslinjer for sikker transport af data
- Retningslinjer for kryptering
- Kriterier for anonymisering
- Initiativer til løsninger der kan benyttes af mindre organisationer.
- Byggeblokke for Sporbarhed og uafviselighed
- Efterhånden som arbejdet med nationale byggeblokke konsolideres og bliver beskrevet og defineret, vil de blive medtaget i nærværende referencearkitektur.
- Borgerautentifikation

7 Bilag B – Begreber

Begreb	Beskrivelse	Kilde
aktuel behandling	Er en patients igangværende sundhedsfaglige indsats udført af en sundhedsperson eller en sundhedsorganisation.	Sundhedsloven
Akkreditiver	Se identifikationsmiddel	Referencearkitektur for brugerstyring v 1.09
anonymisering	Oplysninger, der er gjort anonyme, sådan at ingen fysiske personer kan identificeres ud fra oplysningerne eller i kombination med andre oplysninger, er ikke længere beskyttet af databeskyttelsesreglerne. Det skyldes, at databeskyttelsesreglerne kun finder anvendelse, så længe oplysningerne kan føres tilbage til en identificerbar eller identificeret fysisk person. Det er en betingelse, at **anonymiseringen** er uigenkaldelig.	Hvad er personoplysninger?
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.	Dette dokument
autentifikation	Proces som genkender og verificerer en digital identitet gennem anvendelse af et identifikationsmiddel, der er koblet til identiteten.	Referencearkitektur for brugerstyring v 1.09

	Ved multifaktor autentifikation forstås en autentifikationsproces, hvor det anvendte Elektroniske Identifikationsmiddel tilvejebringer flere Autentifikationsfaktorer fra forskellige kategorier	National Standard for Identiteters Sikringsniveauer (NSIS) Version 2.0.1a (PDF)
autorisation	tilladelse der tildeles en bruger, så denne kan benytte et informationssystem	Sundhedsvæsenets begrebsbase (NBS)
autoriseret bruger	En autoriseret bruger er en bruger, der har fået tildelt adgangsrettigheder til funktioner eller data i et informationssystem	Rapport fra nbs06
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 geografisk afgrænsning. En sundhedsproducerende enhed danner rammen for de sundhedsprofessionelles sundhedsaktiviteter	Sundhedsvæsenets begrebsbase (NBS)
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	Sundhedsloven
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[23].	Sundhedsloven

	Hvis en sundhedsperson overdrager retten til at indhente patientrelateret information på sine vegne til en anden, er dette reguleret via Sundhedslovens[24] §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.	
entitet	En fysisk person eller juridisk enhed, som ønsker adgang til en tjeneste gennem Autentifikation med Elektroniske Identifikationsmidler. En Entitet kan have flere Identiteter – fx kan en fysisk person både have en privatidentitet og flere erhvervsidentiteter.	National Standard for Identiteters Sikringsniveauer (NSIS) Version 2.0.1a (PDF)
fortrolighed	Egenskab ved informationssystem der medfører, at kun bestemte brugere har adgang til bestemte data eller bestemt information	ISO 27001
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.	Forældreansvarsloven
fuldmagt	Tilladelse, som en person giver til en anden person, sådan at denne bliver umiddelbart berettiget og forpligtet over for tredjemand ved handlinger, som den befuldmægtigede foretager i fuldmagtsgiverens navn og indenfor fuldmagtens grænser	Aftaleloven
identifikationsmiddel	Identifikationsmiddel omfatter altid både det udstedte og bindingen mellem det udstedte og en digital identitet.	Referencearkitektur for brugerstyring v 1.09
identitet	En digital persona repræsenteret ved et sæt af attribut- ter, som fx kan repræsentere en fysisk person (privat- identitet), en juridisk enhed (virksomhedsidentitet), eller en fysisk person, der	National Standard for Identiteters Sikringsniveauer (NSIS) Version 2.0.1a (PDF)

	er associeret med en juridisk enhed (fx erhvervsidentitet). En Identitet kan rumme Personidentifikationsdata men kan også være pseudonym.	
integritet	Egenskab ved et informationsaktiv, der sikrer at data er korrekte og fuldstændige, og at der ikke er foretaget uautoriseret ændringer af data	ISO 27001
Frabedelse af indhentning	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.	Sundhedsloven
Organisatorisk sikringsforanstaltning	Sikringsforanstaltning der benytter organisatoriske midler 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	ISO 27001

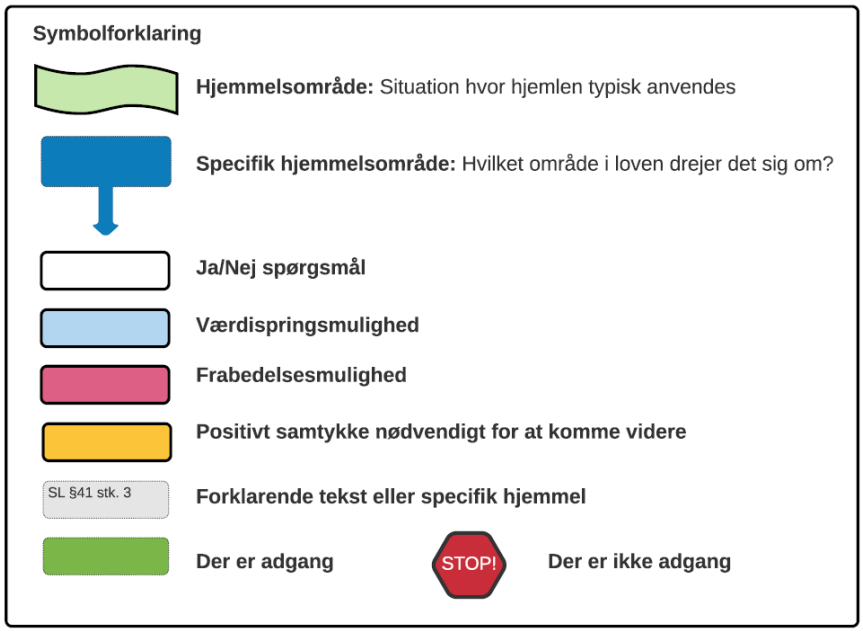
	- ledelsesbeslutninger	
pseudonymisering	Behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger.	Persondataforordningen
privacy (”privatlivets fred”)	egenskab ved data, information eller informationssystem der beskytter potentielt personhenførbar information mod at komme i forkerte hænder.	Dette dokument
privacy-by-design	Egenskab for at den dataansvarlige allerede fra tidspunktet, hvor midlerne for behandlingen fastlægges, skal gennemføre passende tekniske og organisatoriske foranstaltninger.	Persondataforordningen
privacy-by-default	tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles.	Persondataforordningen
samtykke	egenskab ved patientrelateret information, der giver en person mulighed for frivillig 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 databeskyttelsesforordningens (Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger) 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.	Dette dokument Persondataforordningen Sundhedsloven

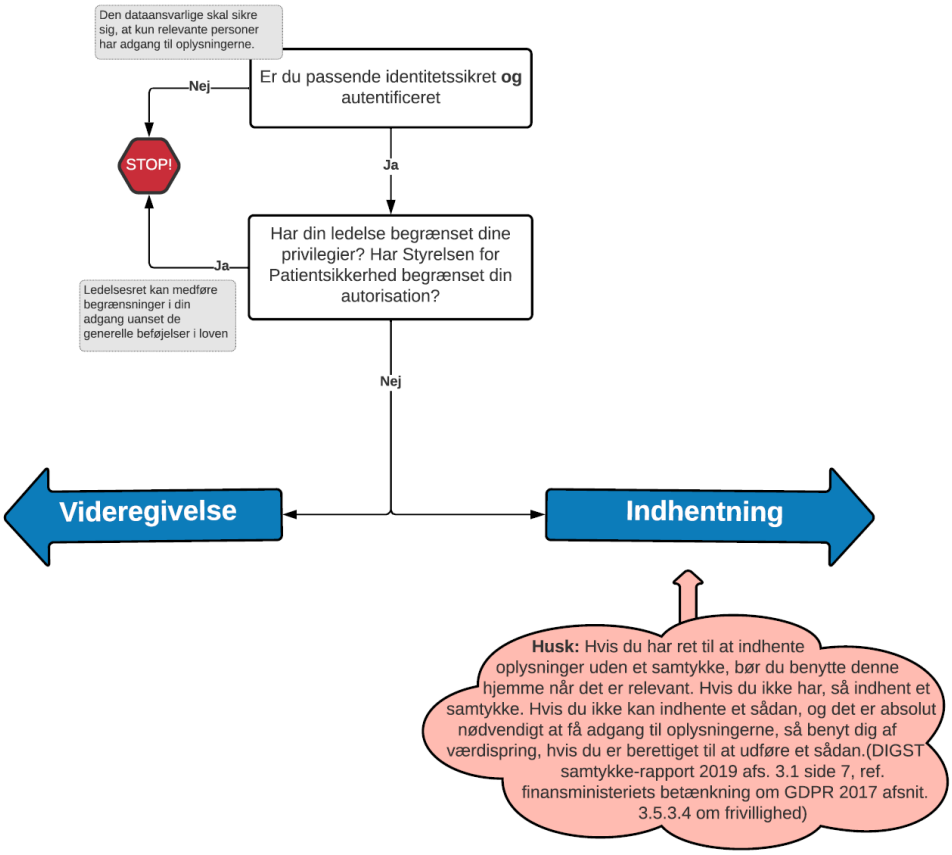
sikringsforanstaltning	Foranstaltning der har til formål at øge informationssikkerhed	ISO 27001
sikringsniveau	Graden af tillid til en autentificeret identitet. (LoA – Level of Assurance) Omfatter både tekniske, organisatoriske og økonomiske forhold	Referencearkitektur for brugerstyring v 1.09
sundhedsaktivitet (sundhedsfaglig opgave)	Sundhedsrelateret aktivitet, der er rettet mod én patient	Sundhedsvæsenets begrebsbase (NBS)
sundhedsperson	Person, der er autoriseret i henhold til særlig lovgivning til at varetage sundhedsfaglige opgaver, og personer, der handler på disses ansvar	Sundhedsloven
sundhedsorganisation	En organisation, der danner ramme for sundhedsprofessionelles sundhedsaktiviteter.	Sundhedsvæsenets begrebsbase (NBS)
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)	ISO 27001
tilgængelighed	egenskab ved service der sikrer, at servicen er til rådighed for en bruger i henhold til fastlagte rammer	ISO 27001

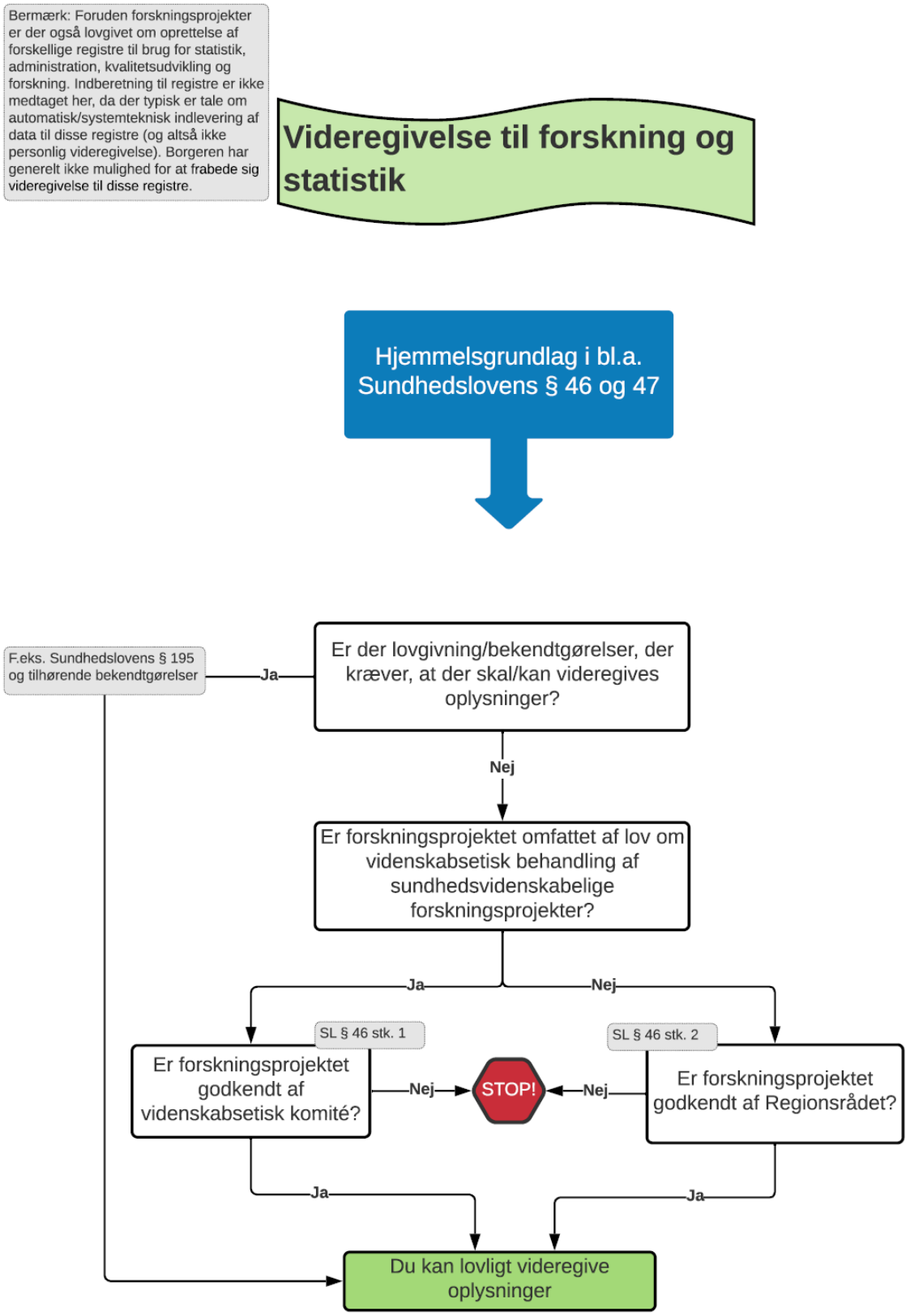
uafviselighed	egenskab ved information der gør det muligt at bevise, at en given bruger har udført en given handling på et givet tidspunkt	ISO 27001

8 Bilag C - Videregivelse og indhentning

Videregivelse og indhentning af personoplysninger i sundhedsvæsenet

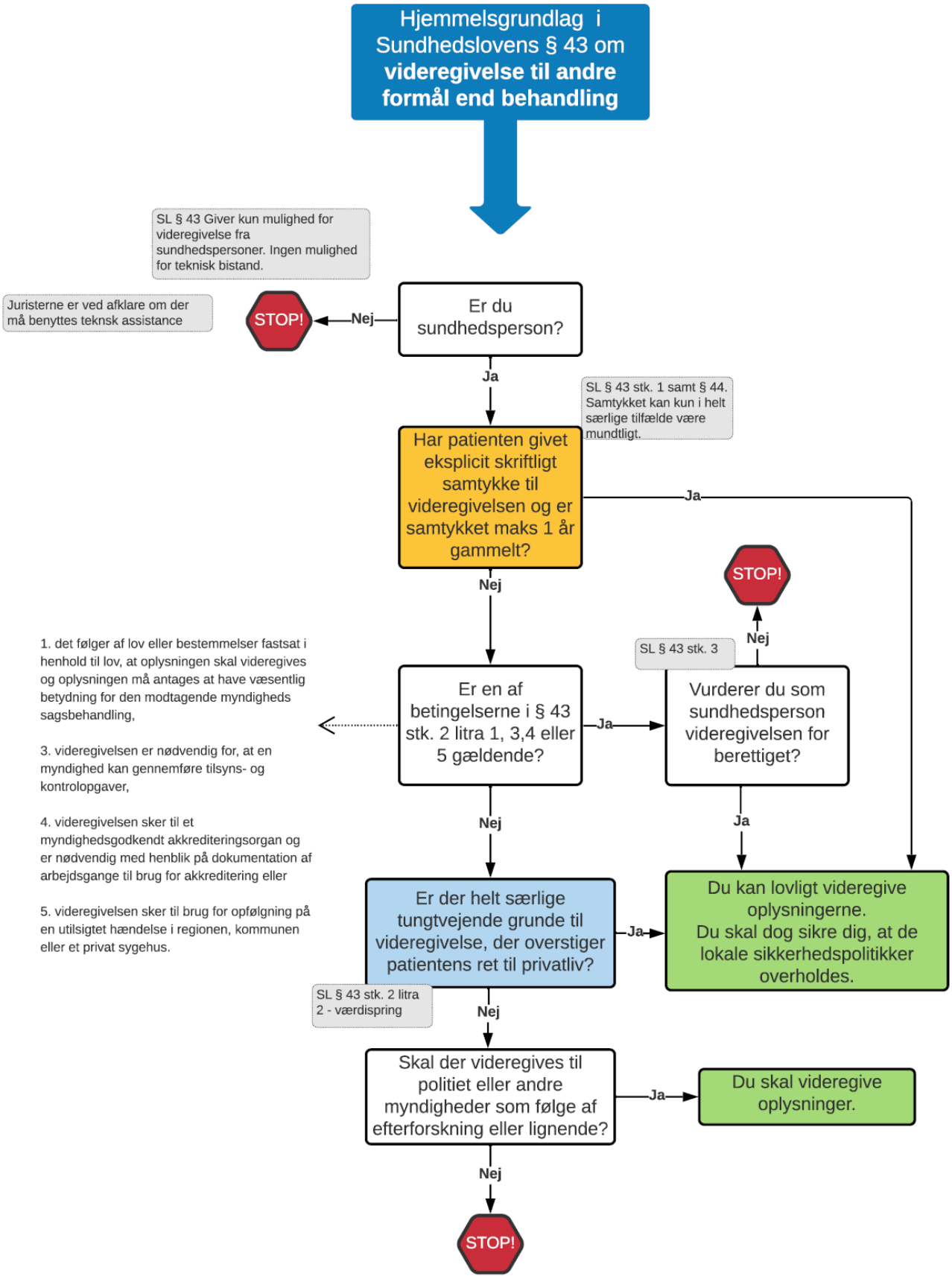



Den dataansvarlige skal sikre sig, at kun relevante personer har adgang til oplysningerne.
Er du passende identitetssikret og autentificeret
Nej
STOP!
Ja
Har din ledelse begrænset dine privilegier? Har Styrelsen for Patientsikkerhed begrænset din autorisation?
Ja
Ledelsesret kan medføre begrænsninger i din adgang uanset de generelle beføjelser i loven
Nej
Videregivelse
Indhentning
Husk: Hvis du har ret til at indhente oplysninger uden et samtykke, bør du benytte denne hjemme når det er relevant. Hvis du ikke har, så indhent et samtykke. Hvis du ikke kan indhente et sådan, og det er absolut nødvendigt at få adgang til oplysningerne, så benyt dig af værdispring, hvis du er berettiget til at udføre et sådan.(DIGST samtykke-rapport 2019 afs. 3.1 side 7, ref. finansministeriets betænkning om GDPR 2017 afsnit. 3.5.3.4 om frivillighed)

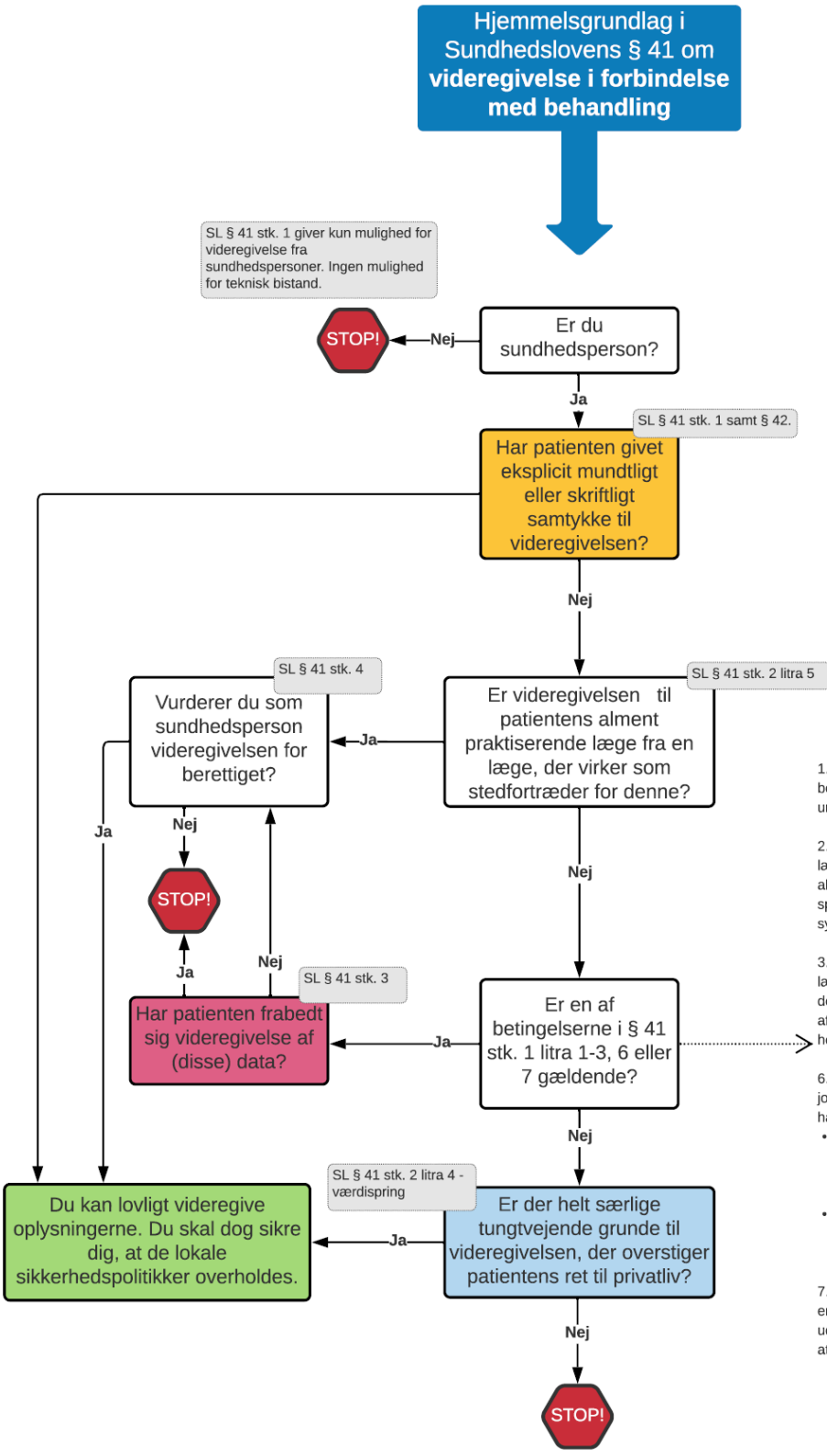

Bermærk: Foruden forskningsprojekter er der også lovgivet om oprettelse af forskellige registre til brug for statistik, administration, kvalitetsudvikling og forskning. Indberetning til registre er ikke medtaget her, da der typisk er tale om automatisk/systemteknisk indlevering af data til disse registre (og altså ikke personlig videregivelse). Borgeren har generelt ikke mulighed for at frabede sig videregivelse til disse registre.
Videregivelse til forskning og statistik
Hjemmelsgrundlag i bl.a. Sundhedslovens § 46 og 47
F.eks. Sundhedslovens § 195 og tilhørende bekendtgørelser
Ja
Er der lovgivning/bekendtgørelser, der kræver, at der skal/kan videregives oplysninger?
Nej
Er forskningsprojektet omfattet af lov om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter?
Ja
Nej
SL § 46 stk. 1
Er forskningsprojektet godkendt af videnskabsetisk komité?
Nej
STOP!
Nej
SL § 46 stk. 2
Er forskningsprojektet godkendt af Regionsrådet?
Ja
Ja
Du kan lovligt videregive oplysninger

SUNDHEDSDATA-
STYRELSEN

Videregivelse til andre formål end behandling



Videregivelse i forbindelse med behandling



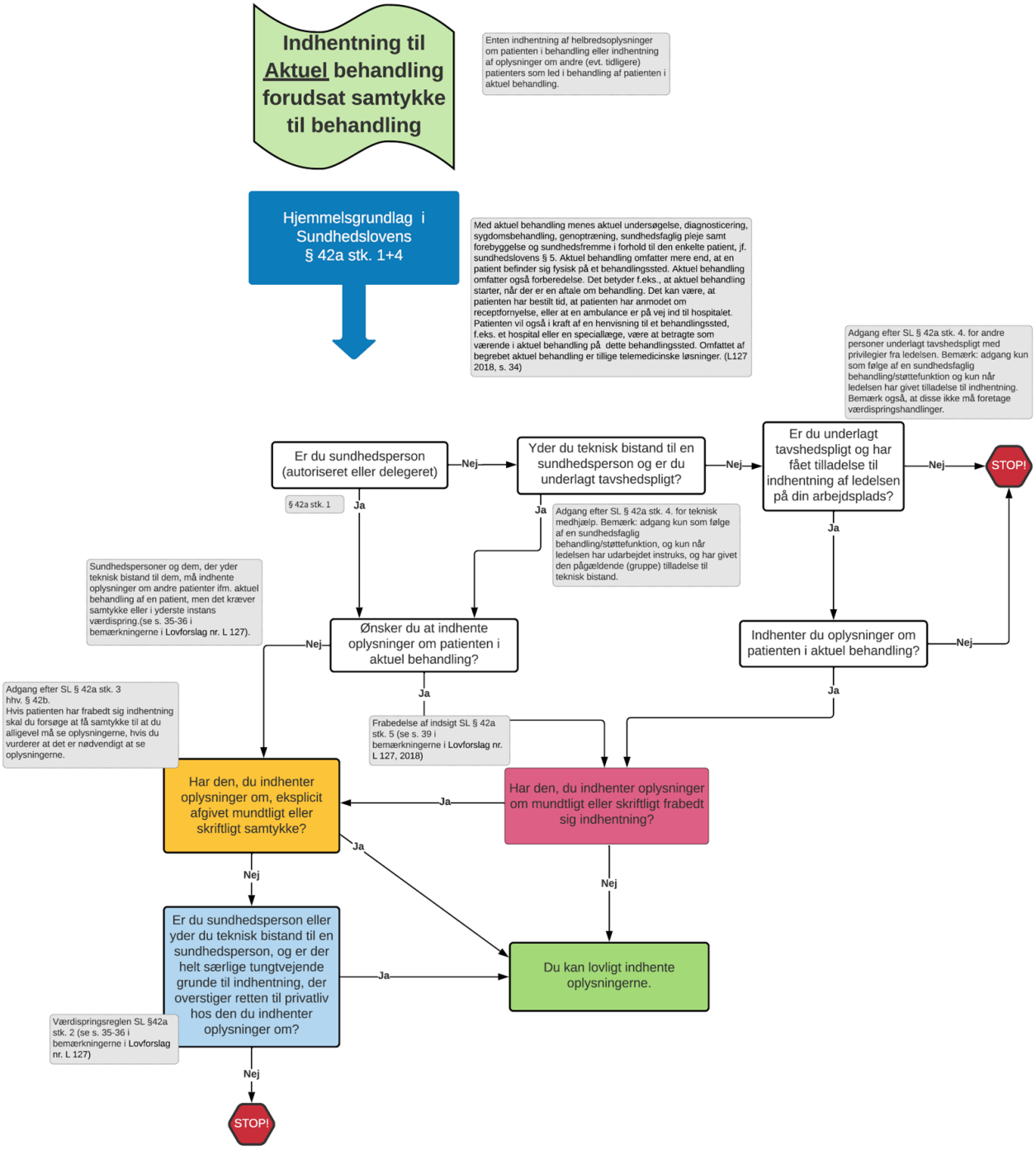
1. det er nødvendigt af hensyn til et aktuelt behandlingsforløb for patienten, og videregivelsen sker under hensyntagen til patientens interesse og behov,

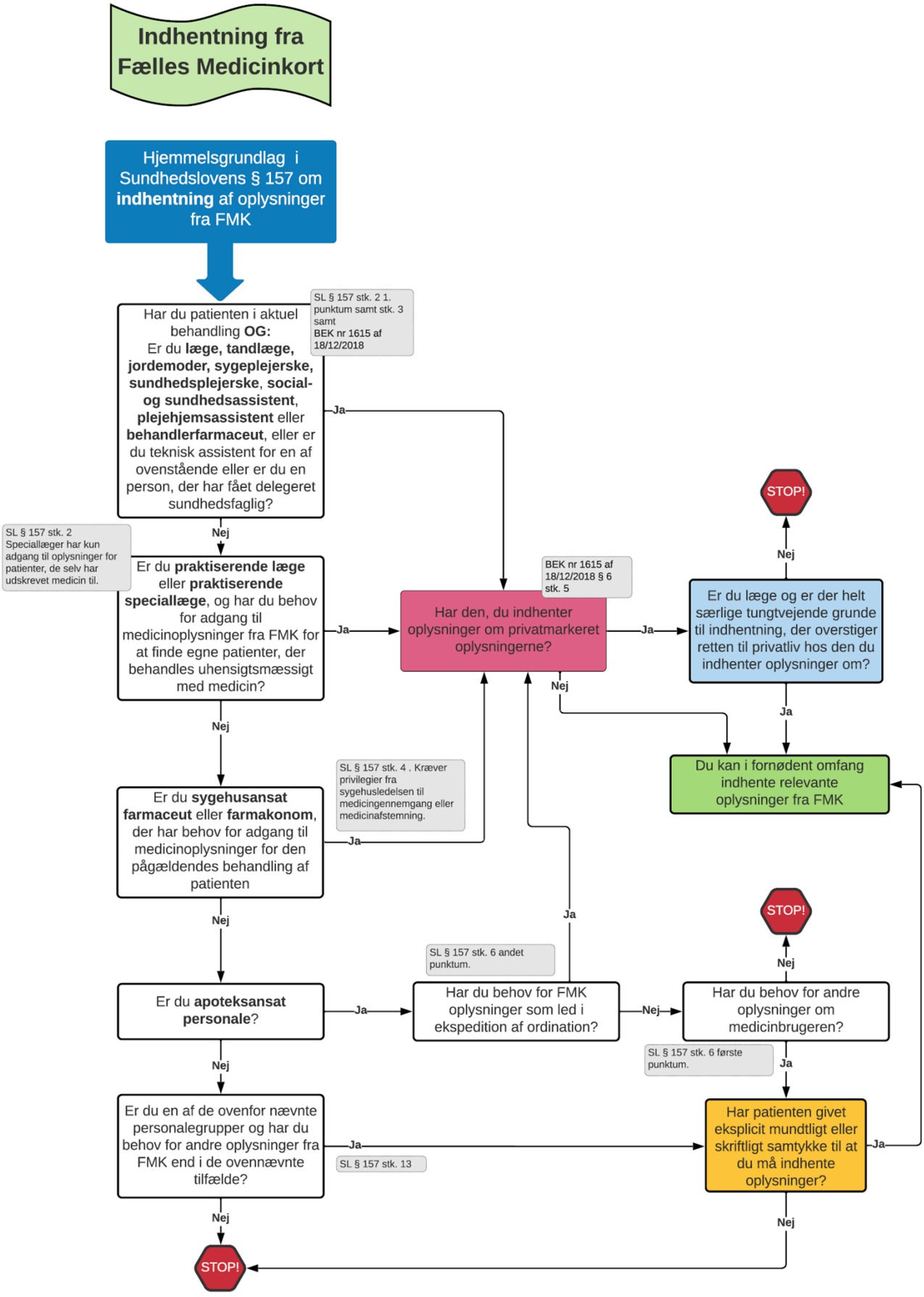
2. videregivelsen omfatter et udskrivningsbrev fra en læge, der er ansat i sygehusvæsenet, til patientens alment praktiserende læge eller den praktiserende speciallæge, der har henvist patienten til sygehusbehandling,

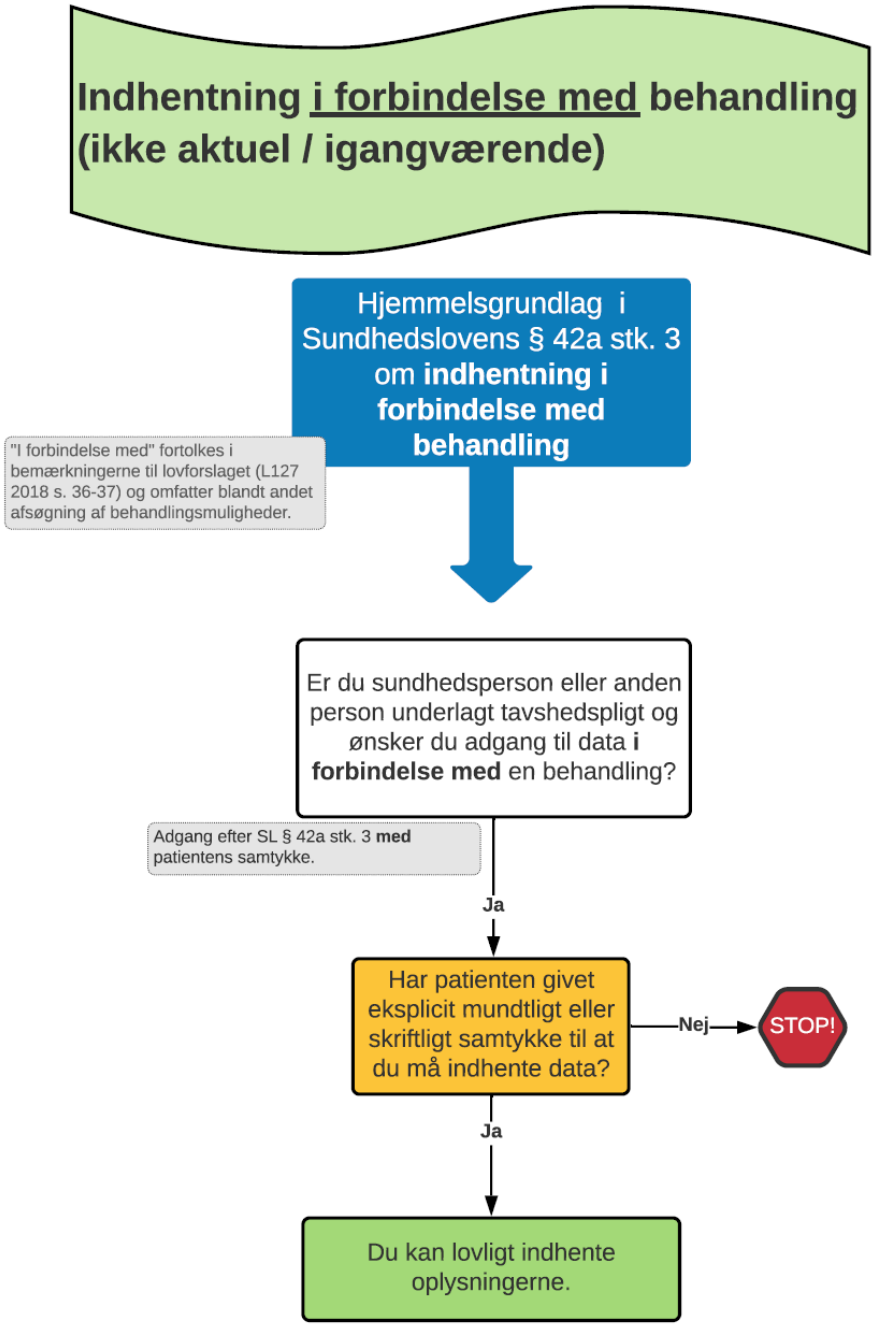
3. videregivelsen omfatter et udskrivningsbrev fra en læge, der er ansat på privatejet sygehus, klinik m.v., til de i nr. 2 nævnte læger, når behandlingen er ydet efter aftale med et regionsråd eller en kommunalbestyrelse i henhold til denne lov,

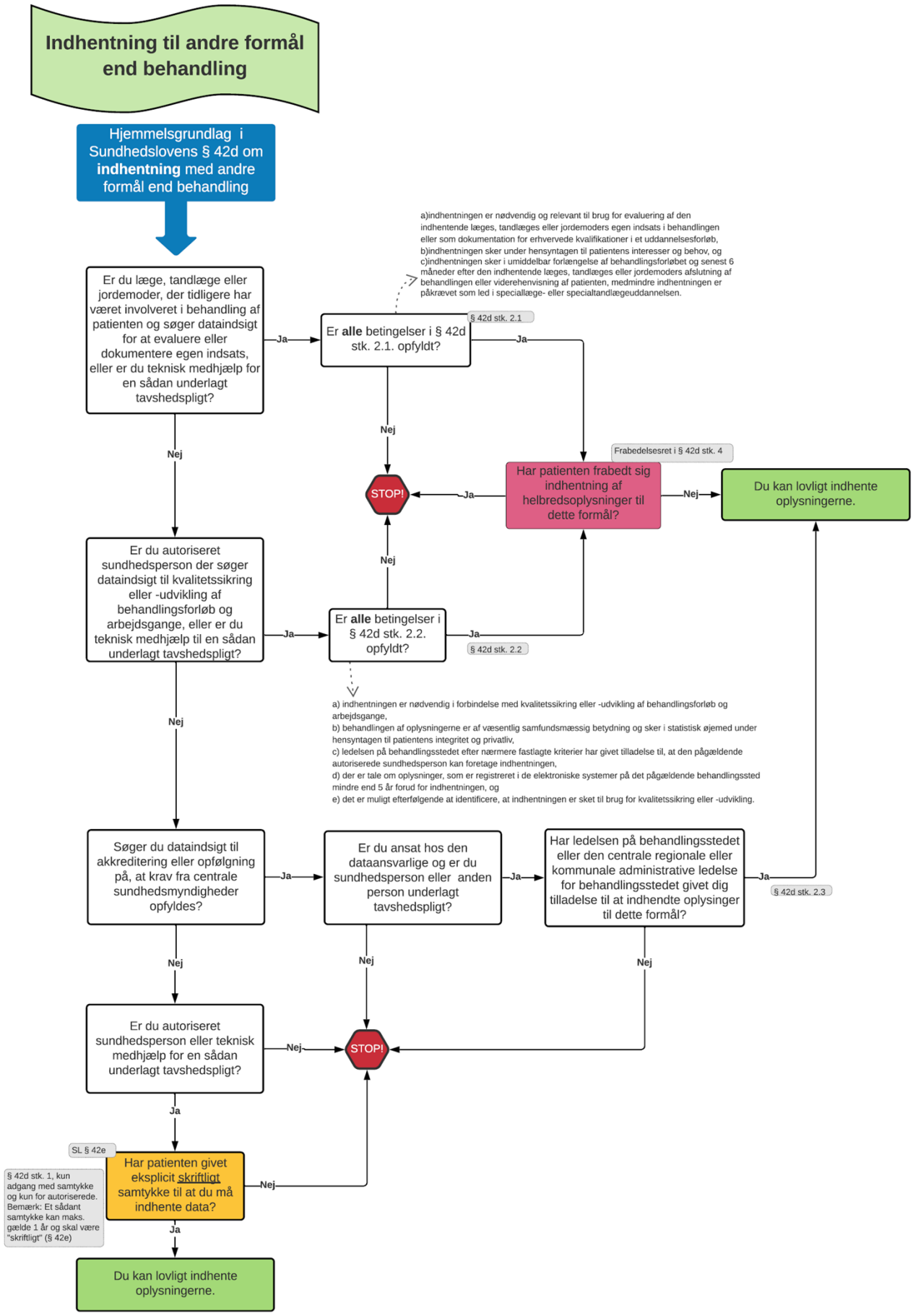
6. videregivelsen sker til en læge, tandlæge eller jordemoder om en patient, som modtageren tidligere har deltaget i behandlingen af, når
- videregivelsen er nødvendig og relevant til brug for evaluering af modtagerens egen indsats i behandlingen eller som dokumentation for erhvervede kvalifikationer i et uddannelsesforløb og
- videregivelsen sker under hensyntagen til patientens interesse og behov, eller
(Se også § 41 stk. 6+7)

7. videregivelsen sker til en studerende, der som led i en sundhedsvidenskabelig eller sundhedsfaglig uddannelse deltager i behandlingen af en patient uden at være medhjælp, når
- videregivelsen er nødvendig for den studerendes forståelse af behandlingssituationen eller evaluering af den studerendes deltagelse i behandlingssituationen og
- videregivelsen sker under hensyntagen til patientens interesse og behov.


Indhentning til Aktuel behandling forudsat samtykke til behandling
Enten indhentning af helbredsoplysninger om patienten i behandling eller indhentning af oplysninger om andre (evt. tidligere) patienters som led i behandling af patienten i aktuel behandling.
Hjemmelsgrundlag i Sundhedslovens § 42a stk. 1+4
Med aktuel behandling menes aktuel undersøgelse, diagnosticering, sygdomsbehandling, genoptræning, sundhedsfaglig pleje samt forebyggelse og sundhedsfremme i forhold til den enkelte patient, jf. sundhedslovens § 5. Aktuel behandling omfatter mere end, at en patient befinder sig fysisk på et behandlingssted. Aktuel behandling omfatter også forberedelse. Det betyder f.eks., at aktuel behandling starter, når der er en aftale om behandling. Det kan være, at patienten har bestilt tid, at patienten har anmodet om receptfornyelse, eller at en ambulance er på vej ind til hospitalet. Patienten vil også i kraft af en henvisning til et behandlingssted, f.eks. et hospital eller en speciallæge, være at betragte som værende i aktuel behandling på dette behandlingssted. Omfattet af begrebet aktuel behandling er tillige telemedicinske løsninger. (L127 2018, s. 34)
Adgang efter SL § 42a stk. 4. for andre personer underlagt tavshedspligt med privilegier fra ledelsen. Bemærk: adgang kun som følge af en sundhedsfaglig behandling/støttefunktion og kun når ledelsen har givet tilladelse til indhentning. Bemærk også, at disse ikke må foretage værdispringshandlinger.
Er du sundhedsperson (autoriseret eller delegeret)
Nej
Yder du teknisk bistand til en sundhedsperson og er du underlagt tavshedspligt?
Nej
Er du underlagt tavshedspligt og har fået tilladelse til indhentning af ledelsen på din arbejdsplads?
Nej
STOP!
§ 42a stk. 1
Ja
Ja
Adgang efter SL § 42a stk. 4. for teknisk medhjælp. Bemærk: adgang kun som følge af en sundhedsfaglig behandling/støttefunktion, og kun når ledelsen har udarbejdet instruks, og har givet den pågældende (gruppe) tilladelse til teknisk bistand.
Ja
Sundhedspersoner og dem, der yder teknisk bistand til dem, må indhente oplysninger om andre patienter ifm. aktuel behandling af en patient, men det kræver samtykke eller i yderste instans værdispring.(se s. 35-36 i bemærkningerne i Lovforslag nr. L 127).
Nej
Ønsker du at indhente oplysninger om patienten i aktuel behandling?
Indhenter du oplysninger om patienten i aktuel behandling?
Nej
Ja
Ja
Adgang efter SL § 42a stk. 3 hhv. § 42b.
Hvis patienten har frabedt sig indhentning skal du forsøge at få samtykke til at du alligevel må se oplysningerne, hvis du vurderer at det er nødvendigt at se oplysningerne.
Frabedelse af indsigt SL § 42a stk. 5 (se s. 39 i bemærkningerne i Lovforslag nr. L 127, 2018)
Har den, du indhenter oplysninger om, eksplicit afgivet mundtligt eller skriftligt samtykke?
Ja
Har den, du indhenter oplysninger om mundtligt eller skriftligt frabedt sig indhentning?
Ja
Nej
Nej
Er du sundhedsperson eller yder du teknisk bistand til en sundhedsperson, og er der helt særlige tungtvejende grunde til indhentning, der overstiger retten til privatliv hos den du indhenter oplysninger om?
Ja
Du kan lovligt indhente oplysningerne.
Værdispringsreglen SL §42a stk. 2 (se s. 35-36 i bemærkningerne i Lovforslag nr. L 127)
Nej
STOP!


Indhentning fra Fælles Medicinkort
Hjemmelsgrundlag i Sundhedslovens § 157 om indhentning af oplysninger fra FMK
Har du patienten i aktuel behandling OG: Er du læge, tandlæge, jordemoder, sygeplejerske, sundhedsplejerske, social- og sundhedsassistent, plejehjemsassistent eller behandlerfarmaceut, eller er du teknisk assistent for en af ovenstående eller er du en person, der har fået delegeret sundhedsfaglig?
SL § 157 stk. 2 1. punktum samt stk. 3 samt BEK nr 1615 af 18/12/2018
Ja
Nej
SL § 157 stk. 2 Speciallæger har kun adgang til oplysninger for patienter, de selv har udskrevet medicin til.
Er du praktiserende læge eller praktiserende speciallæge, og har du behov for adgang til medicinoplysninger fra FMK for at finde egne patienter, der behandles uhensigtsmæssigt med medicin?
Ja
Nej
BEK nr 1615 af 18/12/2018 § 6 stk. 5
Har den, du indhenter oplysninger om privatmarkeret oplysningerne?
Ja
Nej
STOP!
Nej
Er du læge og er der helt særlige tungtvejende grunde til indhentning, der overstiger retten til privatliv hos den du indhenter oplysninger om?
Ja
Du kan i fornødent omfang indhente relevante oplysninger fra FMK
Er du sygehusansat farmaceut eller farmakonom, der har behov for adgang til medicinoplysninger for den pågældendes behandling af patienten
SL § 157 stk. 4 . Kræver privilegier fra sygehusledelsen til medicingennemgang eller medicinafstemning.
Ja
Nej
Ja
Er du apoteksansat personale?
Ja
SL § 157 stk. 6 andet punktum.
Har du behov for FMK oplysninger som led i ekspedition af ordination?
Nej
Har du behov for andre oplysninger om medicinbrugeren?
STOP!
Nej
SL § 157 stk. 6 første punktum.
Ja
Nej
Er du en af de ovenfor nævnte personalegrupper og har du behov for andre oplysninger fra FMK end i de ovennævnte tilfælde?
Ja
SL § 157 stk. 13
Har patienten givet eksplicit mundtligt eller skriftligt samtykke til at du må indhente oplysninger?
Ja
Nej
Nej
STOP!


Indhentning i forbindelse med behandling (ikke aktuel / igangværende)
Hjemmelsgrundlag i Sundhedslovens § 42a stk. 3 om indhentning i forbindelse med behandling
"I forbindelse med" fortolkes i bemærkningerne til lovforslaget (L127 2018 s. 36-37) og omfatter blandt andet afsøgning af behandlingsmuligheder.
Er du sundhedsperson eller anden person underlagt tavshedspligt og ønsker du adgang til data i forbindelse med en behandling?
Adgang efter SL § 42a stk. 3 med patientens samtykke.
Ja
Har patienten givet eksplicit mundtligt eller skriftligt samtykke til at du må indhente data?
Nej
STOP!
Ja
Du kan lovligt indhente oplysningerne.


Indhentning til andre formål end behandling
Hjemmelsgrundlag i Sundhedslovens § 42d om indhentning med andre formål end behandling
Er du læge, tandlæge eller jordemoder, der tidligere har været involveret i behandling af patienten og søger dataindsigt for at evaluere eller dokumentere egen indsats, eller er du teknisk medhjælp for en sådan underlagt tavshedspligt?
Ja
Er alle betingelser i § 42d stk. 2.1. opfyldt?
§ 42d stk. 2.1
a)indhentningen er nødvendig og relevant til brug for evaluering af den indhentende læges, tandlæges eller jordemoders egen indsats i behandlingen eller som dokumentation for erhvervede kvalifikationer i et uddannelsesforløb,
b)indhentningen sker under hensyntagen til patientens interesser og behov, og
c)indhentningen sker i umiddelbar forlængelse af behandlingsforløbet og senest 6 måneder efter den indhentende læges, tandlæges eller jordemoders afslutning af behandlingen eller viderehenvisning af patienten, medmindre indhentningen er påkrævet som led i speciallæge- eller specialtandlægeuddannelsen.
Ja
Nej
Nej
Har patienten frabedt sig indhentning af helbredsoplysninger til dette formål?
Frabedelsesret i § 42d stk. 4
Ja
STOP!
Nej
Du kan lovligt indhente oplysningerne.
Er du autoriseret sundhedsperson der søger dataindsigt til kvalitetssikring eller -udvikling af behandlingsforløb og arbejdsgange, eller er du teknisk medhjælp til en sådan underlagt tavshedspligt?
Ja
Er alle betingelser i § 42d stk. 2.2. opfyldt?
Ja
§ 42d stk. 2.2
Nej
Nej
a) indhentningen er nødvendig i forbindelse med kvalitetssikring eller -udvikling af behandlingsforløb og arbejdsgange,
b) behandlingen af oplysningerne er af væsentlig samfundsmæssig betydning og sker i statistisk øjemed under hensyntagen til patientens integritet og privatliv,
c) ledelsen på behandlingsstedet efter nærmere fastlagte kriterier har givet tilladelse til, at den pågældende autoriserede sundhedsperson kan foretage indhentningen,
d) der er tale om oplysninger, som er registreret i de elektroniske systemer på det pågældende behandlingssted mindre end 5 år forud for indhentningen, og
e) det er muligt efterfølgende at identificere, at indhentningen er sket til brug for kvalitetssikring eller -udvikling.
Søger du dataindsigt til akkreditering eller opfølgning på, at krav fra centrale sundhedsmyndigheder opfyldes?
Ja
Er du ansat hos den dataansvarlige og er du sundhedsperson eller anden person underlagt tavshedspligt?
Ja
Har ledelsen på behandlingsstedet eller den centrale regionale eller kommunale administrative ledelse for behandlingsstedet givet dig tilladelse til at indhendte oplysninger til dette formål?
Ja
§ 42d stk. 2.3
Nej
Nej
Nej
Er du autoriseret sundhedsperson eller teknisk medhjælp for en sådan underlagt tavshedspligt?
Nej
STOP!
Ja
SL § 42e
Har patienten givet eksplicit skriftligt samtykke til at du må indhente data?
§ 42d stk. 1, kun adgang med samtykke og kun for autoriserede. Bemærk: Et sådant samtykke kan maks. gælde 1 år og skal være "skriftligt" (§ 42e)
Nej
Ja
Du kan lovligt indhente oplysningerne.