RAPPORT 2024

Målbillede for identitets-sløring af ansatte i det danske sundhedsvæsen

SUNDHEDSDATA-
STYRELSEN

Resumé:

Dette dokument er et målbillede for 'Identitetsløring af ansatte i det danske sundhedsvæsen'. Det har til hensigt at sætte rammerne for national digital understøttelse af identitetsløring inden for sundhedsdomænet, så alle parter foretager identitetsløring på samme måde og kan kommunikere løringsbehov til hinanden.

Ansatte i det danske sundhedsvæsen oplever i nogle sammenhænge truende eller grænseoverskridende adfærd hos patienter, borgere og pårørende af en sådan alvorlighedsgrad, at det vurderes nødvendigt at sløre identiteten på de personer, der er involveret i behandlingsforløbet. Identitetsløringen har til formål at beskytte de ansattes privatperson, så patienten ikke direkte kan finde navne på de involverede; navne der i nogle tilfælde kan gøre det muligt at finde privatadresse, familiemedlemmer mv. og udøve repressalier i privatsfæren.

Når en identitetsløring slår igennem hos en borger, vil borgeren i stedet for navnet på de ansatte få præsenteret tekniske pseudonymer i de borgervendte visninger eller udskrifter. Pseudonymet vil for den enkelte ansatte være ens på tværs af løsninger. Dermed kan borgeren stadig sammenholde forskellige registreringer, og se at disse handlinger er foretaget af den samme person. Borgeren kan bare ikke se navnet. Jf. 'logningsbekendtgørelsen' har borgeren ret til at henvende sig til behandlingsstedet og anmode om at få udleveret identiteten bag et bestemt pseudonym. Medmindre der er helt særlige forhold der kræver beskyttelse af de ansatte, skal anmodningen imødekommes.

Dette målbillede fastlægger begreber, principper, processer og forretningsregler for identitetsløring så alle, der kommer til at beskæftige sig med digitalisering af identitetsløring, har et ensartet sprog for og 'billede' af, hvad identitetsløring er, hvilken rækkevidde løringer har osv. Desuden dokumenterer målbilledet hvilke mål, der sigtes efter, og hvilken hjemmel, der er for løsningerne. Formålet er som ovenfor nævnt at sætte rammer og retning, så der opnås en ensartet praksis og digital understøttelse på tværs af hele sundhedsvæsenet.

Udgiver	Arkitekturfunktionen, Sammenhængende Digital Sundhed
Ansvarlig institution	Sundhedsdatastyrelsen
Design	
Copyright	
Version	0.95
Versionsdato	3. maj 2024
Web-adresse	www.sundhedsdata.dk
Titel	Målbillede for identitetssløring af ansatte i det danske sundhedsvæsen.

Indhold

1. Indledning

1.1 Formål

Formålet med dette målbillede er at sætte rammerne for national digital understøttelse af identitetssløring af personer, der arbejder i det danske sundhedsvæsen. Rammerne i dette målbillede består blandt andet af juridiske rammer, af principper som løsninger skal holde sig inden for, en opgørelse af 'forretningens' behov (brugere, borgere, administratorer, myndigheder osv.) og motivationen for behovet, samt overvejelser i forhold til struktur af digital understøttelse af behovet. Tilsammen skal målbilledet sikre, at alle interessenter har en tilstrækkelig god forståelse af området til, at der kan skabes gode digitale løsninger.

Udarbejdelsen af målbilledet er sket I samarbejde mellem SDS og repræsentanter fra regionerne. Herudover har både KL, PLO og Danske Patienter haft målbilledet til kommentering tidligt i forløbet.

1.2 Indhold og afgrænsning

1.2.1 Hvad er et målbillede?

Et målbillede beskriver en ønsket fremtid for et givent område. Det konkretiserer en overordnet vision for området, og skaber dermed rammerne for en forandring - ofte gennem digitalisering eller en forbedret digitalisering af området.

Inden man igangsætter egentlige digitaliseringstiltag, er det vigtigt at blive enige om grundlaget, omfanget og ambitionen af den digitale transformation. De emner, som behandles i målbilledet, er netop dem, der erfaringsmæssigt er væsentlige at afdække i forbindelse med digitale transformationer. Målbilledet formulerer og dissekerer visionen, uddyber enkeltdelene så hensigten og omfanget bliver tydeligt, specificerer hvilke principper, der skal gælde for digitaliseringen, og hvilke processer og regler, der forventes at gælde efter forandringen. Et målbillede er derfor rammesættende og retningsskabende. Det udpeger "målet", der ligger på den anden side af forandringen, som typisk kan tage lang tid at nå, særligt i store komplekse tilfælde som nærværende. Målbilledet skaber grundlaget for de mere detaljerede transitionsprodukter som gap-analyser, roadmaps, kravspecifikationer, og implementeringsplaner, der udarbejdes efterfølgende med afsæt i målbilledet[1].

Behandlingen af emner, hvis afklaring ikke har haft betydning for fastlæggelsen og forståelsen af den overordnede retning, udskydes til det efterfølgende arkitektur- og implementeringsarbejde. Dette understreger også, at der fortsat må forventes, at der skal udarbejdes afklaringer

[1] I det internationale TOGAF rammeværk [TOGAF], som den fællesoffentlige arkitekturmetode baserer sig på, svarer dette til, at vi med målbillede-arbejdet udfører fase A og dermed lægger grunden for faserne B-G.

og specifikationer i forbindelse med de efterfølgende implementeringsprojekter (dette er ikke alene klaret med målbilledet).

Et målbillede må ikke betragtes som statisk. Det skal genbesøges og justeres med jævne mellemrum, så det afspejler den aktuelle virkelighed, og eventuelt ændrede ambitioner og justerede mål. Eksempelvis vil arbejdet med at konkretisere arkitekturen og specificere, implementere og anvende løsninger bidrage med ny viden, der bør indarbejdes i fremtidige versioner af målbilledet. Desuden forandrer verden sig; nye muligheder opstår og behov ændres. Det er derfor hensigtsmæssigt, at man med mellemrum forholder sig til, om målbilledet fortsat har det rette scope og peger i den ønskede retning[2].

Dette målbillede er et reduceret målbillede, hvor enkelte elementer der primært retter sig mod governance og vedligeholdelse af et nationalt målbillede er taget ud. Målbilledets målgruppe er primært entreprise arkitekter og projektdeltagere hos de involverede parter. En generel introduktion til identitetssløring af ansatte i det danske sundhedsvæsen kan læses i nærværende kapitel nedenfor suppleret af afdækningen af forretningsarkitekturen i kapitel 3. For en mere teknisk gennemgang kan kapitlerne 3, 4, 5 og 6 læses.

1.2.2 Afgrænsninger

Målbilledet forholder sig udelukkende til identitetssløring i borgervendte visninger og udskrifter af journaler og logs. Målbilledet forholder sig derfor ikke til lovgivning og tilfælde, hvor der ikke logges/journalføres. Hvis der ikke logges eller journalføres, er der ikke noget at sløre. Tilsvarende er målbilledet afgrænset til pseudonymisering – ikke andre typer af informationssløring, udraderinger og minimering af visning af data.

1.3 Baggrund

Sidst i 00'erne blev der i sundhedsloven indsat en bestemmelse, som gav borgere adgang til at se informationer om, hvem der har slået op i deres patientjournaler, og hvornår opslaget er sket.

Med bekendtgørelse nr. 200 af 7. februar 2022 er regionsrådet fra 1. marts 2024 forpligtet til at udstille logoplysninger til borgeren om alle anvendelser af personoplysninger i alle elektroniske patientjournaler. Det betyder, at blandt andet fornavn, efternavn samt titel, behandlingssted og tidspunkt for den medarbejder, der har foretaget opslaget, bliver tilgængeligt for borgeren i loggen. Bekendtgørelsen tillader imidlertid, at der i stedet for fornavn/efternavn benyttes en anden entydig identifikation, et pseudonym, for den ansatte. Denne mulighed er indført for at beskytte medarbejdere mod repressalier fra specifikke borgere, f.eks. hvis borgeren/patienten har udvist truende adfærd. Muligheden kan også anvendes til at beskytte medarbejdere på særlige afsnit, hvor der ofte forekommer vold eller trusler om vold.

[2] Igen, i TOGAF-termer [TOGAF] svarer dette til fase H, der kan udløse en ny fase A med et efterfølgende gennemløb af de øvrige faser B-G.

Pseudonymiseringsmuligheden eksisterer allerede for journalføring i patientjournaler, men med bekendtgørelsen udbredes omfanget til også at gælde logning. Ordlyden af de to bekendtgørelser er koordineret, så de samme retningslinjer er gældende for pseudonymisering i journaler og i logs.

Sundhedsdatastyrelsen (SDS) har forpligtet sig til at støtte med tekniske løsninger i en forventning om, at der er tale om et behov som flere parter på sundhedsområdet har, og for at sikre at sløringer engang i fremtiden også vil slå igennem i alle relevante kilder, eksempelvis i Det Fælles Medicinkort og DDV.

1.3.1 Sammenhæng til andre målbilleder mv.

Der er for nærværende målbillede ingen sammenhæng til andre målbilleder eller nationale strategier. Behovet for identitetssløring er opstået og drevet af anvenderne af servicen, som følge af ændringer i Logningsbekendtgørelsen (BEK nr. 192 af 27/02/2024).

1.4 Centrale begreber og aktører

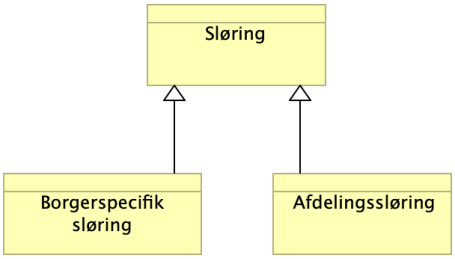
Dette afsnit introducerer de centrale begreber, der anvendes i dette målbillede. Flere af begreberne definerer centrale aktører og forretningsobjekter. Begreberne er i videst muligt omfang afstemt med Begrebsbasen[3] fra Sundhedsdatastyrelsens begrebssekretariat. En komplet liste over begreber og termer findes i Appendiks A – Begrebsliste.

1.4.1 Identitetssløring

Identitetssløring – eller blot sløring – er en 'pseudonymisering' af ansatte i sundhedsvæsenet. Sløringen har til hensigt at fjerne muligheden for, at patienter umiddelbart ved opslag i elektroniske visninger af journaler eller logs let kan finde frem til den ansattes bopæl, familierelationer eller andet. Nøgleordet er her 'umiddelbart', for borgeren vil stadig kunne henvende sig til behandlingsstedet og bede om at få den rigtige identitet oplyst. Borgere vil som hovedregel få identiteten udleveret, medmindre der foreligger særlige private hensyn til den pseudonymiserede. Denne vurdering (og afgørelse) ligger hos ledelsen af behandlingsstedet.

Dette målbillede definerer to typer af sløring: En borgerspecifik sløring og en afdelingssløring. Disse gennemgås i de efterfølgende afsnit.

[3] https://sundhedsdata.iterm.dk

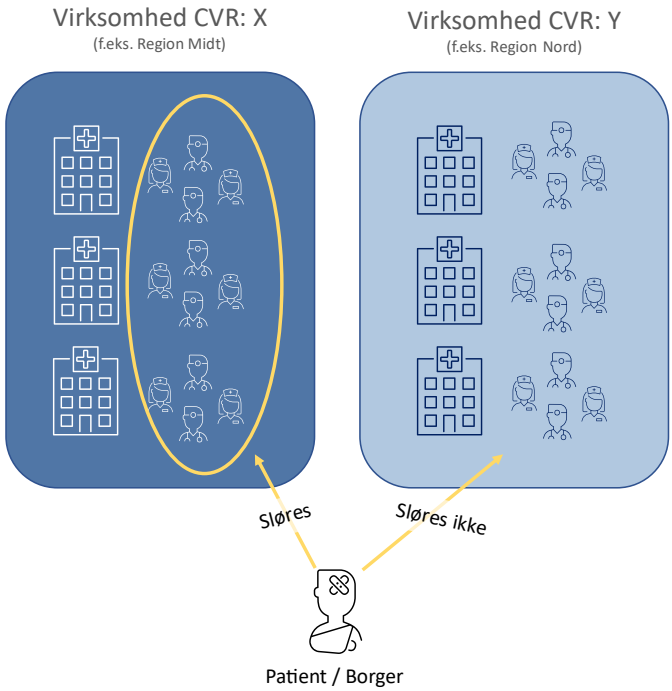


Figur 1: Sløringstyper

1.4.2 Borgerspecifik sløring

En borgerspecifik sløring er hændelsesbestemt og i sin natur reaktiv. Registrering af en borgerspecifik sløring udløses af, at en medarbejder i sundhedsvæsenet oplever adfærd (f.eks. truende, forfølgende eller på anden vis upassende), som gør medarbejderen utryg ift. deres privatperson eller privatsfære.

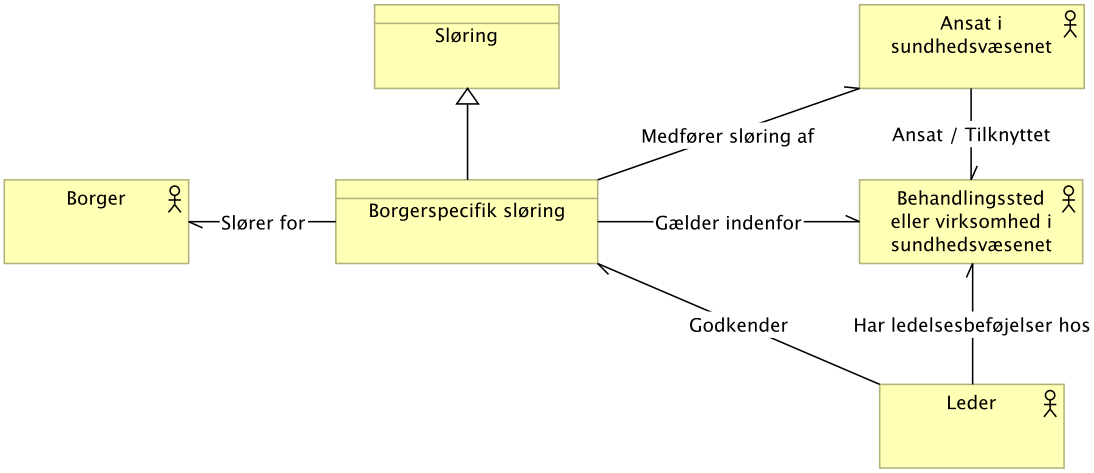
Hvis en ansat registrerer en borgerspecifik sløring, vil alle kolleger også optræde som sløret overfor borgeren/patienten. En sløringsregistrering er således lige dele selvbeskyttelse som beskyttelse af kolleger (inden for samme organisation baseret på CVR nummer). En sløring af medarbejdere i en region vil ikke afstedkomme sløring af medarbejdere i en anden region eller i en kommune. Det hænger sammen med, at sløringer kræver godkendelse og ansvar fra virksomhedsledelse, og at der er klare ansvarsskel mellem virksomheder.



Figur 2: Borgerspecifik sløring. Alle medarbejdere indenfor CVR-nummeret sløres for den pågældende patient.

Den registrerende myndighed skal løbende vurdere relevansen af alle registrerede sløringer. Som udgangspunkt kan en borgerspecifik sløring maksimalt have effekt i 90 dage, med mindre den eksplicit forlænges. Myndigheden skal sikre sig, at ikke-relevante sløringer nedlægges hurtigst muligt efter den vurderes som ikke-relevant.

Arkitekturmæssigt er en borgerspecifik sløring en relation mellem en virksomhed i sundhedsvæsenet (f.eks. en region, en kommune eller et apotek) og en specifik borger.



Figur 3: Borgerspecifik sløring er en relation mellem en specifik borger og en virksomhed i sundhedsvæsenet.

Arbejdsgangene ift. oprettelse/registrering, stadfæstelse, (re)evaluering og nedlæggelse gennemgås senere i målbilledet.

Sløringsregistrering for borgerspecifik sløring:

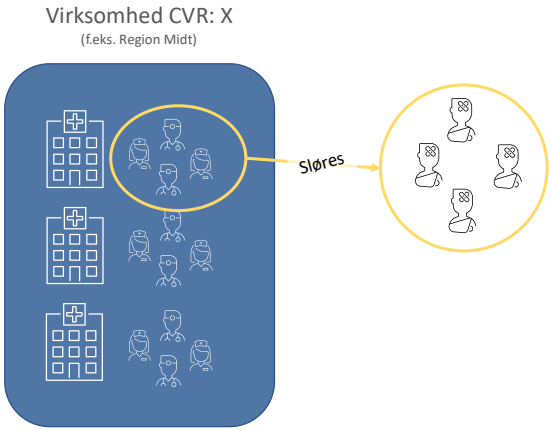
En sløringsregistrering dækker over den tekniske registrering af en sløring, dvs. registrering i eget fagsystem. En sløringsregistrering behandles af en leder/administrativ medarbejder hurtigst muligt efter registreringen. Sløringsregistreringen opbevares i et register, som anvendes af borgervendte løsninger til at afgøre, om der skal sløres for den pågældende borger. En sløringsregistrering kan således logisk set have status ”ikke-stadfæstet”, ”stadfæstet” eller ”afsluttet”.

1.4.3 Afdelingssløring

En afdelingssløring er en generel sløring af alle ansatte, der fremgår i registreringer fra afdelinger eller afsnit, hvor det på forhånd er vurderet, at der eksisterer et behov for at beskytte de ansattes identitet. Det kan f.eks. være på et særligt psykiatrisk afsnit. Afdelingssløringer er i modsætning til den borgerspecifikke sløring pro-aktive og er ikke knyttet til en bestemt borger. Afdelingssløringer har ikke en udløbsdato, og er således gyldige indtil afdelingssløringen eksplicit nedlægges.

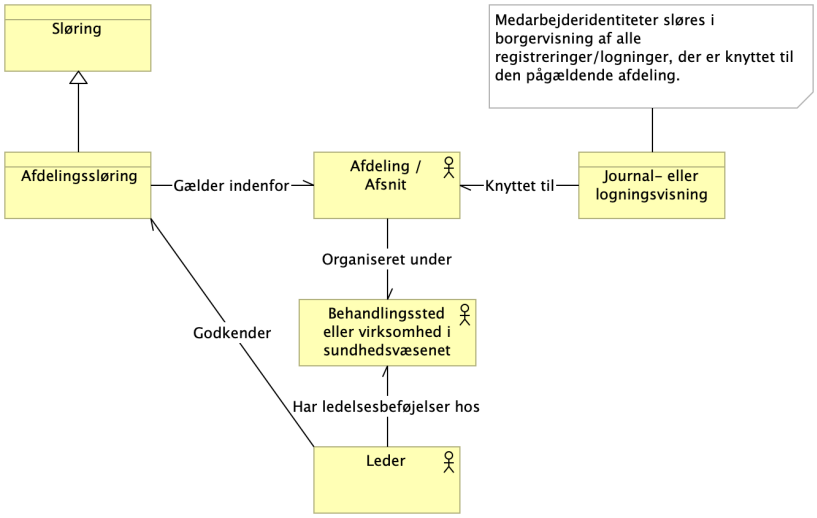
Ansatte, der optræder i visning af journal- eller logningsoplysninger fra den pågældende afdeling eller afsnit, vil blive sløret, uanset hvilken borger/patient der er tale om, og uanset om medarbejderen aktuelt er tilknyttet den pågældende afdeling.

Bemærk: Som ovenfor nævnt knytter denne type sløringer sig til afdelingen, ikke til patienten/borgeren eller til de ansatte, der aktuelt er på afdelingen. Det betyder, at også "eksterne" ansatte, f.eks. læger på tilsyn i afdelingen mv., vil optræde sløret over for en patient, der har haft berøring med den pågældende afdeling. Omvendt vil der ikke blive sløret for registreringer fra andre afdelinger, hvor der ikke er registreret et behov for afdelingssløring[4].



Figur 4: Afdelingssløringer gælder for alle patienter, der har berøring med bestemte afdelinger/afsnit.

Afdelinger, hvor der skal afdelingssløres, udpeges gennem anvendelse af SOR-klassifikationen.



Figur 5: Afdelingssløring slører medarbejderidentitet i alle visninger, der har med en bestemt afdeling at gøre.

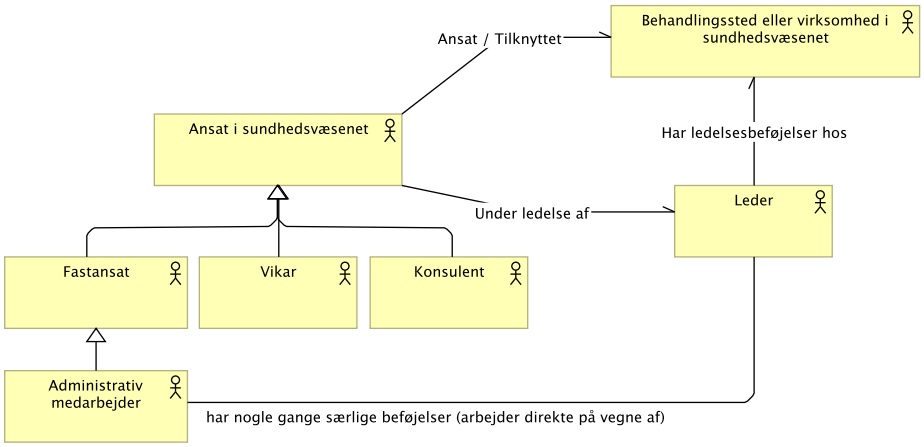
1.4.4 Ansættelse, ansatte og ledelse

Det er forventningen, at behovet for sløring findes hos alle ansatte i sundhedsvæsenet. I en terminologisk sammenhæng er det her vigtigt at fastslå, at 'ansatte' i denne sammenhæng ikke kun er sundhedspersoner (sundhedspersoner, der arbejder på et behandlingssted), men også

[4] medmindre der er registreret en borgerspecifik sløring for netop denne borger i det pågældende CVR-nummer. Borgerspecifikke sløringer vil altid resultere i sløring for alle registreringer indenfor det pågældende CVR-nummer.

f.eks. apotekspersonale og andre ansatte i de virksomheder, der 'betjener' patienter og borgere i sundhedsvæsenet. Ansat er således bredere end begreberne 'sundhedsperson', 'sundhedsprofessionel' og 'sundhedsperson'.

En ansat er en person, der er under ledelse i en virksomhed. Der er ikke nødvendigvis tale om fastansættelse – begrebet omfatter også løst tilknyttede som f.eks. konsulenter eller vikarer. Selvom konsulenter og vikarer er fastansat og får løn af et andet selskab, er de stadig under ledelse i den virksomhed, som de er konsulenter eller vikarer i. I digital sammenhæng er det typisk også årsagen til, at disse løst tilknyttede får en digital identitet i virksomheden, så ledelsen i virksomheden kan styre, hvilke privilegier (roller og rettigheder) den løst tilknyttede skal have som led i deres vikariat eller konsulentstøtte.



Figur 6: Ansatte kan være fastansatte, vikarer, konsulenter eller lignende. Fælles for dem alle er, at de er under ledelse af den virksomhed, som de er ansat i eller tilknyttet.

1.4.5 Anden identifikation / pseudonym

Et pseudonym dækker over en identifikation andet end fulde navn, autorisationsnummer eller CPR-nummer. Da pseudonymet er en borgervendt information, som skal kunne anvendes i henvendelser til behandlingsstedet, vil det være et krav til pseudonymer, at de relativt nemt skal kunne kommunikeres, dvs. de må ikke være for lange, komplicerede eller indeholde mærkelige tegn.

For at undgå, at borgere kan samarbejde om at finde frem til en ansats faktiske identitet, vil den samme ansatte optræde under forskelligt pseudonym overfor forskellige borgere. Der er ikke afdækket behov som fordrer komplet entydighed af pseudonymer, og henvendelser der søger at få oplyst navnet på den ansatte, hvis pseudonym fremgår af den borgervendte visning, vil altid suppleres med anden kontekst (tid/sted/behandling). Det betyder at en ansat efter bedste evne altid skal fremstå med entydigt pseudonym, men det afgørende er primært, at pseudonym + registreringstidspunkt er tilstrækkeligt til at finde frem til den rette identitet, og at borgeren som udgangspunkt skal kunne sammenholde registreringer, så vedkommende kan se, at det er foretaget af den samme person.

Kollision mellem pseudonymer (samme pseudonym for to forskellige medarbejdere) forventes således ikke at være en større udfordring, fordi pseudonym + tidspunkt er tilstrækkeligt til at fastlægge den faktiske identitet.

1.4.6 Aktindsigt

En aktindsigt er adgangen til at se dokumenter fra en pågældende myndigheds interne systemer, i en sag hvor en borgers forhold er omtalt, eller hvor borgeren er part, dvs. en sag hvor anmoder har væsentlig, direkte, retlig og individuel interesse i sagens[5] afgørelse. Retten til aktindsigt gælder som hovedregel alle dokumenter, der vedrører den pågældende sag, herunder indførelser i journaler, registre og andre fortegnelser der vedrører den pågældende sags dokumenter.

Afgørelsen om retten til aktindsigt afgøres af den myndighed, der søges aktindsigt hos. Da pseudonymiseringen af en sundhedsaktør sker i den borgervendte løsning, skal myndigheder være opmærksomme på, at der ved godkendte ansøgninger for aktindsigt, kan indgå identiteter på ansatte som ellers kan være sløret. Det er derfor op til myndigheden at afgøre om der er hjemmel til enten at afvise en anmodning på aktindsigt, eller om der skal sløres i de dokumenter der udleveres. Offentlighedsloven § 9 stk. 2, nr. 2 foreskriver at "Behandlingen af en anmodning om aktindsigt efter § 7 kan, uanset at betingelserne i stk. 1 er opfyldt, afslås, i det omfang, 2) anmodningen må antages at skulle tjene et retsstridigt formål el.lign."[6]. Det vil sige at anmodningen om aktindsigt kan afslås, hvis det formodes at aktindsigten har til formål (på nogen måde) at forfølge eller chikanere myndighedens ansatte.

En borger kan anmode om indsigt i den bagvedliggende identitet hos behandlingsstedet. Dette er *ikke* en aktindsigt, men behandlingsstedet skal på samme måde som ved en anmodning om aktindsigt, vurdere om der foreligger særlige hensyn til den ansatte, hvis identitet er sløret inden de eventuelt udlevere navnet på denne. Får borgeren afslag her, har denne ret til at anmode om aktindsigt, som efterfølgende skal behandles efter overstående lovgivning.

1.4.7 Centrale aktører

De centrale aktører er ikke selvstændigt beskrevet, men indgår i både afsnit 3.2 om user stories og forretningsprocessernes beskrivelse i afsnit 3.5. Kort beskrevet består de centrale aktører dog af borgeren samt regionernes aktører; leder, ansatte og administratorer. Yderligere aktører vil fremgå af førnævnte afsnit.

[5] https://www.retsinformation.dk/eli/lta/2014/433

[6] https://www.retsinformation.dk/eli/lta/2020/145

Strategisk

1.5 Hvad driver udviklingen?

Der er en række drivere i og omkring identitetssløringsområdet. Grundlæggende skal der findes en optimal balance mellem på den ene side beskyttelse af ansatte i sundhedsvæsenet og på den anden side borgeres ret til indsigt i hvem, der har været involveret i patientbehandling og registrering/lavet opslag i helbredsoplysninger.

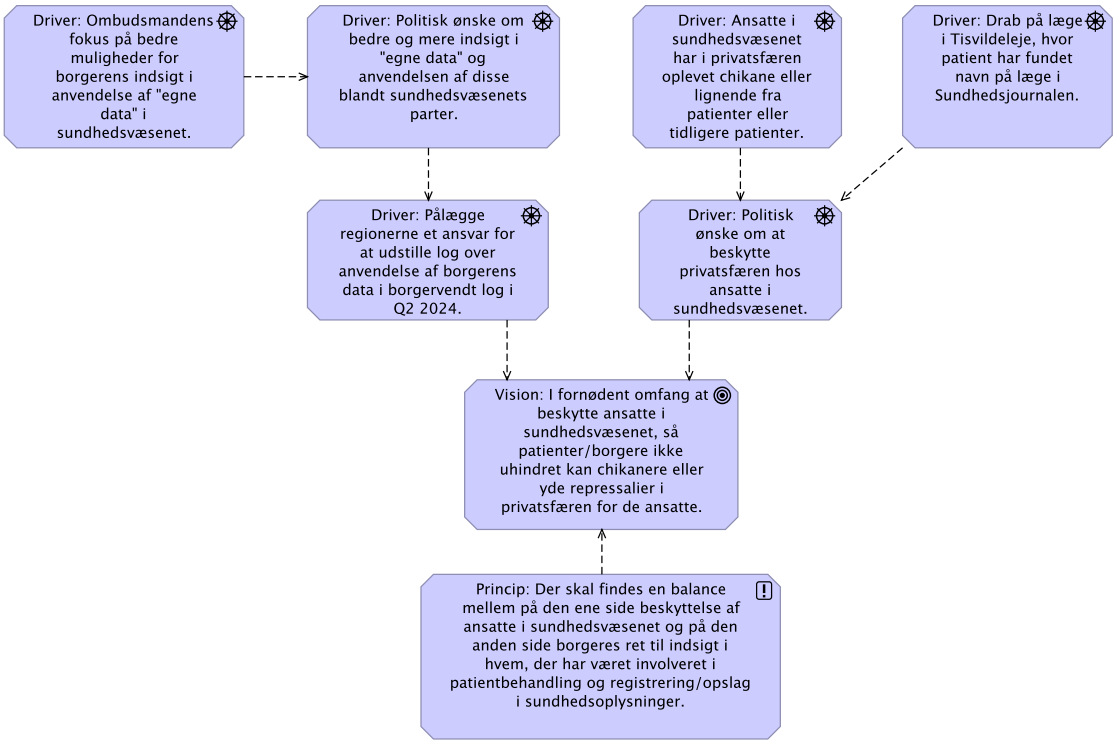
I forhold til indsigt i anvendelsen af helbredsoplysninger blev der allerede før 2010 indskrevet krav om at foretage borgervendt oplysning om anvendelse, i sundhedsloven. Dette krav har ombudsmanden løbende gennem 2010'erne fulgt op på[7]. Ønsket om bedre og mere indsigt fra borgere i sundhedsvæsenets anvendelse af deres helbredsoplysninger er også indskrevet som indsatsområder i flere strategier for sundheds-it over de seneste 10 år. Med logningsbekendtgørelsen (se mere om denne i afsnit 2.1 'Logningsbekendtgørelsen og journalføringsbekendtgørelsen') er regionerne nu blevet pålagt at udstille en borgervendt log over anvendelsen af helbredsoplysninger internt i regionerne inden udgangen af Q1 2024.

På den anden side er der eksempler på, at udstilling af de ansattes navne i offentlige digitale løsninger kan bruges til at finde frem til privatadresse og andre oplysninger om de ansatte i sundhedsvæsenet. Under efterforskningen af drabet[8] på en læge i Tisvildeleje i 2019 blev der fundet udskrifter fra Sundhedsjournalen, hvor den dræbtes navn var understreget. De ansatte i sundhedsvæsenet er utrygge, og der er i skrivende stund stadig mediebevågenhed[9] på behovet for at kunne beskytte de ansattes identitet.

[7] https://www.ombudsmanden.dk/find/nyheder/alle/patientjournaler/#cp-title

[8] https://www.berlingske.dk/samfund/56-aarig-er-kendt-skyldig-i-drab-paa-laege-i-tisvildeleje-0

[9] https://www.altinget.dk/sundhed/artikel/psykiatriansat-regionernes-bud-paa-navnebeskyttelse-er-som-at-tage-selen-paa-efter-bilen-er-koert-galt



Figur 7: Drivere, vision og grundlæggende retfærdighedsprincip for identitetsløring.

1.6 Interessenter og interesser

Den primære driver for målbilledet har været ændring i Logningsbekendtgørelsen og de deraf påvirkede parter, der i første omgang primært består af regionerne. Der er ikke yderligere uddybende afdækning af interessenter og interesser, men disse og deres behov afdækkes i afsnit 3.2 om forretningens krav og user stories. Dertil er mulige interessenter, herunder KL, PLO og Danske Patienter blevet tilbudt at kommentere på løsningen tidligt i forløbet, og deres behov vurderes i høj grad at blive dækket af regionernes input.

1.7 Vision

Visionen med arbejdet er følgende:

> ***I fornødent omfang at beskytte ansatte i sundhedsvæsenet, så patienter/borgere ikke uhindret kan chikanere eller yde repressalier i privatsfæren for de ansatte.***

Med 'i fornødent omfang' indarbejdes ovennævnte princip om, at borgerens almindelige ret til indsigt i navne på de ansatte, der har haft adgang til patientens helbredsoplysninger, ikke skal fratages borgere i almindelighed. Med 'ikke uhindret' menes at borgeren ikke umiddelbart kan

få adgang til de ansattes identitet for eksempel via. Simpel online-søgning på den ansattes navn.

1.8 Målsætninger

Der er følgende overordnede mål:

- At sikre ensartet gode muligheder for at få sløret sin identitet overfor udvalgte borgere som ansat i det danske sundhedsvæsen.
- At borgere (uanset om der sløres for dem eller ej) har gode muligheder for indsigt i, hvem, der har haft adgang til deres helbredsoplysninger, hvornår og i hvilken sammenhæng.
- At borgere, for hvem der er registreret behovet for sløring, har mulighed for at søge indsigt i identiteter bag pseudonymer[10], og generelt har gode klagemuligheder.
- At sløringer ikke bidrager til forskelsbehandling i behandling, pleje eller betjening i det danske sundhedsvæsen.

1.9 Kvaliteter

De centrale kvaliteter er for nærværende målbillede ikke eksplicit beskrevet, men dækkes i det store hele af principperne i afsnit 1.9 og sikkerhedsafsnittet i kapitel 6.

1.10 Principper

Følgende arkitekturprincipper er identificeret i udformningen af målbilledet. Det skal bemærkes, at arbejdsgruppen bag målbilledet har besluttet at fremlægge "løsningsnære" principper frem for at profilere diverse fællesoffentlige eller nationale principkataloger. Der er dog i flere tilfælde en god sammenhæng med de overordnede arkitekturprincipper for sundhedsområdet[11], som i flere af tilfældene er afledt af principper fra hvidbogen om fællesoffentlig digital arkitektur[12]. Principperne har til formål at sikre at det videre arbejde med national digital understøttelse af identitetssløring, fordeles til de rigtige parter og retter sig mod visionen med initiativet.

[10] I en konkret henvendelse kan myndigheden dog vurdere, at der er hensyn til de ansatte eller andre, der gør, at identiteterne ikke udleveres.

[11] Arkitekturprincipper for Sundhedsområdet. https://sundhedsdatastyrelsen.dk/-/media/sds/filer/rammer-og-retningslinjer/referenceaktitektur-og-it-standarder/arkitekturprincipper_version-2,-d-,0.pdf?la=da

[12] Hvidbog om fællesoffentlig digital arkitektur. https://arkitektur.digst.dk/sites/default/files/241_hvidbog_om_arkitektur_for_digitalisering_version_1.0_kolofon.pdf

Balancen mellem borger og sundhedsvæsnet	
Princip 1	Der skal findes en balance mellem på den ene side beskyttelse af ansatte i sundhedsvæsenet og på den anden side borgeres ret til indsigt i hvem, der har været involveret i patientbehandling og registrering/opslag i sundhedsoplysninger.
Rationale	Princippet er en anerkendelse af at der i nogle tilfælde er behov for beskyttelse af de ansattes identitet, men at langt de fleste borgere opfører sig ordentligt og derfor har ret til uhindret indsigt.
Implikationer	Balancen skal findes mellem på den ene side, at ansatte ikke altid optræder pseudonymiseret, men at de på den anden side i særlige tilfælde skal kunne optræde pseudonymiseret. Desuden skal princippet resultere i at sløringsregistret alene anvendes til sløringsformål i borgervendte løsninger, og ikke misbruges til andre formål.
Evt. Referencer*	

Opdeling af administration og effektuering	
Princip 2	Der skal skelnes mellem administration af sløringsbehov, og hvordan sløringer effektueres så de to dele er uafhængige og kan udvikles selvstændigt.
Rationale	Princippet skal medvirke til at: - Imødegå uhensigtsmæssig sammenblanding af behov og delløsninger. - Administrationen og effektueringen er to forskellige processer, der typisk foregår i to forskellige systemer. - Paralleliseringsmulighed i udvikling af løsninger.
Implikationer	Arkitekturbeskrivelser og teknisk løsning deles op i administration og sløringseffektuering.
Evt. Referencer*	

Borgervendt pseudonymisering	
Princip 3	Der skal kun sløres overfor borgere, ikke sundhedspersoner. Pseudonymiseringen skal kun ske i borgervendte visninger, og kun når det er nødvendigt.
Rationale	Det er i flere sammenhænge vigtigt, at sundhedspersoner i et behandlingsforløb kan kontakte kolleger, der tidligere har journalført

	noget om patienten (spørgsmål, sparring, udredning). Navne skal derfor ikke sløres overfor kolleger. Det er kun når borgeren ser sine egne journaloplysninger (eller logs), at navne skal udskiftes.
Implikationer	- Der skal alene sløres i borgervendte visninger f.eks. Sundhedsjournalen (borgerdelen), MinLog (borgerdelen) etc. - Der skal ikke pseudonymiseres i kilderegistre eller i fagsystemer. De rigtige identiteter skal altid fremgå i visninger for sundhedspersoner.
Evt. Reference*	Fastholdt i afsnit 3.5.1 Forretningsproces for sløring.

Sløringsfunktionaliteten for nuværende og kommende løsninger	
Princip 4	Sløringsfunktionalitet skal kunne indgå i alle relevante nuværende og kommende borgervendte løsninger.
Rationale	Det forventes at sløringsbehovet rækker et stykke ind i fremtiden. Derfor skal model og løsning udformes på en måde, så det med rimelighed må kunne forventes, at det kan implementeres i fremtidige løsninger. Tilsvarende skal viden om relevante eksisterende løsninger indgå i designet, så der ikke udformes en løsning, der kun kan implementeres i de nært forestående løsninger, som de første parter anvender.
Implikationer	Designet skal i videst muligt omfang holde sig inden for anvendte standarder i det danske sundhedsvæsen og ”best practices” inden for pseudonymisering. Løsningerne må ikke være programmeringssprogsspecifikke. Koblinger og bindinger skal reduceres til et minimum, så datakilder i videst muligt omfang kan skabe pseudonymer autonomt.
Evt. Reference*	T2^{aps}: Teknisk interoperabilitet opnås gennem anvendelse af udbredte, åbne standarder

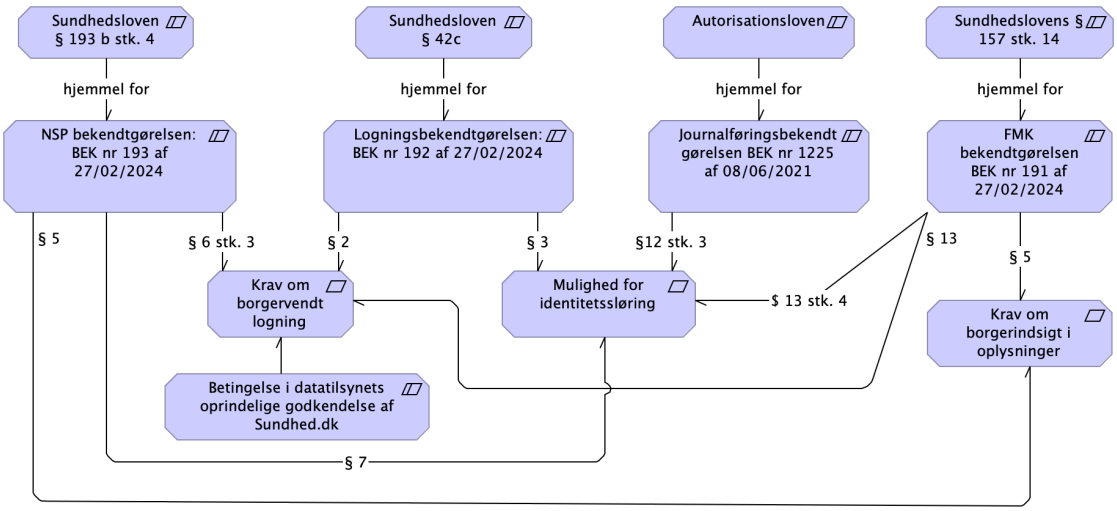
Kommunikation af en sløring	
Princip 5	Behovet for at kommunikere sløringer til tjenester, der skal sløre for flere parter, skal ske gennem en central service.
Rationale	Løsninger baseret på bilaterale aftaler og udvekslinger, anses for værende uhensigtsmæssige, blandt andet fordi det kræver vedligeholdelse af en række aftaler og integrationer mellem parterne. Desuden er det mere hensigtsmæssigt at styre sletninger, logninger og opklaring i forbindelse med fejl i centrale løsninger.
Implikationer	• Parter, der administrerer sløringer, skal sikre, at deres sløringsregistreringer (også) oprettes/rettes/nedlægges i datagrundlaget for den centrale sløringskommunikationsløsning. • Borgervendte visningsløsninger skal have oplysninger fra den centrale løsning for at kunne effektuere sløringer fra andre parter i sundhedsvæsenet.
Evt. Reference*	

Arbejdsgang for sløringsregistrering	
Princip 6	Det administrative arbejde ved en sløring, dvs. de processer/arbejdsgange, der skal til for at foretage registreringen, tilrettelægges af de enkelte parter.
Rationale	Der skal med løsningen sikres, at man ikke unødigt hindrer de enkelte organisationer i frit at kunne tilrettelægge kerneopgaver og registreringspraksis omkring disse.
Implikationer	Sløringsregistreringsservicen stilles til rådighed for de parter, der fremgår i bekendtgørelserne, men det vil være op til hver enkelt part at tilrettelægge de lokale processer ift. registrering og administration af sløringer. Sløringsregistreringsservicen foretager kun basale valideringer af gyldighed (f.eks. eksisterende organisation, gyldig borgeridentifikation (CPR) etc.)
Evt. Reference*	F3^{aps}: Fælles løsninger skal respektere, at samarbejdet sker mellem uafhængige juridiske enheder, som kan have egne regler, retningslinjer og processer.

* Referencer angivet med hævet ”aps” henviser til arkitekturprincipper for sundhedsområdet. Det første tegn henviser til arkitekturniveauet princippet opererer på (F for forretning, I for information, A for applikation, og T for teknologi/infrastruktur).

2. Lovgivning

Som ovenfor nævnt omhandler målbilledet muligheder og løsninger på at erstatte ansattes navne med 'anden entydig identifikation' i de borgervendte digitale visninger på sundhedsområdet. Nedenfor redegøres for de love og bekendtgørelser, der kræver at de sundhedspersoners identiteter registreres i journaler og logs, og hvor der er hjemmel til at vise og sløre for dem. I figuren nedenfor ses et overblik over de relevante love og bekendtgørelser:



Figur 8: Overblik over relevante love og bekendtgørelser ift. borgervendt visning, logning og identitetssløring.

Som lovarbejdet er udformet, er det derfor tilladt at identitetssløre i MinLog visninger og i E-journal/Sundhedsjournal borgervisningen, uanset om logningerne kommer direkte fra et behandlingssted eller indirekte fra behandlingssteder gennem FMK eller den fælles nationale infrastruktur. Det er endvidere muligt at erstatte navne på sundhedspersoner med pseudonymer i visninger af journaloplysninger.

2.1 Logningsbekendtgørelsen og journalføringsbekendtgørelsen

Sundhedslovens § 42 c[13] giver sundhedsministeren hjemmel til at tilrettelægge nærmere regler for logning i forbindelse med opslag i elektroniske systemer inden for sundhedsvæsenet. I 2024 blev denne hjemmel brugt til 'logningsbekendtgørelsen', BEK nr. 192 af 27/02/2024[14], hvor det i bekendtgørelsens § 2 pålægges regionerne at udstille logoplysninger for borgere. I bekendtgørelsen står der, at der som minimum skal udstilles fornavn, efternavn og titel på den ansatte,

[13] https://www.retsinformation.dk/eli/lta/2019/903

[14] https://www.retsinformation.dk/eli/lta/2024/192

der foretog opslaget. Desuden skal behandlingssted og tidspunkt udstilles. Der stilles krav om at oplysningerne skal fremstilles i en overskuelig og letforståelig oversigt.

I bekendtgørelsens § 3 kan regionsrådet i den enkelte region beslutte, at patienten i stedet for fornavn og efternavn får adgang til oplysninger om 'anden entydig identifikation' på den person, der har foretaget et opslag.

I § 3 stk. 2 kræves det endvidere, at "Behandlingsstedet skal efter anmodning fra patienten udlevere oplysninger om identiteten på personen bag oplysningerne i stk. 1, medmindre der foreligger afgørende hensyn til andres private interesser".

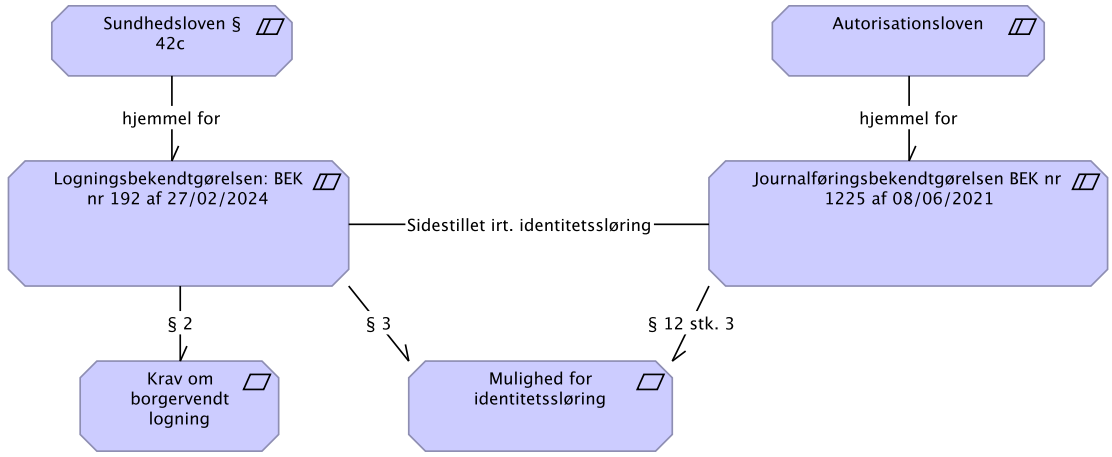
Lovarbejdet kommer ikke nærmere ind på, hvorledes sløringen mere præcist foretages, og hvilken rækkevidde en sløring har. Dog kan man af i § 3 se, at en sløring maks kan gælde i 90 dage hvorefter den automatisk skal bortfalde. Desuden kan man af folketingsbehandlingen af bekendtgørelsen[15] se, at:

- sløring har primært til hensigt at sikre ansatte i sundhedsvæsenet mod repressalier fra borgere
- at sløring er relateret til ledelsesret og arbejdsmiljøloven, hvor en arbejdsgiver har pligt til at indrette en tryg arbejdsplads
- at det ikke kun er trusler, men også anden adfærd hos en patient/borger, der kan udløse behovet for sløring
- at der skal findes en hensigtsmæssig balance mellem på den ene side beskyttelse af ansatte i sundhedsvæsenet og på den anden side borgeres ret til indsigt i hvem, der har været involveret i patientbehandling og registrering/opslag i sundhedsoplysninger.

Endelig kan man af ministerens svar på indkomne spørgsmål fra medlemmer af sundhedsudvalget se, at det er hensigten at sidestille logningsbekendtgørelsens sløringsparagraf med journalføringsbekendtgørelsens[16] tilsvarende bestemmelse om, at sundhedspersoner kan optræde med anden identitet end navn i journaler (eller i borgervendt visning af journaldata).

[15] https://www.ft.dk/samling/20211/beslutningsforslag/b35/index.htm

[16] https://www.retsinformation.dk/eli/lta/2021/1225



Figur 9: Logningsbekendtgørelsen og journalføringsbekendtgørelsen levner begge mulighed for at ansatte i sundhedsvæsenet kan optræde med anden entydig identitet end navn.

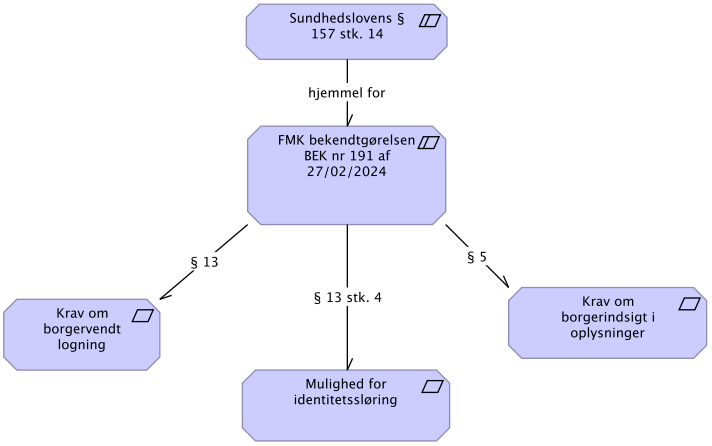
2.2 FMK-bekendtgørelsen

Fælles Medicin Kort (FMK[17]), der giver borgere og sundhedspersoner adgang til oplysninger om borgernes medicin og vaccinationer, er reguleret i § 157 i sundhedsloven. I § 157 stk. 14 findes der hjemmel til, at sundhedsministeren kan tilrettelægge de nærmere bestemmelser for registrets indhold, adgang til registret mv. Denne hjemmel er anvendt i forbindelse med "FMK-bekendtgørelsen" BEK nr 191 af 27/02/2024[18], hvor SDS i § 5 forpligtes til at udstille FMK-oplysninger til borgere via Sundhed.dk, herunder oplysninger om ansattes adgang til og registrering af medicinoplysninger mv. Jævnfør bekendtgørelsens § 4 stk. 3 skal de ansatte registreres med oplysninger *"der entydigt identificerer sundhedspersoner m.v. ved navn, ansættelsessted/organisation og autorisations-ID, såfremt sundhedspersoner har et sådant*".

Ifølge bekendtgørelsens § 13 er FMK endvidere forpligtet til at føre log over adgang og registrering i FMK og at stille denne log til rådighed for borgere (ift. indsigt i adgang til egne oplysninger, hhv. visse oplysninger i forældre- og værgerelationer). I den omtalte bekendtgørelse fra 1. kvartal 2024 blev det muligt at sløre identiteten af sundhedspersoner i borgervendte visninger af logs.

[17] https://sundhedsdatastyrelsen.dk/da/registre-og-services/om-faelles-medicinkort

[18] https://www.retsinformation.dk/eli/lta/2024/191



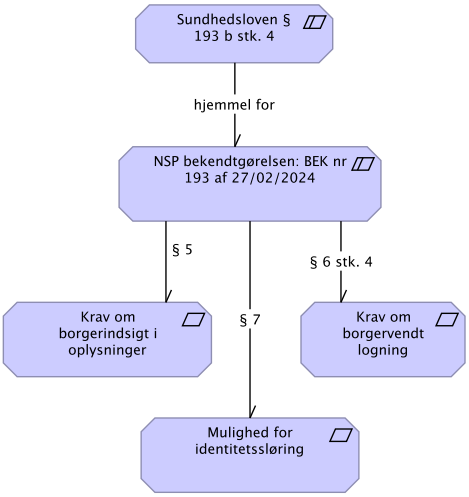
Figur 10: FMK-bekendtgørelsen stiller krav om borgervendt logning og borgervendt visning. I den nyeste FMK-bekendtgørelse er det nu muligt at sløre identiteten på sundhedspersoner i visning af logs overfor borgere.

2.3 Bekendtgørelse om drift mv. af den fælles digitale infrastruktur ("NSP-bekendtgørelsen")

BEK nr 193 af 27/02/2024[19] (med hjemmel i Sundhedslovens § 193b) forpligter i § 6 SDS til at logge anvendelser af personoplysninger i den fælles digitale infrastruktur. Logningen skal mindst indeholde oplysninger om: hvem der har foretaget opslag, med angivelse af fornavn, efternavn samt autorisationsnummer eller titel, behandlingssted, hvorfra opslaget er foretaget og tidspunkt for opslaget.

I bekendtgørelsens § 5 fremgår det desuden, at helbredsoplysninger m.v. i den fælles digitale infrastruktur skal udstilles i et digitalt patientoverblik. I § 7 er det fra 2024 blevet muligt at sløre navne i borgervendte visninger af logs.

[19] https://www.retsinformation.dk/eli/lta/2024/193



Figur 11: "NSP-bekendtgørelsen" stiller krav om både borgerindsigt i oplysninger og borgervendt logning. I begge disse kræves der navn på ansatte. I § 7 er det fra 2024 blevet muligt at sløre navne i borgervendte visninger af logs.

3. Forretningsarkitektur

I dette kapitel gennemgås krav, ønsker og begrænsninger fra de væsentligste interessenter.

3.1 Forretningens krav (fra lovgivning)

Som ovenfor nævnt stiller lovgivningen en række krav til borgervendt logning, borgervendt visning af helbredsoplysninger og mulighed for identitetssløring:

- De i kapitel 2nævnte bekendtgørelser specificerer, at flere forskellige dele af den nationale infrastruktur i sundhedsvæsenet i Danmark skal give borgere adgang til oplysninger (logs) over, hvem der har haft adgang til borgerens oplysninger på en *" overskuelig og letforståelig"* måde. Samtidig får behandlingssteder ret til at *"… patienten i stedet for oplysningerne om fornavn og efternavn får adgang til oplysninger om anden entydig identifikation på den person, der har foretaget et opslag."*
- I relation til foregående punkt: *"Behandlingsstedet skal efter anmodning fra patienten udlevere oplysninger om identiteten på personen bag oplysningerne i stk. 1, medmindre der foreligger afgørende hensyn til andres private interesser."*
- En registreret sløring skal gælde i maksimalt 90 dage.
- Parterne på sundhedsområdet skal føre journal over behandling af patienten i det danske sundhedsvæsen. I visning af journaldata for borgeren kan de ansatte optræde under pseudonym.

3.2 Forretningens krav og ønsker fra User Stories

Som input til målbilledet og forretningsprocesserne, er der identificeret en række user stories. En detaljeret liste med user stories og deres hensigt kan findes i Appendiks B.

User stories beskriver de konkrete behov de forskellige aktører forventes at have i kontekst af identitetssløring. Behovet hos den ansatte i sundhedsvæsnet opstår, når der opleves truende eller anden adfærd fra patienter/borgere, der gør den ansatte bekymret for eget og/eller kollegers privatperson. Derudover er der en række behov i forhold til administration af sløringsregistreringer. Borgerens behov består primært i, at det på trods af en sløringsregistrering skal være muligt at tilgå sine sundhedsoplysninger, samt at det skal være muligt at kunne sammenholde identiteterne på de sundhedsansatte, der har foretaget opslag i ens journal. Desuden skal borgeren have mulighed for at kunne henvende sig til behandlingsstedet for at få oplyst identiteten bag et pseudonym, og der skal være klagemuligheder hvis borgeren mener, at der er sløret uretmæssigt.

3.2.1 User stories for ansatte i sundhedsvæsnet

De væsentligste user stories for ansatte i sundhedsvæsnet kan sammenfattes til følgende:

Som ansat i sundhedsvæsnet ønsker jeg at …

- i en behandlingssituation med en borger, hvor jeg føler mig utryg i forhold til min privatperson på grund af patientens/borgerens opførsel, kunne sløre min og mine kollegers identitet, og vide at sløringen slår igennem øjeblikkeligt.
- kende konsekvenserne af en sløringsregistrering (hvor vil jeg optræde sløret, er der steder jeg ikke gør?), og at jeg er informeret om de administrative processer omkring sløringer.
- kunne se mine kollegers identiteter, når jeg tilgår mine patienters sundhedsdata. Identitetssløringer skal derfor kun ske i borgervisninger, ikke i visninger overfor sundhedspersoner.

3.2.2 User stories for borgere

Som borger ønsker jeg at …

- have adgang til mine egne sundhedsdata.
- vide hvem, hvornår og i hvilken sammenhæng der har været adgang til mine sundhedsdata.
- kunne sammenholde forskellige opslag, så jeg kan se omfanget af adgang til mine helbredsoplysninger, også selv om en identitet evt. er sløret for mig.
- kunne henvende mig ved det behandlingssted, hvor der er foretaget en sløringsregistrering, og få indsigt i identiteten bag pseudonymet, eller klage hvis jeg mener at sløringsregistreringen er uberettiget.

3.2.3 User stories for øvrige aktører

Som sløringsadministrator ønsker jeg at …

- have en overskuelig arbejdsgang for arbejdet med sløringsregistreringer, og at jeg har et overblik over de sløringer, der allerede er foretaget.

Som myndighed ønsker jeg at …

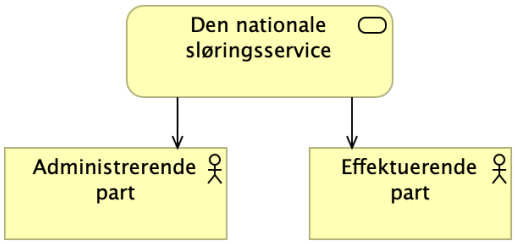
- den løsning, der benyttes, er lovmedholdelig, og at jeg kan regne med at databehandlere også er det.
- kunne oprette en proaktiv sløring for bestemte afdelinger, og kommunikere disse på en let forståelig måde.

3.3 Centrale forretningsobjekter

De centrale forretningsobjekter er ikke yderligere beskrevet i nærværende målbillede. Der henvises til afsnit 1.4.1 hvor de centrale forretningsobjekter for løsningen fremgår.

3.4 De væsentligste forretningskomponenter

Som beskrevet i afsnit 1.9, skal det tværgående kommunikationsbehov håndteres at en central service. Den omtales i den resterende del af målbilledet som "Den nationale sløringsservice". Den nationale sløringsservice leverer både de nødvendige administrative services (registrering, ændring, nedlæggelse af sløringer) og services, der gør det muligt for relevante komponenter at udlevere data til effektuering af sløringer i en konkret borgerlogin kontekst.



Figur 12 Forretningskomponenter for den nationale sløringsservice

3.5 Forretningsprocesser

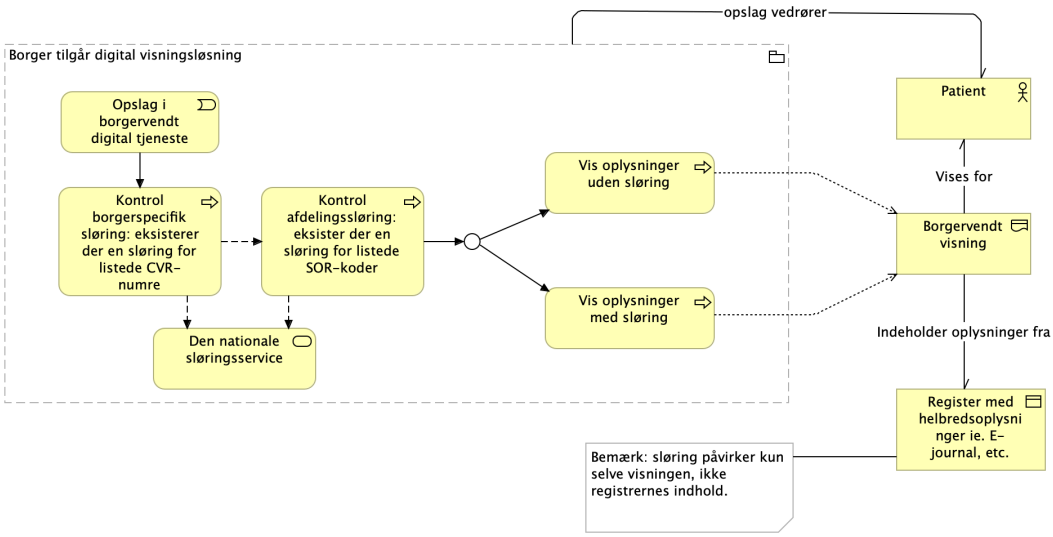
I dette afsnit gennemgås de centrale forretningsprocesser, der er gældende for samtlige brugere af den nationale sløringsservice. I dette målbillede er "forretningen" (de væsentligste interessenter) de behandlingssteder og virksomheder i sundhedsvæsnet, der har ansatte, der behandler eller betjener patienter eller borgere generelt. Forretningsprocesserne skal sikre en ensartet håndtering af sløringsregistreringer, sløringsadministrering og ved borgerhenvendelser, hvor der søges indsigt i en ansats pseudonym.

3.5.1 Forretningsproces for sløring

Når en borger tilgår en digital tjeneste som E-journal eller FMK, vil den borgervendte løsning fremover kontrollere, om de medarbejdere, der fremgår i visningen, skal sløres for den pågældende borger. Hvis en sløringsregistrering eksisterer, skal borgervisningen udskifte fornavn/efternavn med et pseudonym for de medarbejdere, der arbejder for den organisation eller afdeling, der har registreret sløringen. Eksisterer der ikke en sløringsregistrering, vil borgeren kunne se fornavn/efternavn som normalt. Bliver borgervisningen tilgået af en forælder, værge eller fuldmagtshaver vil en sløring overfor barnet også slå igennem for disse.

Bemærk: på det forretningsmæssige plan er processen den samme, om der er tale om en digital tjeneste eller en analog tjeneste (f.eks. print).

Indholdet i det bagvedliggende register forbliver det samme (sløringen sker på visningstidspunktet). Derfor vil ansatte i deres fagsystemer og i de nationale løsninger rettet mod sundhedspersoner stadig kunne se den rigtige identitet, selvom der sløres i visningen for borgeren.

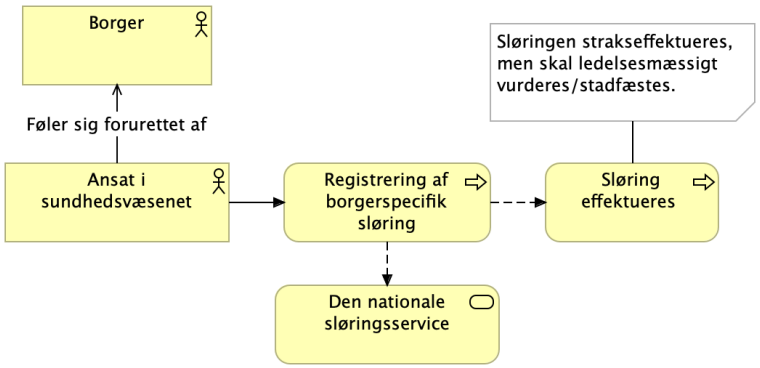


Figur 13: Forretningsproces for sløring i digitale borgervendte løsninger.

3.5.2 Forretningsproces for registrering af en borgerspecifik sløring

En borgerspecifik sløring affødes som ovenfor nævnt typisk af, at en ansat føler sig utryg i forhold til sin privatperson på grund af en borger. Den ansatte kan i et egnet fagsystem registrere sløringen, som træder i kraft øjeblikkeligt. Der er dog tale om en sløring, som **skal** stadfæstes af en ledelsesrepræsentant på behandlingsstedet (se næste afsnit).

En borgerspecifik sløring registreres ved hjælp af forretningsservicen "Sløringsregistreringsservice".



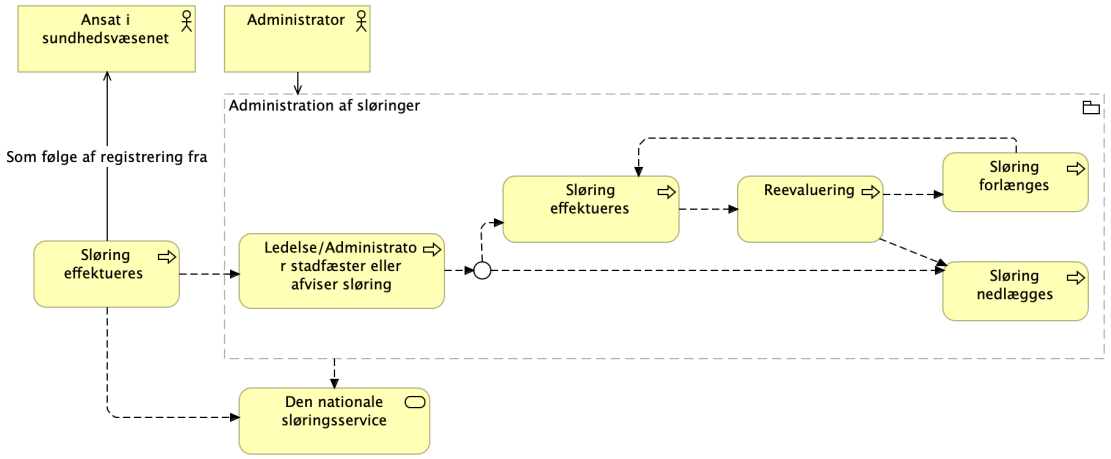
Figur 14: Forretningsproces ved ansattes registrering af en (midlertidig) sløring.

3.5.3 Forretningsproces for administration af borgerspecifikke sløringer

Administrationen af en sløring følger et typisk forløb, hvor en sløring kan skifte status (fra ikke-stadfæstet til stadfæstet), kan forlænges eller kan nedlægges. Det er kun administratorer, dvs. ansatte med særlige privilegier til sløringsadministration, der på vegne af ledelsen kan foretage disse handlinger.

En nyregistreret sløring skal behandles hurtigst muligt af en administrator/leder, så den enten kan blive stadfæstet eller afvist (nedlagt). Hvis en sløring skal fortsætte, skal der registreres en ny sløring fra den dato, den første udløber.

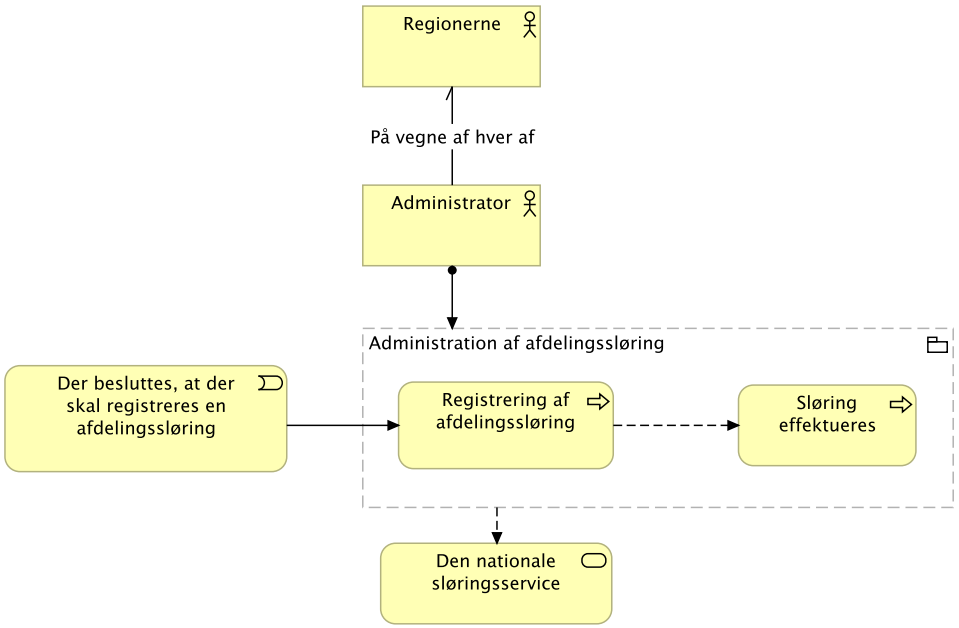
Bemærk: Det er op til den registrerende part at have processer og arbejdsgange, der sikrer rettidig stadfæstelse og reevaluering. Den nationale service har ingen viden om status, kun om udløbstidspunkt.



Figur 15: Administrativ livscyklus for sløringer.

3.5.4 Forretningsproces for registrering af en afdelingssløring

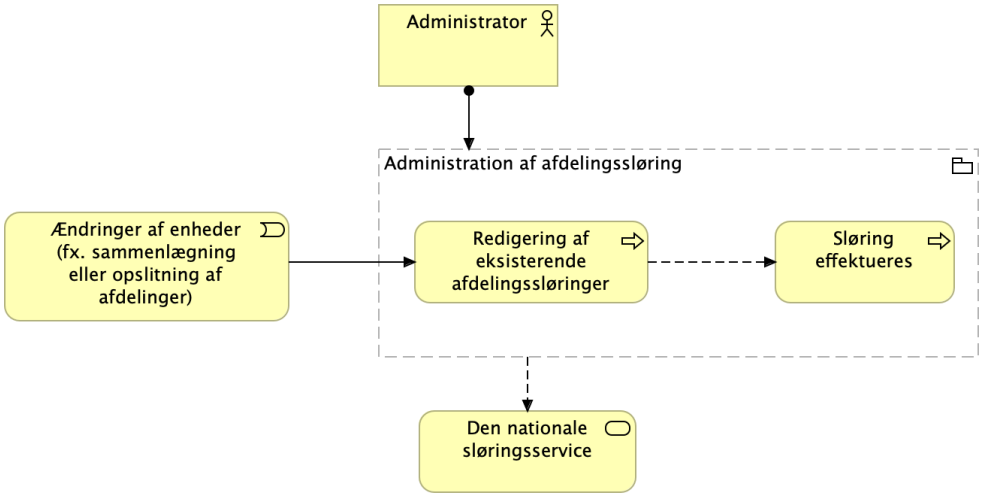
Regionerne udpeger hver en administrator, som skal være ansvarlig for administrationen af afdelingssløringerne. Det er disses ansvar at indgive de SOR-koder på afdelinger, hvor regionen har vurderet et behov for en afdelingssløring. Når en administrator registrerer en afdelingssløring, effektueres den øjeblikkeligt. I modsætning til borgerspecifikke sløringer, har afdelingssløringer som udgangspunkt ikke en udløbsdato.



Figur 16: Registrering af en afdelingssløring. Afdelinger angives i SOR klassifikationen, og det kontrolleres, at den angivne SOR-enhed findes ved oprettelse.

3.5.5 Forretningsprocessen for administration af afdelingssløring

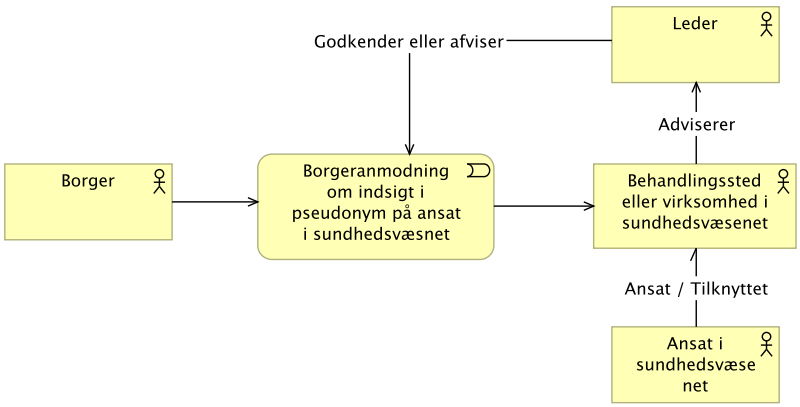
Administrationen af en afdelingssløring effektueres med det samme, og kan kun foretages af en administrator. En ændring affødes typisk af ændringer i enheder, som medfører ændringer i SOR-hierarkiet. Det kunne eksempelvis være ved sammenlægning eller opsplitning af afdelinger.



Figur 17: Administration af en afdelingssløring.

3.5.6 Forretningsproces for borgerhenvendelse om indsigt

En borger har ret til at anmode et behandlingssted om indsigt i et pseudonym på en ansat i sundhedsvæsnet, der har tilgået borgerens sundhedsdata. I logning og journalføringsbekendtgørelsens § 3 stk. 2 kræves det, at "Behandlingsstedet skal efter anmodning fra patienten udlevere oplysninger om identiteten på personen bag oplysningerne i stk. 1, medmindre der foreligger afgørende hensyn til andres private interesser". Det er op til den/de ledere tilknyttet behandlingsstedet at afgøre, hvorvidt en borger må få indsigt.

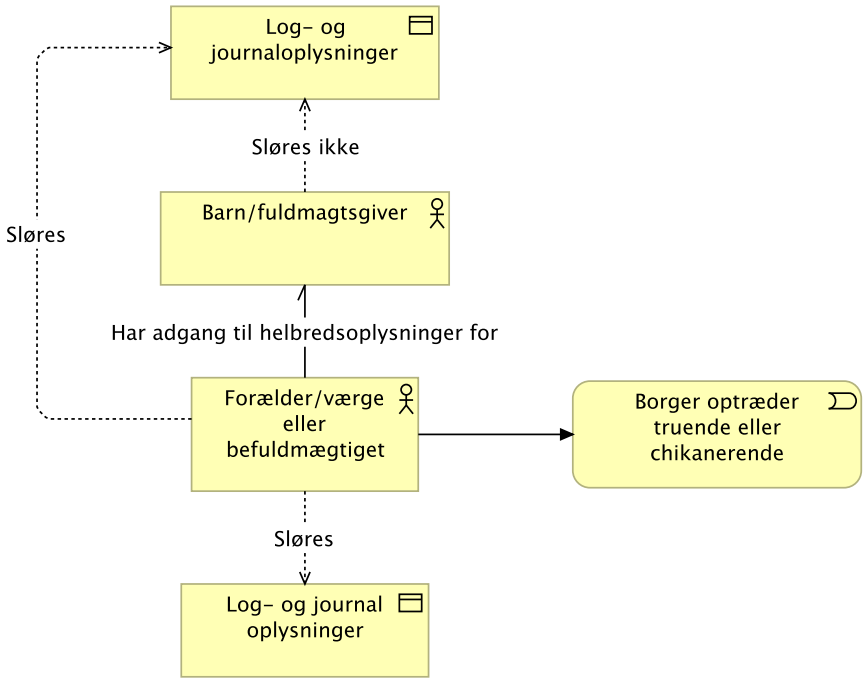


Figur 18: Forretningsproces for borgerhenvendelse ift. udlevering af den rigtige identitet bag et pseudonym.

Bemærk: Jf. afsnit 1.4.6, er anmodning om indsigt i pseudonymiserede identiteter er ikke aktindsigt. Det vil sige at en borger potentielt ved afslag på indsigt i pseudonymet, kan anmode om aktindsigt, hvorefter myndigheden igen skal vurdere, hvorvidt der i det hele taget vil gives aktindsigt, eller om der skal sløres i de akter, der gives indsigt i.

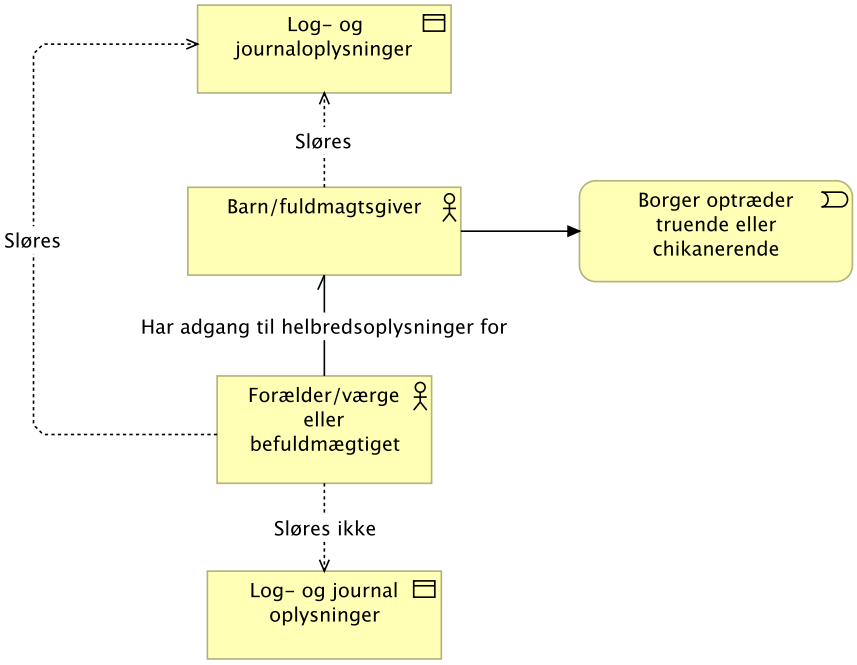
3.5.7 Forretningsproces for sløring af relaterede personer

Hvis en nærtstående, f.eks. en forælder eller en værge har optrådt truende eller på anden vis skaber utryghed for en ansat i sundhedsvæsenet, kan den ansatte registrere en sløring overfor vedkommende. Hvis forælderen eller værgen herefter tilgår log- eller journaloplysninger, uanset om det er egne eller for dem de er forælder eller værge for, skal identiteter sløres for vedkommende.



Figur 19: Sløring for forælder/værge/befuldmægtiget der har optrådt truende eller chikanerende

Er der registreret en borgerspecifiksløring for barnet, vil både forældre, værger og bemyndiget, få sløret for barnets log- og journaloplysninger, men ikke for egne.

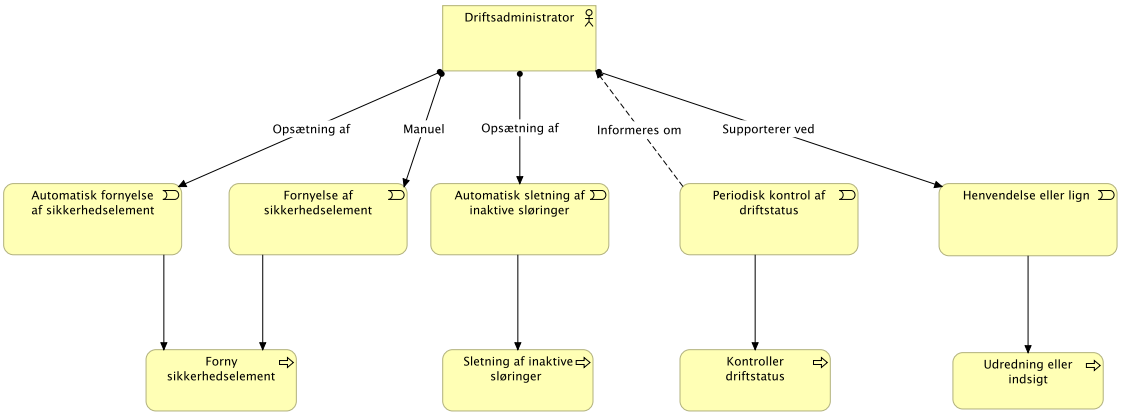


Figur 20: Sløring for forælder/værge/befuldmægtiget hvis barn/fuldmagtsgiver har optrådt truende eller chikanerende

3.5.8 Forretningsproces for driftsadministration

For den driftsansvarlige administrator for sløringsservicen er der en række vedligeholdelses opgaver:

- Sikkerhedselementer ift. pseudonymers sikkerhed og entydighed mv. skal periodisk fornyes. Dette uddybes i efterfølgende afsnit.
- Sikkerhedselementerne skal også ved behov kunne fornyes manuelt. Dette uddybes i efterfølgende afsnit.
- Inaktive sløringer slettes fra servicen automatisk.
- Den nationale sløringsservice skal være tilgængelige 24/7 under overvågning, og derfor får administrator en alarm, hvis servicen ikke er tilgængelig.



Figur 21: Forretningsprocesser for vedligehold for driftsadministrator samt andre henvendelser.

3.6 Forretningsregler for borgerspecifikke sløringer

I dette afsnit listes de forretningsregler, der er identificeret i forbindelse med tilblivelsen af dette målbillede i relation til borgerspecifikke sløringer.

#	Forretningsregel	Beskrivelse
BSS-1	Stadfæstning af borgerspecifikke sløringer	En borgerspecifik sløring kan registreres af en vilkårlig ansat i sundhedsvæsenet. Sløringen vil straks træde i kraft, men skal ledelsesvurderes før den kan betragtes som stadfæstet.
BSS-2	Behandling af ikke-stadfæstede borgerspecifikke sløringer inden for 24 timer.	En midlertidig sløring bør stadfæstes eller afvises inden for 24 timer fra registreringen.
BSS-3	Reevaluering af borgerspecifikke sløringer.	En myndighed skal løbende evaluere alle borgerspecifikke gyldige sløringer så det fortsatte sløringsbehov vurderes. En borgerspecifik sløring kan maksimalt være gyldig i 90 dage. Ved reevaluering af en borgerspecifik sløring kan denne for hver evaluering forlænges i op til 90 dage. Myndigheden skal sikre sig, at ikke-relevante sløringer nedlægges hurtigst muligt efter den vurderes som ikke-relevant.
BSS-4	Anvendelse af sløringsregistreringer	En registrering af en borgerspecifik sløring må kun anvendes til at afgøre, hvilke identiteter der skal vises i en borgervendt præsentation (digitalt eller analogt).
BSS-5	Sletning ved dødsfald.	Såfremt en borger dør slettes data i registret automatisk jf. forretningsregel **Ø-3** nedenfor.
BSS-6	Sløring følger personen ved adgang til andres oplysninger.	Er der sløret for en person, og denne person som forælder, værge eller bemyndiget tager adgang til en anden persons log- eller journaloplysninger, skal der også sløres.
BSS-7	Sløring for nærtstående.	Er der lagt sløring på en person gælder følgende ved andres adgang til dennes oplysninger: Forældre: der skal sløres. Værge: der skal sløres. Bemyndiget: der skal sløres.

BSS-8	Rækkevidde af sløringer, kun egen organisation.	En organisation kan kun oprette sløringer for egen organisation (CVR-nummer).

3.7 Forretningsregler for afdelingssløring

#	Forretningsregel	Beskrivelse
AS-1	Registrering af afdelingssløring.	Alle SHAK og SOR-koder for en afdeling skal registreres. Løsningen tilbyder ikke traversering op eller ned i afdelingshierarkier. Derfor er det den registrerende parts ansvar at registrere alle de nødvendige SHAK og SOR-koder for at få den nødvendige beskyttelse af de ansatte. Det gælder også eventuelle historiske SHAK og SOR-koder, hvor der har været behov for at foretage sløring.
AS-2	Afdelingssløring for underafdelinger.	Hvis afdelingens underafdelinger også skal sløres, skal alle tilknyttede SHAK/SOR-koder registreres for disse.
AS-3	Ændringer i afdelingshierarkier.	Ændringer i afdelingshierarkier slår ikke igennem automatisk i sløringsregistret. Det er derfor op til den pågældende part at foretage nødvendige ændringer i sløringsregistret ved ændring i egen organisation både ift. SHAK og SOR-koder.
AS-4	Effektuering af afdelingssløring.	En registrering skal træde i kraft umiddelbart efter registrering.
AS-5	Sletning af afdelingssløring.	Afdelingssløringer har ingen udløbsdato, men skal kunne eksplicit nedlægges af den registrerende part.
AS-6	Oversigt over registrerede afdelinger.	En part kan fremsøge en liste over registrerede afdelinger inden for eget CVR-nummer.

3.8 Øvrige forretningsregler

#	Forretningsregel	Beskrivelse
Ø-1	Pseudonymers entydighed	Pseudonymer skal kunne kommunikeres af en borger. Der er ikke krav om global entydighed, men et pseudonym skal sammen med et tidspunkt være tilstrækkeligt til at kunne re-identificere den ansatte inden for den pågældende organisation. Pseudonymer skal ikke være entydige over tid, men bør være entydige i visningsøjeblikket (på tværs af løsninger).
Ø-2	Pseudonymet skal knyttes til den specifikke borger	Pseudonymer skal knyttes til den enkelte borger, så den samme ansatte optræder med forskellige pseudonymer overfor forskellige borgere. Pseudonymer beregnes af visningsløsningerne, men skal være ens på tværs af løsninger.
Ø-3	Opbevaring af logs i 5 år og opbevaring af registerdata i 5 år efter sløringen er nedlagt.	Alle logs der indeholder oplysninger om administration og anvendelse af sløringsregistret skal opbevares i 5 år (loglinjer der er mere end 5 år gamle skal slettes). Registrerede sløringsdata skal slettes 5 år efter sløringen er nedlagt (5 år efter slutgyldighedstidspunkt).
Ø-4	Elementer til sikring af pseudonymers entydighed og sikkerhed skal løbende fornys.	For at sikre mod at pseudonymer kan afsløres ved tekniske analyser eller angreb, ændres sikkerhedselementer som indgår i beregning af pseudonymer periodisk med et passende interval. Desuden er det muligt at aktivere manuel fornyelse, hvis der er mistanke om kompromittering af pseudonymer.
Ø-5	Borgeren skal kunne se arbejdsfunktion og rolle for den ansatte, selvom identiteten er sløret.	Sløring må kun omfatte de ansattes navne. Borgeren skal stadig kunne se, hvilken arbejdsfunktion og rolle den slørede ansatte har, så den overordnede relevans stadig kan afgøres af borgeren.
Ø-6	Sletning efter borgerens død	Sløringer på en borger slettes 1 år efter borgerens død.

4. Informationsarkitektur

I dette kapitel beskrives koncepterne for informationsarkitekturen for identitetssløring af medarbejdere i det danske sundhedsvæsen. Kapitlet har til formål at beskrive de anvendte informationer i både den borgerspecifikke sløring, samt i afdelingssløringer, og de koncepter der går på tværs af de to løsninger. Herudover beskrives de komponenter, profiler og snitflader der anvendes i sløringsservicen.

4.1 Informationsarkitektur for borgerspecifikke sløringer

Til en sløringsregistrering af borgerspecifikke sløringer anvendes følgende informationer:

- Borgeridentifikation (CPR og på længere sigt evt. andre identifikationsklassifikationer)
- Organisations-ID (pt. CVR-nummer)
- Slutgyldighedstidspunkt

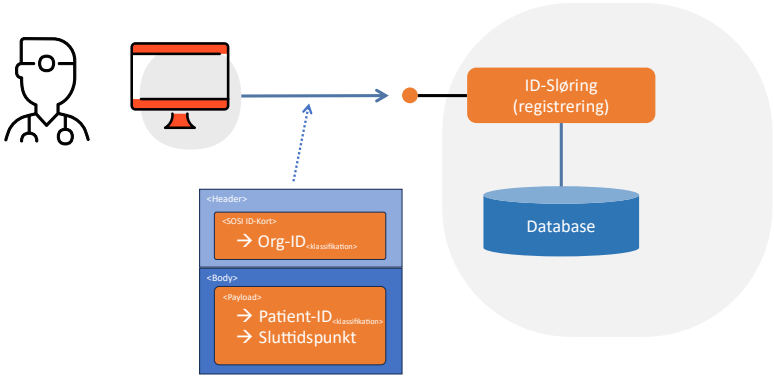
Borgeridentifikation anvendes til at knytte sløringen til den borger, der har udvist chikanerende eller truende adfærd, og som sløringen skal gennemføres overfor i borgervendte løsninger. Gyldigheden af identiteten kontrolleres af den nationale sløringsservice ved registrering, når der er et autoritativt register til rådighed, her CPR-registret. Hvis patient-ID'et ikke findes i det autoritative register, skal servicen fejle på en måde, så den ansatte er klar over at sløringsregistreringen ikke er sket.

Organisations-ID (CVR-nummeret) anvendes til at afgøre, hvilke ansatte der skal sløres. I sløringsservicen vil organisations-ID'et være det CVR-nummer, der er indlejret i autentifikationsbeviset[20], i kaldet til sløringsregistrering. Da autentifikationsbeviset er baseret på autentifikation gennem gyldigt OCES-certifikat eller MitID erhverv, sikrer det, at CVR-nummeret er gyldigt/retvisende for den registrerende part. Samtidig sikrer det, at en organisation ikke kan registrere sløringer for andre parter end sig selv. Bemærk i øvrigt at det kun er whitelistede organisationer, der kan oprette sløringer for egen organisation, og der er i whitelistningsprocessen indlagt kontrol af, at den organisation, der søger om whitelistning, har hjemmel til at kunne oprette sløringer.

Slutgyldighedstidspunkt angiver det datotidspunkt, hvor sløringen automatisk skal bortfalde. Det er et krav at registrere slutgyldighedstidspunkt, og slutgyldighedstidspunktet kan maksimalt være 90 dage efter registreringstidspunktet, se afsnit 4.4.1 for hvordan denne indgår i sløringsadministrationen. Skal sløringen opretholdes efter sluttidspunktet, skal sløringen genregistreres (se forretningsregel **BSS-3** i afsnit 3.6).

[20] SOSI ID-kort (niveau 3 eller 4) – se begrebslisten for uddybning.

For CVR-nummer og patient-ID medsendes klassifikationsoplysninger, så der i fremtiden vil kunne sløres for organisationer udtrykt i andre klassifikationer eller for borgere identificeret gennem andre identitetsklassifikationer end CPR.



Figur 22: Informationer der medsendes ved registrering af en sløring. Organisations-ID (CVR-nummeret) aflæses fra adgangsbilletten (ID-kort), patient-ID og sluttidspunkt medsendes som egentlige parametre.

Ændring af borgerspecifik sløringsregistrering

Når der registres en sløring, bruges sløringsadministrations-API 'et (se afsnit 4.4.1) for at oprette en sløring. Da de ansatte ikke har adgang til at se, hvorvidt en sløring allerede eksisterer, kan to ansatte i princippet lave en sløringsregistrering på samme borger. Sker dette, overskriver den sidste registrering blot den første, hvis registreringerne er inden for samme CVR-nummer. Ellers eksisterer der to sløringsregistreringer på samme borger, i forskellige CVR-numre.

Af hensyn til sporing og for at kunne påvise, hvad der lå til grund for en bestemt visning på et bestemt tidspunkt, må en sløring ikke slettes fra registret før et stykke tid efter den ikke længere er gyldig (se **Ø-3** i afsnit 3.8). Afslutning/Sletning af sløringer sker derfor ved at overskrive en eksisterende sløring med en ny med slutgyldighedstidspunkt "nu". Sløringen forbliver i registret som inaktiveret sløring indtil den slettes permanent.

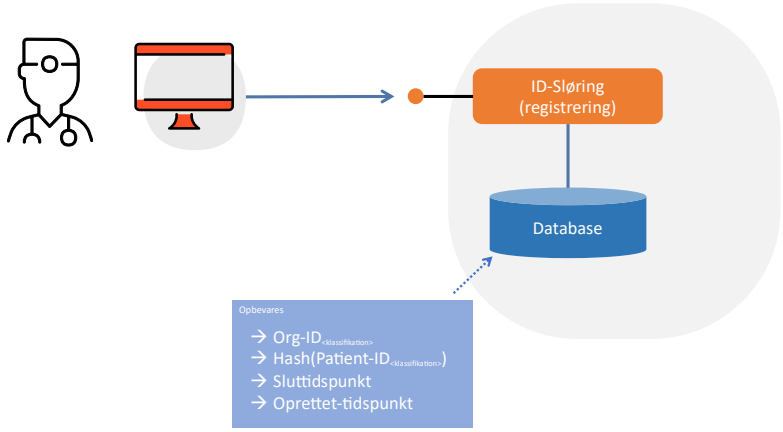
Tilsvarende for ændring af en sløring. Her slutmarkeres en evt. eksisterende sløring, og der oprettes en ny sløring med det nye gyldighedstidspunkt (maks. 90 dage fra nyt registreringstidspunkt).

Opbevarede informationer i registret

For at kunne udveksle informationer om borgerspecifikke sløringer på tværs af løsninger, er det nødvendigt at kunne rekvirere de gældende sløringer på tværs af sundhedssektoren ved en autoritativ service. Det er besluttet, at denne service leveres på den nationale service platform (NSP) i den nationale infrastruktur. Der er med løsningen lagt vægt på, at oplysningerne skal være placeret et sted, hvor der kun er adgang fra godkendte systemer, da informationerne er personhenførbare og følsomme, idet de kan indikere noget om personens adfærd/karakter. Hvis der gives adgang til de forkerte, vil informationerne kunne misbruges f.eks. til at skabe ulighed i

behandling eller forringelse af forsikringsmuligheder eller lignende. Der opbevares følgende informationer:

- Et hash[21] af Patient-ID og tilhørende klassifikation, for de borgere, hvor der er oprettet en sløring.
- Organisations-ID og dertilhørende klassifikationer, for de organisationer hvis ansatte skal sløres overfor den pågældende borger
- Slutgyldighedstidspunkt for sløringen.
- Oprettelsestidspunkt (ved oprettelse hhv. opdatering).



Figur 23: Oplysninger der opbevares per sløringsregistrering.

4.2 Informationsarkitektur for afdelingssløring

En afdelingssløring er som nævnt i afsnit 1.4.3 en proaktiv sløring, der ikke er knyttet til den enkelte borger, men er i stedet knyttet til afdelinger, hvor der generelt er større forekomster af vold, trusler om vold eller anden chikane. Afdelingssløring oprettes ved at registrere et SOR-ID[22] i den nationale service. En afdelingssløring har ingen udløbsdato, dvs. den er gyldig, indtil den nedlægges/slettes, så en registrering er på den måde en ON/OFF-registrering. Følgende informationer anvendes til at registrere en afdelingssløring:

- Organisations-ID
- Organisations-klassifikation (SOR/SHAK)
- CVR-nummer
- Valid to (anvendes kun ved nedlæggelse af en afdelingssløring)

Organisations-ID'et anvendes til at angive de afdelinger, hvor der er registreret en afdelingssløring. For en afdelingssløring skal organisationsklassifikationen angives som en SOR-kode og i

[21] Se begrebsliste

[22] I den tekniske udformning vil det i den første fase blive krævet at registrere afdelinger i såvel Sygehus- afdelingsklassifikationen (SHAK) som i SOR. Kravet om at registrere i SHAK vil bortfalde på et senere tidspunkt.

starten også en SHAK-kode, af hensyn til historikken. Derudover hentes et **CVR-nummer** fra autentifikationsbeviset, som anvendes til at bekræfte at SOR/SHAK-koden er en afdeling fra denne arbejdsplads. Derudover bruges CVR-nummeret til at afgrænse hvilke afdelinger der kan administreres på.

'Valid to' er som udgangspunkt "null", men anvendes fx til at nedlægge en afdelingssløring ved en angiven dato.

4.3 Pseudonymisering

Pseudonymisering af den ansatte sker på baggrund af en algoritme som alle borgervendte løsninger skal anvende. Pseudonymerne udregnes lokalt i den borgervendte løsning ved hjælp af UUIDv5, se afsnit 4.3.1 for uddybning. Pseudonymet udregnes på baggrund af tre inputs:

- Patient-ID/Borger-ID (typisk CPR)[23]
- For- og efternavn på den ansatte
- Et "secret salt", der er genereret ved hjælp af en tilfældighedsgenerator (består af tilfældige karakterer).

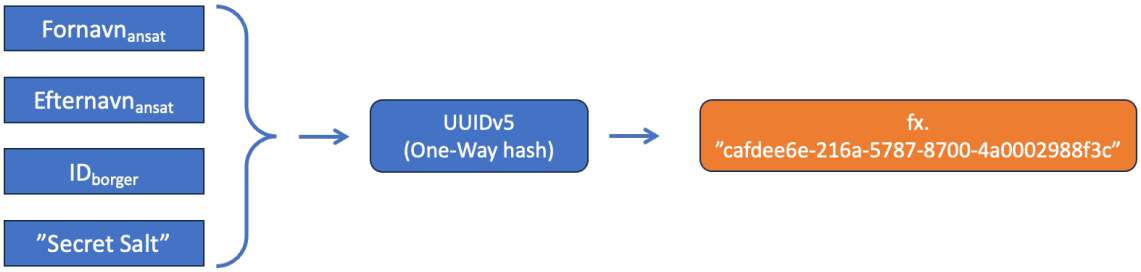
På den måde sikres det, at pseudonymet så vidt muligt er entydigt på tværs af løsninger. Derudover giver det borgeren mulighed for at sammenholde opslag i forskellige borgervendte løsninger på et givet opslagstidspunkt.

Borgerens ID (patient-ID) vil i første omgang altid være et CPR-nummer, men i fremtiden kan det være id'er fra andre klassifikationer. For- og efternavn på den ansatte er valgt som input til pseudonymet, da det er den laveste fælles nævner af identifikationsinformation, der fremgår på ansatte i de journalsystemer, der anvendes i de borgervendte løsninger. På den måde opnås entydighed på tværs af løsningerne bedst muligt. Hvis der er diskrepans i angivelsen af for- eller efternavn i forskellige anvendte systemer, vil pseudonymberegningen give forskellige pseudonymer for den samme ansatte. Det er en kendt risiko, som er afklaret med arbejdsgruppen bag dette målbillede.

Det fortrolige "salt" skal være med til at sikre hemmeligholdelsen af den ansattes identitet, så borgere ikke kan finde frem til den faktiske identitet ved at beregne pseudonymer for alle sundhedspersoner ('brute force' beregning på lækket CPR-register med navne samt viden om algoritmen[24]). Derfor udskiftes "secret salt" også periodisk. Det betyder at en sundhedsperson på forskellige opslagstidspunkter kan fremgå med forskellige pseudonymer, men på et givet tidspunkt som udgangspunkt altid vil fremstå med samme pseudonym på tværs af løsninger.

[23] **Bemærk:** hvis brugeren er en befuldmægtiget, forældre eller værge, der ser data for en anden person, skal man bruge ID'et for den, man ser data på (fuldmagtsgiverens, barnets eller værgemålsindehaveren).

[24] Hvilket man har, hvis man f.eks. læser dette (ikke-hemmelige) målbillede.



Figur 24: Psedonymberegningsalgoritmen binder pseudonymer til borgeren og sikret med et "secret salt".

4.3.1 UUIDv5

UUID er en Universal Unique Identifier, der returnerer en 32-karakter alfanumerisk streng på baggrund af et fast input. I modsætning til de typiske anvendelser af UUID, der returnerer et tilfældigt UUID, returnerer UUIDv5 det samme UUID, for et givet input, hvilket netop er hvad der er brug for i sløringssammenhæng[25]. Denne egenskab anvendes til at sikre at alle parter beregner det samme pseudonym på tværs af løsninger baseret på en anerkendt standard, ved at fastlægge hvilket input, der skal sendes til UUIDv5 algoritmen.

Ved udregningen af et UUID v5 pseudonym, gives som input generelt et namespace og en tekststreng. I sløringssammenhæng (nærværende målbillede) fastlægges:

- Namespace: OID-namespace, der per definition er 6ba7b812-9dad-11d1-80b4-00c04fd430c8.
- Tekststreng: "Fornavn+Efternavn+PatientID+'Secret Salt'"

"Secret Salt" gennemgås i afsnit 4.3.2. Bemærk at patientens ID også indgår i psedonym-beregningen. Den samme sundhedspersoner vil derfor fremstå med forskellige pseudonymer overfor forskellige patienter. Det øger sikkerheden idet flere patienter dermed ikke kan samarbejde om at afsløre pseudonymer.

For yderligere tekniske detaljer og eksempler henvises til Guiden på NSP-hjemmesiden[26].

4.3.2 "Secret Salt"

Saltet er den randomiserede værdi, der medregnes i pseudonymet, og har til formål at øge beskyttelsen af den bagvedliggende information, altså den ansattes identitet. Saltets længde har betydning for robustheden og sikkerheden i pseudonymet. Hvis saltet bliver for kort, kan det gættes (beregnes) hvis angriberen har adgang til blot få pseudonymer og viden om algoritmen (hvilket vi antager, da dette dokument ikke forventes at blive hemmeligholdt). Hvis saltet bliver

[25] https://developer.hashicorp.com/terraform/language/functions/uuidv5

[26] https://www.nspop.dk/pages/viewpage.action?pageId=220266653#id-3.(C)Pseudonymiseringidatakildertilborgervendtebruger-grænsefladesystemer-Trin5:Beregningafpseudonymer

for langt, vil det påvirke beregningen af hash-værdierne i negativ retning, da det har for stor vægt i forhold til de dynamiske dele af inputtet (fornavn + efternavn + patientID).

På grund af sikkerheden og følsomheden af informationen der ligger bag pseudonymet, er saltet dynamisk i den forstand, at det som ovenfor nævnt udskiftes periodisk. Det betyder, at selv hvis algoritmen og det aktuelle salt bliver kendt, kan der genereres et nyt salt, og algoritmen er igen sikker. Det aktuelle salt hentes med en af funktionerne i sløringsopslags-API'et. API'et uddybes i afsnit 4.4.2 og 4.4.3.

Generelt er det i kryptografiske analyser vist, at saltets længde helst skal være nogenlunde det samme som længden af de dynamiske dele. I denne sammenhæng sættes længden til 16 bytes, hvilket i base64 kodning svarer til 22 karakterer bestående af værdierne [a-z, A-Z, 0-9, / , + , . , -] (små og store bogstaver, tal, /, + , . og -). 16 bytes er samtidig længden af UUID (Universal Unique Identifier), som per definition er et godt salt[27] pga. de indbyggede tilfældighedselementer i UUID.

Saltet skal være hemmeligt og må kun anvendes i de dele af infrastrukturen, hvor det er bedst beskyttet. Frem for at have processer til manuel udveksling af "salt", er det besluttet at etablere en beskyttet service, hvor kun relevante løsninger kan hente det aktuelle salt. Samtidig vil der være tilslutningskrav til denne service, hvor anvendere forpligtes til ikke at persistere eller videregive saltet.

4.3.3 IDWS-billetten (IdentityToken)

IDWS-billetten er en teknisk "borgerbillet" der kan give adgang til OIO identitetsbaserede webservices, når en borger er logget ind i en borgervendt løsning[28]. I relation til ID-sløring er det besluttet, at alle sløringsinformationer om den borger, der er logget ind for at se sine[29] data, kommunikeres gennem disse tekniske borgerbilletter.

Derfor indeholder IDWS-billetten fremover en række elementer som gør det muligt for datakilder at sløre for den pågældende borger. Elementernes indhold og struktur reguleres gennem nogle XML subprofiler til IDWS-standarden. Der er i forbindelse med ID-sløring udarbejdet to subprofiler (gennemgås nærmere nedenfor):

- BIP-profilen indeholder sløringsinformationer om, hvilke organisationers ansatte der skal sløres for.
- SRP-profilen indeholder informationer om de relationer brugeren har til den, vedkommende ønsker at se data for (person i værge eller barn).

Derudover genbruges en eksisterende profil (OIO Basic Privilege Profile) til kommunikation af fuldmagter afgivet i den fællesoffentlige fuldmagtsløsning.

[27] https://docs.rs/password-hash/latest/password_hash/struct.Salt.html

[28] Læs om omveksling til IDWS adgangsbillet: https://www.nspop.dk/pages/viewpage.action?pageId=231286807

[29] Eller se data for børn, værgemyndlinge eller for fuldmagtsgivere

4.3.4 Blurring instructions profile (BIP[30])

BIP er en subprofil til OIO Identy Token Profile, og regulerer indholdet af sløringsinformationer i Identity Tokenet. BIP kan sammenlignes med OIO Basic Privilege Profile (BPP), men hvor BPP angiver en række privilegier en person kan have fået tildelt, fx fuldmagter, så fratager BIP'en den pågældende borger noget de ellers har ret til – at se navne på sundhedspersoner i borgerettede løsninger. Profilen anvendes ved omveksling af bootstrap tokens hhv. JWT tokens til OIO SAML Identity Tokens (gennemgås nærmere i afsnit 5.3.2).

BIP kommunikerer alle sløringer for den person, der er logget ind, samt de sløringer der evt. måtte gælde for den relaterede person, som den indloggede person søger oplysninger om (barn, person i værge eller fuldmagtsgiver). Hvis der ikke eksisterer aktive sløringer for den pågældende borger, sendes en tom liste.

I BIP elementet medsendes også det aktuelle salt, der skal anvendes til pseudonymiseringen af den sundhedsansattes identitet. Dermed har modtageren alt, hvad der skal bruges for at kunne effektuere sløringer, og skal derfor ikke selv til at rekvirere oplysninger fra andre systemer.

Nedenstående figur er et ikke-normativt eksempel på en borgerspecifik sløring, hvor CVR-nummeret på den organisation der har registreret sløringen fremgår. Reason="specific_for_person" angiver at det er en borgerspecifik sløring.

```
<?xml version="1.0" encoding="UTF-8"?>
<bip:BlurringInstructions
   xmlns:bip="urn:dk:healthcare:saml:blurring_instruction_profile:1.1"
   currentSalt="5kZZLNQMNIkz1Y7tCDj3GQ==">

   <bip:BlurEmployeeNamesFromOrg orgType="CVR" reason="specific_for_person">
      29190925
   </bip:BlurEmployeeNamesFromOrg>

   <bip:BlurEmployeeNamesFromOrg orgType="CVR" reason="specific_for_person">
      29190941
   </bip:BlurEmployeeNamesFromOrg>

</bip:BlurringInstructions>
```

Figur 25: Eksempel på en borgerspecifik sløring fra både Region Midtjylland og Region Nordjylland

En afdelingssløring vil have angivet både afdelingens organisationstype og angivelsen af at det er en afdelingssløring; reason="specific_for_department".

[30] Nyeste profil ligger her: https://www.nspop.dk/pages/viewpage.action?pageId=214161460. Bemærk eksemplerne i dette dokument er ikke-normative, og kan være misvisende ift. nyeste profil-standard.

```
<?xml version="1.0" encoding="UTF-8"?>
<bip:BlurringInstructions
   xmlns:bip="urn:dk:healthcare:saml:blurring_instruction_profile:1.1"
   currentSalt="5kZZLNQMNIkz1Y7tCDj3GQ==">

   <bip:BlurEmployeeNamesFromOrg orgType="CVR" reason="specific_for_person">
      <!-- Slør for alle medarbejdere i Reg. Midt, CVR kode -->
      29190925
   </bip:BlurEmployeeNamesFromOrg>

   <bip:BlurEmployeeNamesFromOrg orgType="SOR" reason="specific_department">
      <!-- Retspsykiatrien Glostrup, SOR kode -->
      536331000016003
   </bip:BlurEmployeeNamesFromOrg>

   <bip:BlurEmployeeNamesFromOrg orgType="SHAK" reason="specific_department">
   <!-- Retspsykiatrien Glostrup, SHAK kode -->
   1500P1V
   </bip:BlurEmployeeNamesFromOrg>
</bip:BlurringInstructions>
```

Figur 26: Eksempel på en borgerspecifik sløring sammen med afdelingssløring.

4.3.5 Subject Relations Profil (SRP[31])

Ligesom BIP, er Subject Relations Profile (SRP), en subprofil til OIO Identity Token Profile, der udtrykkes som en SAML attribut i IDWS Identity Tokens. SRP kommunikerer oplysninger om verificerede relationer mellem et subjekt - dvs. den person der er logget ind i den borgerrettede løsning - og en anden person. Eksempelvis udtrykkes her, hvis en borger har forældremyndighed over et barn, eller hvis en borger er værge. Profilen skal anvendes i omveksling af Bootstrap tokens hhv. JWT tokens til OIO SAML Identity Tokens, ligesom BIP.

Relationen mellem subjektet og den anden person (i tilfælde af forældremyndighed barnet, og ved værgerelationen, den person borgeren er værge for) skal verificeres hos en autoritativ kilde, ellers kan billetten ikke udstedes.

Nedenstående figur er et eksempel på XML'en for en forældremyndighedsindehaver.

```
<?xml version="1.0" encoding="UTF-8"?>

<srp:SubjectRelations
   xmlns:srp="urn:dk:healthcare:saml:subject_relations_profile:1.1">

   <srp:VerifiedRelation
      relationType="parentalCustodyHolder"
      relatedPersonID="0101111234"
      relatedPersonIDType="URN:OID:1.2.208.176.1.2"
      relatedPersonAge="10”
   />
</srp:SubjectRelations>
```

Figur 27: Eksempel på attribut med subject relations.

[31] Nyeste profil ligger her: https://www.nspop.dk/pages/viewpage.action?pageId=214161460. Bemærk eksemplerne i dette dokument er ikke-normative, og kan være misvisende ift. nyeste profil-standard.

4.4 Logiske snitflader

4.4.1 Sløringsadministrations API

Sløringsadministrations API'et kaldes, når en ansat vil registrere en sløring. API'et har til formål at muliggøre, at:

- en sundhedsperson kan oprette en straks-effektueret sløring i det øjeblik behovet opstår.
- en ledelsesbeføjet medarbejder kan oprette, stadfæste, nedlægge eller forlænge en sløring.

Sløringsadministrations API'et har følgende funktioner:

createBlurring({patientID, idClassification}, enddateTime)

Med kaldet sendes patient ID, og den klassifikation som ID'et er udtrykt i. Gyldigheden af identiteten kontrolleres af den nationale sløringsservice ved registrering, når der er et autoritativt register til rådighed, her CPR-registret. Hvis patient-ID'et ikke findes i det autoritative register, skal servicen fejle på en måde, så den ansatte er klar over at sløringsregistreringen ikke er sket.

Der medsendes også det tidspunkt, der skal være slutgyldighedsdatoen for registreringen. Denne fejler hvis datoen angives i forkert format og hvis den overskrider den maksimale slutgyldighedsdato på 90 dage.

For afdelingssløringer vil der være følgende API:

createOrgBlurring(orgID, orgClassification) —> OK/Fail?

Opretter en ny afdelingssløring. Hvis organisations-ID'et er et SOR-id, kontrolleres det at SOR-id'et hører til den kaldende parts organisation (CVR-nummer), og fejler hvis det ikke gør.

listOrgBlurringsForCVR() —> {orgID, orgClassification}*

Returnerer listen af registrerede slørede afdelinger hørende til CVR-nummeret (fra SOSI ID-kortet) (* indikerer liste). Kan anvendes i administrationsløsninger til at vise allerede registrerede afdelingssløringer for det pågældende CVR-nummer.

removeOrgBlurring(orgID, orgClassification) —> OK/Fail?

Nedlægger en afdelingssløring. Her kontrolleres det, at der er match mellem det CVR-nummer, der registrerede afdelingssløringen, og det CVR-nummer der medsendes i kaldet (SOSI-ID-kortet).

4.4.2 Sløringsopslags API

Hvilke organisationers medarbejder-identiteter, der skal sløres for den pågældende borger, indbygges i STS'ens IDWS token. Det er således kun STS'en, der kalder sløringsopslagsservicen. Det skal sikres, at denne service kun kan anvendes af STS'en, da eksternt brug kan føre til misbrug

af sløringsinformationer (se forretningsregel **BSS-4**). STS'en skal i øvrigt konfigureres per audience, så informationer om sløringsregistreringer på givne organisations ID'er kun delegeres videre til relevante services.

API'et består af følgende funktion:

getBlurredOrganisations ({PatientID, idClassification})→{orgID, orgIdClassification}*

Servicen returnerer en liste af organisationer, hvis medarbejdere skal optræde under pseudonym overfor det angivne PatientID (* indikerer liste).

Hvis sløringsopslagsfunktionen af en eller anden årsag er utilgængelig, og STS'en derfor ikke kan få et svar fra servicen, skal STS'en af forsigtighedshensyn ikke udstede billetter. Se afsnit 5.3.4 for uddybende information.

4.4.3 Afdelingssløringsopslag

Informationer om borgerspecifikke sløringer kommunikeres som ovenfor nævnt gennem STS'ens OIOIDWS billet. Foruden disse sløringer, skal datakilder til borgervendte visninger også sløre for afdelinger, som der er registreret et sløringsbehov for (afdelingssløringer). Hvilke enheder, der (altid) skal sløres for, kan STS'en rekvirere gennem servicen:

listAllActiveOrgBlurrings() → {orgID, orgClassification}*

Servicen returnerer alle de organisations-ID'er, der skal sløres for. Listen forventes at være relativt stabil, og det anbefales derfor at cache disse oplysninger og kun periodisk hente dem igen. Servicen anvendes af STS'en til at indlejre sløringsinstruktioner i forhold til afdelingssløringer.

4.4.4 Salt API'et

Dette API anvendes af STS'en til at indlejre det gyldige salt i IDWS-token. API'et består af en enkelt funktion, der returneret de 16 bytes der udgør saltet.

getCurrentSalt() → [byte]

4.4.5 Driftsadministrations API

API´et har flere funktioner som driftspersonalet benytter til vedligehold af den nationale sløringsservice.

Saltet udskiftes løbende, når udskiftningsoperationen aktiveres. Det sker med passende intervaller gennem servicen:

RenewSalt() → ok?

Servicen kan både kaldes timer-baseret (normal periodisk udskiftning) og manuelt, f.eks. hvis der er mistanke om kompromitteret salt.

Sløringer opbevares som udgangspunkt i fem år efter udløbsdato af hensyn til sporbarhed og support. Herefter slettes sløringsregistreringen, så databasen ikke fyldes op med irrelevante sløringer. Derudover er der også behov for at slette sløringer 1 år efter en borgers død. Dertil anvendes driftsservicen:

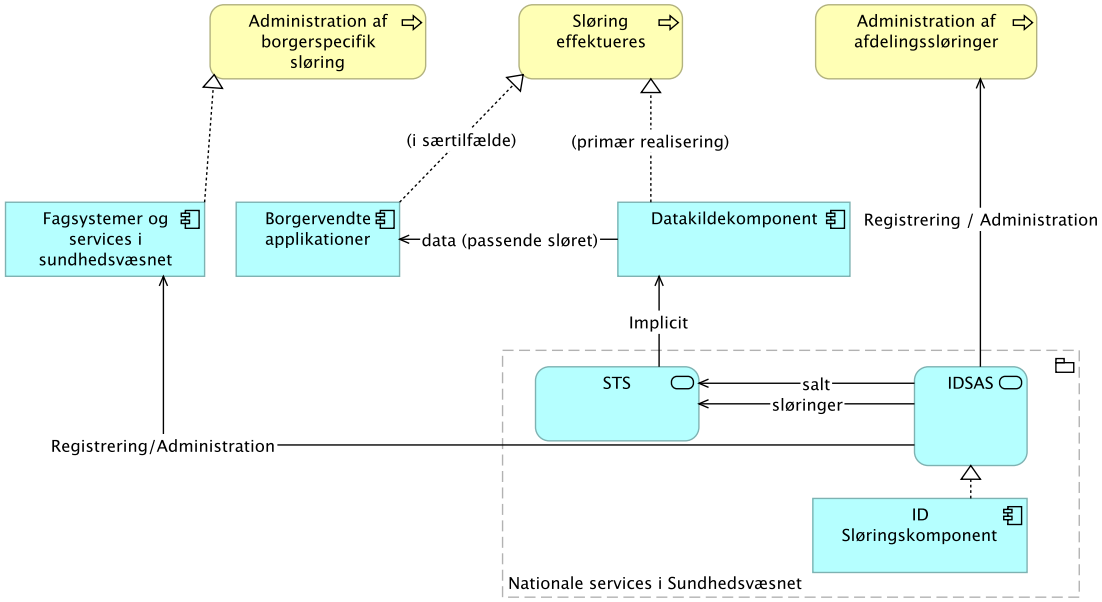
Cleanup-blurrings() → ok?

For at driftsadministratorerne kan sikre sig at ID-sløringsservicen er kørende som forventet, er der udviklet en statusrapporteringsservice hvor man ved kald kan få informationer om aktuel status ("HealthServlet"). Hvis der meldes fejl, vil en driftsadministrator kunne agere og forsøge at genoprette normal drift for servicen.

5. Applikations- og infrastrukturarkitektur

5.1 Applikationer og services vist i komponenter

Applikationsmæssigt realiseres administration af borgerspecifikke sløringer (forventeligt) i de registrerende parters fagsystemer. Sløringer effektueres gennem pseudonymisering i datakilderne til de borgervendte løsninger, men kan i særtilfælde effektueres i de enkelte borgervendte applikationer. Ved at placere sløringseffektuering i datakilderne, vil sløring slå igennem i alle borger-opslag i datakilden. Denne effekt opnås ikke ved at placere sløringseffektuering i den enkelte borgervendte løsning.

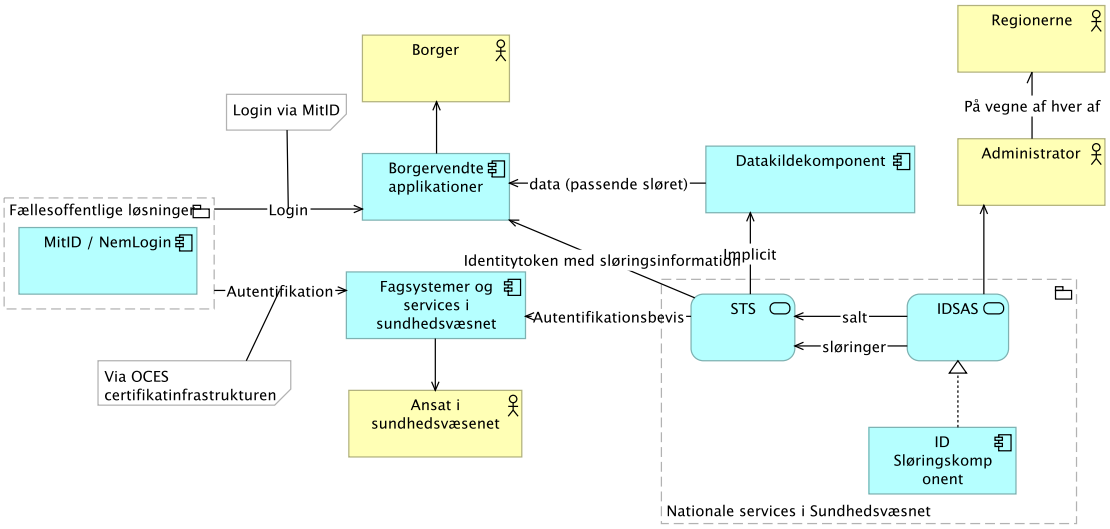


Figur 28: Overordnet komponentunderstøttelse af de væsentligste forretningsprocesser.

5.2 Fælles infrastruktur og støtteservices til komponenterne

Sløringsservicen anvender nogle af de allerede eksisterende nationale og fællesoffentlige services:

- Sikker loginfunktionalitet til borgere i relation til borgerrettede løsninger.
- Virksomhedscertifikater (VOCES) i relation til sikker autentifikation af registrerende organisation til registreringsservices.
- Sikkerhedsservicen STS på NSP'en ift. udstedelse af autentifikationsbevis forud for registrering af sløringer (Den Gode Web Service Niveau 3+4).
- Sikkerhedsservicen STS på NSP'en ift. udstedelse af identitytokens ved kald af datakilder fra borgerrettede løsninger.



Figur 29 Nationale og fællesoffentlige løsningers der er i spil.

Implementeringen af ID-sløringskomponenten (IDSAS) vil stille størst krav til services, der leverer oplysninger til borgervendte løsninger, hvor sundhedspersoners aktiviteter på pågældende borgeres helbredsoplysninger fremgår, og hvor pseudonymiseringen skal ske. En af disse services er MinLog servicen (eksempel på en "datakildekomponent" i ovenstående figur).

IDSAS er i sig selv en kommunikationsservice, og anvendere af systemet (fx regionerne) har ansvaret for administrationen af sløringer. Dette inkluderer oprettelse og sletning af sløringer.

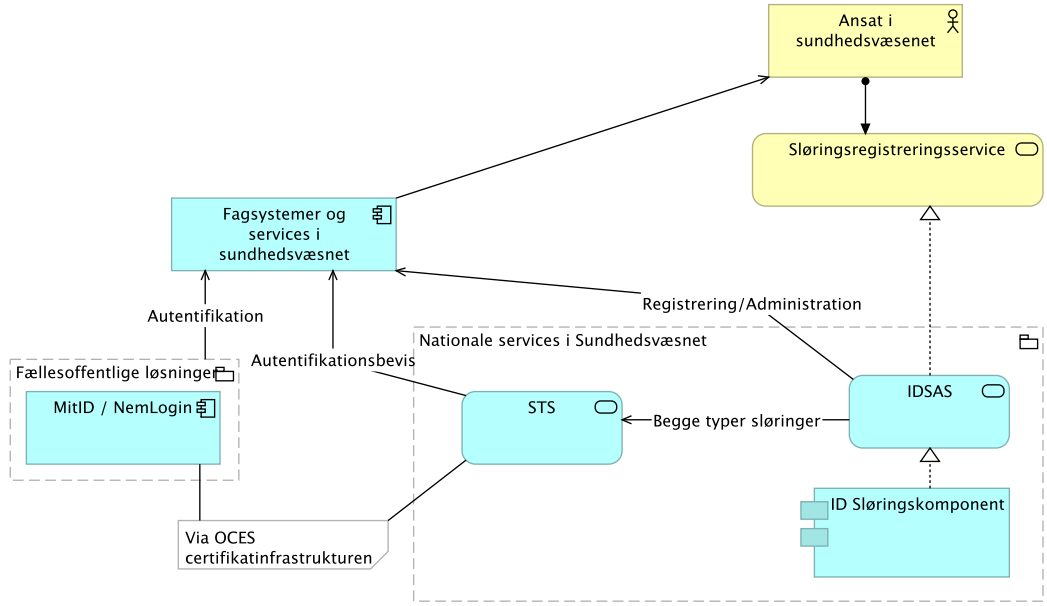
5.3 Applikationsflows

5.3.1 Administration af borgerspecifikke sløringer

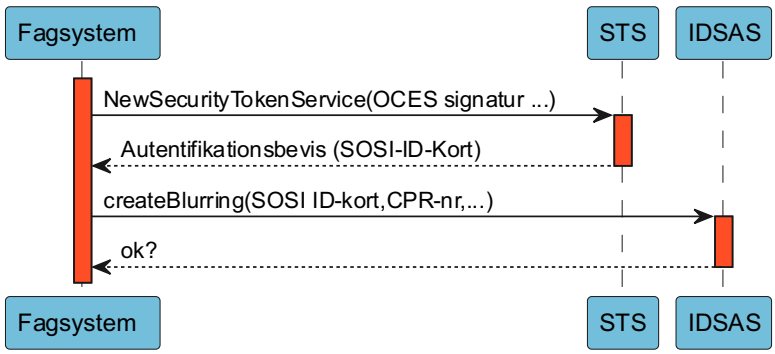
Det logiske forretningsflow for dette blev gennemgået i afsnit 3.4, men det konkrete applikationsflow er noget anderledes, især som følge af sikkerhedshåndtering.

Sløringsregistreringsservicen gøres tilgængelig for ansatte, gennem dennes lokale løsning (fx EPJ). Sløringsregistreringsservicen anvender sløringsregistreringskomponenten til at oprette en sløring, men forinden denne kan kaldes, skal der rekvireres et autentifikationsbevis fra den nationale STS på NSP. Autentifikationsbeviset er nødvendigt af hensyn til kontrol af, om det er en godkendt part (der har den fornødne aftale og hjemmel), der foretager registrering og administration.

Den borgerspecifikke sløring oprettes/administreres ved at benytte funktionen *CreateBlurring*, som beskrevet i afsnit 4.4.1.



Figur 30: Applikationssammenhæng for registrering og administration af borgerspecifikke sløringer.



Figur 31: Simpelt flow for registrering/administration af borgerspecifikke sløringer.

5.3.2 Administration af afdelingssløringer

API'et til administration af afdelingssløring er et simpelt "opret/list/slet" API:

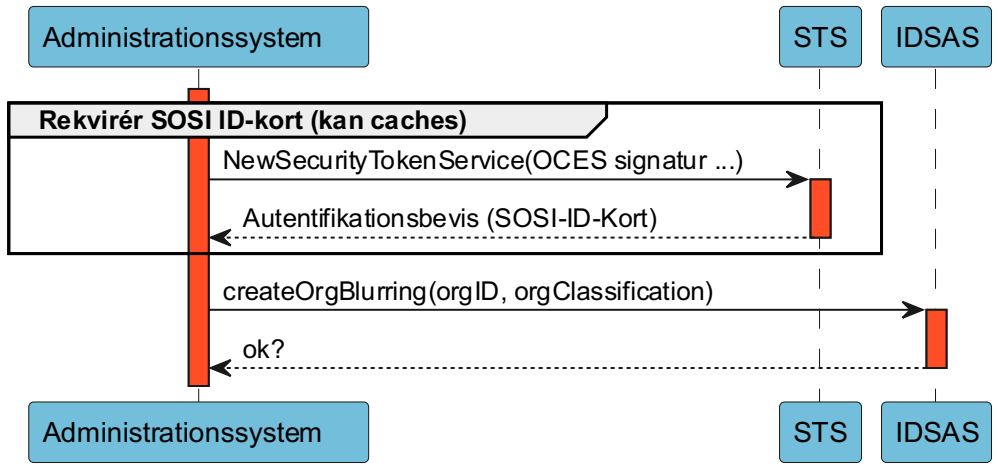
- *createOrgBlurring:* Opretter en afdelingssløring.
- *listOrgBlurringsForCVR*: Returnerer med listen over allerede registrerede afdelingssløringer i den organisation, der kalder list servicen.
- *removeOrgBlurring:* Markerer afdelingssløringen som ophørt.

Funktionerne er yderligere beskrevet i afsnit 4.4.1

Sikkerhedshåndteringen følger samme form som administrationen for individuel sløring (se afsnit 5.3.1), dvs. kald med et SOSI-IDkort på niveau 3 eller højere. Organisationens CVR-nummer registreres sammen med afdelingen i registret og bruges til valideringer:

- Hvis der registreres en SOR-kode kontrolleres det, at SOR-koden er inden for den kaldende organisations CVR-nummer. Bemærk: denne kontrol udføres kun for koder inden for SOR-klassifikationen, da der her er en entydig sammenhæng til CVR-nummer. Kontrollen udføres ikke for SHAK koder, men CVR-nummeret fra billetten gemmes sammen med registreringen.
- Når en organisation kalder listOrgBlurringsForCVR() returneres kun afdelingssløringer hørende til den kaldende organisations CVR-nummer.
- Når en organisation ønsker at slette en registrering, undersøges det om den kaldende part (CVR-nummer) matcher det CVR-nummer der blev gemt sammen med den oprindelige registrering.

Organisationen, som benytter servicen, forventes selv at op sætte regler for begrænsning af, hvilke administrative ansatte der gennem dennes lokale løsning vil få adgang til at administrere afdelingssløringer.



Figur 32: Simpelt flow for registrering/administration af afdelings sløringer.

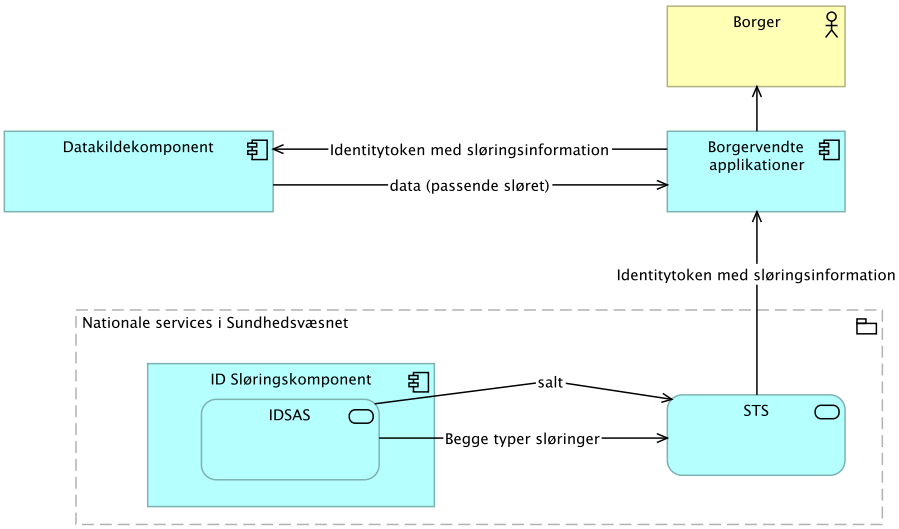
5.3.3 Effektueret sløring: borgervisning

Når en borger foretager et opslag i en borgervendt løsning (f.eks. Sundhedsjournalen i Sundhed.dk), vil den borgervendte løsning typisk indhente data fra forskellige bagvedliggende datakilder. Udskiftning af navne med pseudonymer skal som udgangspunkt foretages i datakilderne, og for at disse får de nødvendige oplysninger om registrerede sløringer, skal de udstilles som OIOIDWS snitflader og modtage et såkaldt identitytoken med sløringsinformationer i kaldet til dem.

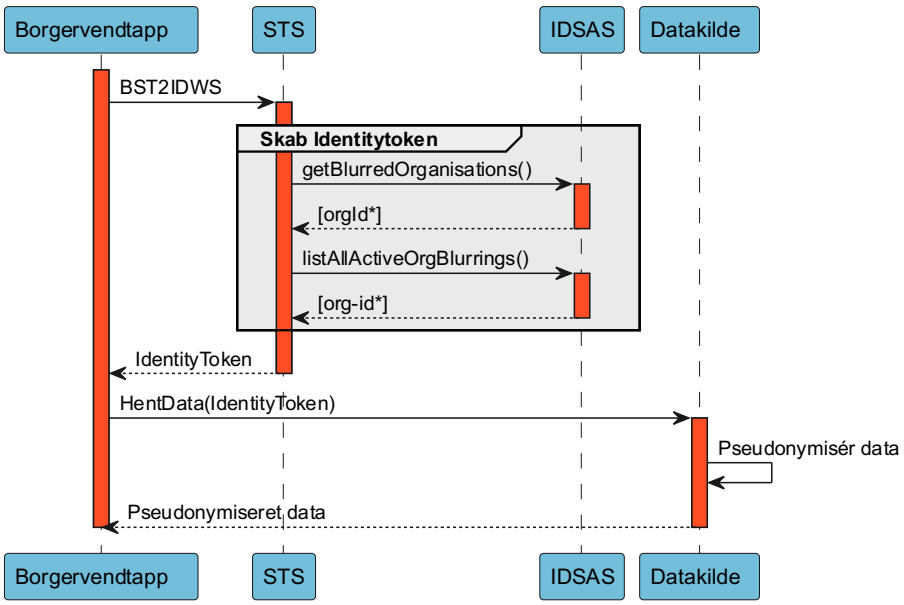
Før en OIOIDWS service kan kaldes, skal der derfor fremskaffes et identitytoken. Det rekvireres hos STS'en på NSP, hvor den borgervendte løsning "veksler" et bootstrap token (der blev udstedt

da borgeren oprindeligt loggede ind) til et identitytoken. STS'en vil bruge IDSAS komponenten (*GetBlurredOrganisations*) til at indlejre relevante sløringsinformationer i identitytokenet.

Dernæst kan den borgervendte løsning kalde datakilden. Den borgervendte applikation videresender det identitytoken den modtager fra STS'en, hvori oplysninger om CVR-numre der skal sløres for, afdelingssløringer og det aktuelle salt indgår. Datakildeservicen skal derudfra selv producere pseudonymer. Figur 33 illustrerer forskellige anvenderes adgang til IDSAS-komponenten.



Figur 33: Applikationssammenhæng for effektuering af sløring.



Figur 34: Flow for effektuering af sløring inkl. rekvirering af Identitytoken

5.3.4 Adfærd ved utilgængelig IDSAS-komponent

Hvis IDSAS-komponenten skulle blive utilgængelig, så det ikke er muligt at hente informationer vedr. sløringer, indtræffer et forsigtighedsprincip, som skal sikre at sundhedspersoners identiteter ikke bliver synlige i disse nedbrudssituationer. Hvis et sådan tilfælde indtræffer, vil STS'en stoppe med at udstede IDWS billetter, og løsninger, der anvender IDSAS, vil ikke kunne udlevere information til visning for borgeren. Der er på NSP'en etableret mitigerende handlinger, for at sikre sig imod overstående. Se afsnit 6 om sikkerhed.

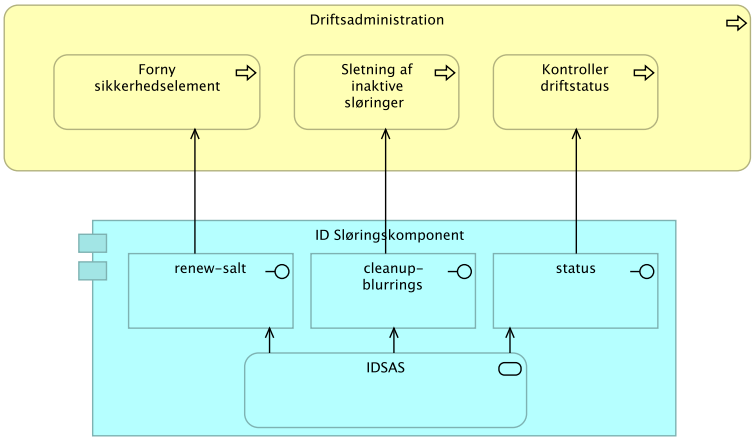
Når IDSAS-komponenten efterfølgende er reetableret vil STS´en igen udstede billetter med målrettede sløringsinformationer.

5.3.5 Driftadministration

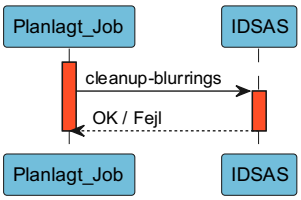
Driftsadministrationen består af tre dele:

- Fornyelsen af salt, det forventes at dette udføres ca. hver 30 dag.
- Tjek om sløringsservicen er tilgængelig, og alarmere administrator hvis der er problemer.
- Oprydning af inaktive (udløbne) sløringer og sløringer der skal slettes som følge af, at borgeren er død. Dette job forventes at blive afviklet en gang om ugen.

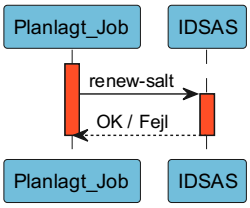
Det er ID sløringskomponenten der understøtter driftsadministrationen med de tre funktioner i Driftsadministrations API'et der blev gennemgået i 4.4.5.



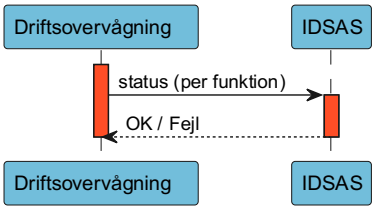
Figur 35 Applikationsunderstøttelse af driftsadministration.



Figur 36: Planlagt job til oprydning i sløringer.



Figur 37: Et andet planlagt job til fornyelse af 'secret salt'.



Figur 38: Kontrol af driftsstatus. Driftsovervågningsværktøj kalder periodisk *status()* på alle IDSAS services for at kontrollere hver enkelt service er kørende.

6. Sikkerhed

Nærværende målbillede omhandler udpegningen af borgere der overfor ansatte har optrådt truende, chikanerende eller på anden måde upassende. Disse individer fratages midlertidigt rettigheden til i digitale løsninger at se ellers tilgængelige informationer om hvem, der har deltaget i behandlingen. Borgeren har dog stadig mulighed for at henvende sig til behandlingsstedet for at søge om indsigt i den ansattes navn som pseudonymet dækker over ved henvendelse til behandlingsstedet. Borgeren har også stadig ret til aktindsigt.

Oplysninger om, hvem der er frataget disse rettigheder, er i sig selv følsomme, da det indikerer noget om personens karakter. Derfor er der i den tekniske løsning indarbejdet nogle ekstra tiltag, der beskytter mod misbrug og fejlanvendelse; blandt andet er det kun muligt, at få informationer om der er registreret en borgerspecifik sløring, når der veksles billetter i en borger login-kontekst. Oplysninger om sløringer er dermed kun tilgængelige for borgerrettede løsninger og f.eks. ikke for fagsystemer rettet mod sundhedspersoner (hvor det jo er de sundhedspersoner der er logget ind og ikke borgere). Samtidig er der etableret forskellige værn mod, at datalækager mv. kan afsløre identiteter på borgere, der er registreret sløringer på.

6.1 Logning

Sløringer anses ikke for at være helbredsoplysninger, og logges derfor ikke i MinLog.

6.2 Autenticitet, Tilgængelighed, Integritet, Uafviselighed og Fortrolighed

Den generelle diskussion af sikkerhed tager udgangspunkt i referencearkitekturen for informationssikkerhed på sundhedsområdet[32]. Heri opereres med følgende fem dimensioner ved sikkerhed:

Dimension	**Uddybning**
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.

[32] Referencearkitektur for informationssikkerhed. https://sundhedsdatastyrelsen.dk/-/media/sds/filer/rammer-og-retningslinjer/referenceaktitektur-og-it-standarder/referencearkitektur/referencearkitektur-informationssikkerhed.pdf?la=da

Dimension	Uddybning
Integritet	Egenskab ved et informationsaktiv, der sikrer dettes nøjagtighed og fuldstændighed. Integritet sikrer f.eks. kommunikation, således at en serviceudbyder og en serviceaftager er garanteret, at beskederne ikke ændres mellem afsender og modtager uden at én af parterne opdager det.
Uafviselighed	Egenskab ved information der gør det muligt at bevise, at en given bruger har udført en given handling på et givet tidspunkt.
Fortrolighed	Egenskab ved informationssystem der medfører, at kun bestemte brugere har adgang til bestemte data eller bestemt information.

Autenticitet

Autenticiteten af anvendere af de forskellige funktioner i IDSAS sikres via de nationale og fællesoffentlige standarder for digitale identiteter:

- Der er kun adgang til sløringsregistreringsservicen med et gyldigt DGWS-adgangsbillet (SOSI ID-kort), som udstedes på baggrund af autentifikation med de fællesoffentlige loginmidler hos MitID / OCES. Derudover er der kun adgang til servicen fra systemer, der er whitelistet til IDSAS på NSP'en. Registreringsservicen sikrer, at der kun kan sløres inden for det CVR-nummer, som det kaldende system eller den kaldende bruger (sundhedspersoner) kommer fra.
- Borgere autentificeres med privat MitID ved adgang til borgervendt digitale løsninger.

Kun driftsadministratorer kan få direkte adgang til selve databasen i registret. I et tilfælde hvor en administrator vil få behov for at tilgå registret, vil der vil være høje krav til sikkerheden for disse medarbejdere. Bemærk: der er lagt yderligere værn ind i dataopbevaringen, så lækager eller kompromitterede driftsadministratorer ikke får umiddelbar adgang til de følsomme oplysninger. Se mere om dette nedenfor.

Tilgængelighed

For at servicen er tilgængelig skal følgende være etableret:

- En sundhedsdatanetaftale og tilsvarende tilslutning.
- En NSP serviceaftale.
- Kun whitelistede organisationer kan kalde servicen. Ikke whitelistede kald afvises øjeblikkeligt.
- Selve servicen skal være tilgængelig (”oppe”).

Er ovenstående opfyldt, stilles sløringsregistreringsservicen tilgængelig for anvendere 24/7. Hvis den ikke er teknisk tilgængelig, vil en administrator få besked. Der er i NSP infrastrukturen indbygget en række værn mod DoS angreb og lignende. I forhold til sikring imod ondsindede

cyber-angreb, bliver der jf. strategien for cyber- og informationssikkerhed i sundhedssektoren[33] afholdt regelmæssige sikkerhedsaudits for at forudse disse, og der er på NSP etableret passende høj beskyttelse af de centrale komponenter for at forebygge angreb mod infrastrukturen. Desuden er der etableret overvågning af NSP-platformen.

Endelig er der i designet indarbejdet værn mod nedbrud som følge af afhængigheder. Et godt eksempel på dette er, at der bag registreringsservicen er et afkoblingspunkt, så et midlertidigt udfald i NSP netværksinfrastrukturen ikke medfører stop af registreringer i det kliniske led.

Integritet

Der er flere tiltag, der sikrer integritet:

- Al kommunikation sker gennem HTTPS / SSL der sikrer integritet på kanal-niveau.
- Anvendelsen af IDWS, hvor der dels kun kan veksles adgangsbilletter hos relevante STS'er, dels at udstedte billetter bliver kontrolleret for korrekt "audience" hos de services, der skal anvende billetterne. Tilsammen sikrer det, at borgervendte services forbliver i rette sikkerhedskontekst, og at det ikke bliver muligt at udvide sine privilegier til uretmæssigt at kunne ændre i oplysninger.
- Og endelig at IDSAS servicen gennem kontrol af CVR numre i parametre hhv. adgangsbilletter sikrer, at medarbejdere eller systemer hos uvedkommende virksomheder ikke kan ændre i oplysninger, der ikke tilhører dem.

Uafviselighed

Uafviselighed sikres typisk via. systembeviser eller digital signering. Ud over almindelig logning (systembevis på lav sikkerhedsniveau) er der ikke indarbejdet særlige uafviselighedsmekanismer i denne løsning.

Fortrolighed

Fortrolighed sikres primært gennem anvendelse af krypterede kommunikationskanaler og ved at sikre, at sløringsinformationer kun bliver kommunikeret i sessioner, hvor en bruger er logget ind.

Der er planer om at kryptere "Data at rest", men da dette ikke kunne etableres i de første versioner, er det besluttet at opbevare borgernes ID'er (CPR-numre) som sikre hashes i stedet, så en tilfældig datalækage ikke afslører de registreredes identitet.

[33]] Strategi for cyber- og informationssikkerhed i sundhedssektoren https://www.sum.dk/Aktuelt/Nyheder/Digitalisering/2019/Januar/~/media/Filer%20-%20dokumenter/2019/Cyberstrategi/SUM-Cyber-og-Informationssikkerhed_WEB_opsl.pdf

7. Governance

Målbilledet for national identitetssløring af sundhedsansatte inddrager ikke strategi for national governance, da denne er etableret i andet regi af projektet og i øvrigt læner sig op ad øvrig NSP governance.

8. Fremtidige versioner af målbilledet

Nærværende målbillede afdækker de hidtil identificerede behov for identitetssløring, og der forventes ikke at være yderligere, snarlige behov i forhold til sløring og sløringsservicen.

9. Appendiks A – Begrebsliste

Foretrukken term	Definition	Evt. borgervendt forklaring/kommentar/kilde
Afdelingssløring	En sløring af de ansattes identitet ved borgervisning af helbredsoplysninger fra udvalgte afdelinger/underenheder. Alle ansatte, der optræder i registreringer/logninger fra sløredе afdelinger, sløres.	
Aktindsigt	Adgang til at se dokumenter, der indgår i sagsbehandlingen hos en offentlig myndighed. Offentlighedslovens § 7. "Enhver kan forlange at blive gjort bekendt med dokumenter, der er indgået til eller oprettet af en myndighed m.v. som led i administrativ sagsbehandling i forbindelse med dens virksomhed."	Offentlighedslovens § 7.
Anden entydig identifikation	Anden identifikation end fulde navn, autorisationsnummer og CPR-nummer, der er sporbar for den sundhedsproducerende enhed.	
Behandlingssted	Organisation med egen ledelse der udfører sundhedsperson behandling og foretager sundhedspersoner optegnelser i et afgrænset informationssystem.	NBS[34]
Borger	Person der har pligter og rettigheder i forhold til en kommune, region eller stat.	NBS
Borgerspecifik sløring	En sløring knyttet til en specifik borger, der eksempelvis har udvist truende adfærd eller lignende.	

[34] https://sundhedsdata.iterm.dk

Foretrukken term	Definition	Evt. borgervendt forklaring/kommentar/kilde
Identitetssløring	Identitetssløring er den generelle betegnelse for sløringen af ansattes identitet. Der findes to måder, hvorpå en identitetssløring kan ske: ved en afdelingssløring og ved en borgerspecifik sløring.	
Hash eller hashværdi	Den resulterende værdi af at føre en tekststreng igennem en hashfunktion. Se mere om hashfunktioner her:	https://csrc.nist.gov/projects/hash-functions
Pseudonym	Tildelt identifikation, se "Anden entydig identifikation".	
Sløringsregistrering	En registrering af en sløring.	
Sundhedsperson	Sundhedsprofessionel der er autoriseret i henhold til særlig lovgivning til at varetage sundhedspersoner opgaver.	NBS
IDSAS	Identitetssløring af ansatte i sundhedsvæsenet.	
SOSI-ID-kort	Et teknisk autentifikationsbevis. Et ID-kort er signeret af STS'en (se nedenfor), og bekræfter identiteten på en sundhedsperson og angiver enkelte attributter om sundhedspersonern.	
STS	Sikkerhedsservices på NSP omfatter STS (Security Token Service). STS'en udsteder SOSI-ID kort og IDWS tokens.	
NSP	National service platform.	

10. Appendiks B – User Stories

Som **Ansat i sundhedsvæsenet** ønsker jeg**:**		
1	at kunne tilgå min patients helbredsoplysninger og uden videre kunne se, hvilke af mine kolleger, der har registreret journaloplysninger …	… så jeg f.eks. kan henvende mig til rette vedkommende og forhøre mig om tidligere forløb.
2	at kunne skjule min og mine kollegers identitet overfor en borger, men stadig har adgang til mine kollegers identiteter i eget fagsystem …	… så jeg ved, at en patient ikke har adgang til information der henviser til mig/os som privatperson.
3	at en sløring slår igennem i alle borgervendte visninger øjeblikkeligt …	… så jeg kan føle mig tryg ved, at borgere ikke får adgang til mine informationer.
4	at det skal være nemt og intuitivt at registrere en sløring …	… så jeg kan foretage sløringen hurtigst muligt når behovet opstår.
5	at stole på at mit ansættelsessted foretager en grundig vurdering af det (fortsatte) sløringsbehov i forbindelse med stadfæstelse eller evaluering af sløringsbehov…	… så jeg kan føle mig tryg ved at sløringer der skal fortsætte, ikke udløber.
6	at vide omfanget af en sløring, og hvordan denne foretages …	… så jeg ved hvilke konsekvenser sløringen har, og føler mig tryg ved at sløringen er fyldestgørende.
7	at jeg bliver informeret, hvis min sløringsanmodning bliver afvist …	… så jeg ved, at en borger, som jeg kan have følt mig forurettet af, har adgang til informationer om mig, og så vi alle får en forståelse af, hvad der lægges til grund for afvisninger.

Som **Borger** ønsker jeg:		
8	at have et overblik over mine sundhedsoplysninger …	… så jeg har adgang til relevant information om mit helbred og min behandling.
9	at kunne se hvem, der har haft adgang til hvilke af mine sundhedsoplysninger, hvornår og i hvilken sammenhæng …	… så jeg kan føle mig tryg ved, at kun relevante personer har haft adgang.
		… så jeg kan se, hvis en bestemt person har haft adgang.
		... så jeg kan danne mig et billede af, hvilke oplysninger, der er indhentet.
10	at kunne sammenholde forskellige opslag …	… så jeg kan se, om det er samme person der har haft adgang i forskellige sammenhænge eller forskellige perioder.
11	at jeg kan henvende mig til behandlingsstedet og henvise til en bestemt identitet, hvis denne er sløret for mig …	… så jeg kan få oplyst den rigtige identitet.
12	at kunne klage over sløringer, jeg mener er uberettigede …	… så jeg kan tilgå de informationer jeg har ret til, hvis sløringen er uberettiget.

som **Sløringsadministrator** ønsker jeg:		
13	at have en overskuelig arbejdsgang for sløringsadministration …	… så jeg kan nemt kan administrere og levere service til medarbejdere og ledelse.
14	at have overblik over de sløringer der er foretaget …	… så jeg har et overblik over hvornår og hvor mange sløringer udløber på en given dato.

som **Myndighed** ønsker jeg:		
15	at løsningen er lovmedholdelig …	… så jeg kan leve op til mit dataansvar.
16	at databehandlere leverer sikker og lovmedholdelig databehandling …	… så ansatte i sundhedsvæsnet får deres ønsker og krav håndhævet.
17	At et sløringsønske bliver behandlet af en administrator/leder hurtigst muligt efter der er anmodet om det …	… så en midlertidig sløring ikke automatisk udløber og at de ansatte ikke længere er sløret.
18	at kunne oprette en afdelingssløring...	... så sundhedspersoner der optræder i registreringer fra de afdelinger, der skal sløres for, automatisk bliver sløret.
19	at kunne kommunikere afdelingssløringer på en let forståelig måde ...	... så sundhedspersoner kan føle sig trygge.
		… så sundhedspersoner ikke opretter unødige personspecifikke sløringer.