RAPPORT 2023

# Målbillede for identitets-sløring af ansatte i det danske sundhedsvæsen

SUNDHEDSDATA-
STYRELSEN

**Resumé:**

Dette dokument er et mini-målbillede for 'Identitetssløring af ansatte i det danske sundhedsvæsen'. Det har til hensigt at sætte rammerne for national digital understøttelse af identitetssløring inden for sundhedsdomænet, så alle parter foretager identitetssløring på samme måde og kan kommunikere sløringsbehov 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. Identitetssløringen 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 identitetssløring 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 mini-målbillede fastlægger begreber, mål, principper, processer og forretningsregler for identitetssløring så alle, der kommer til at beskæftige sig med digitalisering af identitetssløring, har et ensartet sprog for og 'billede' af, hvad identitetssløring er, hvilken rækkevidde sløringer 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.

Nærværende målbillede er en nedskalleret udgave af et målbillede. Målbilledet er i fase 1 udarbejdet i et intensivt forløb med deltagelse af Region Nord, Region Midt, Region H. og Sundhedsdatastyrelsen. Øvrige parter har ikke været direkte involveret, men har fået målbilledet til kommentering. Desuden har målbilledet været præsenteret i rådgivende udvalg for standarder og arkitektur på sundhedsområdet (RUSA). Målbilledet fase 2 – hvor blandt andet afdelingssløringer og de mere tekniske detaljer er blevet fastholdt – er udarbejdet i efteråret 2023.

| | |
|---|---|
| **Udgiver** | Arkitekturfunktionen, Sammenhængende Digital Sundhed |
| **Ansvarlig institution** | Sundhedsdatastyrelsen |
| **Design** | |
| **Copyright** | |
| **Version** | 0.6 |
| **Versionsdato** | 14. december 2023 |
| **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 optimale digitale løsninger.

## 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. Konkrete emneinput til dette efterfølgende arbejde, udover førnævnte detaljerede transitionsprodukter, er givet i bilag 1 "Kommende afklaringer". Dette understreger også, at der fortsat må forventes, at der skal udarbejdes afklaringer og specifikationer i forbindelse med de efterfølgende implementeringsprojekter (dette er ikke alene klaret med målbilledet).

[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.

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].

### 1.2.2 Afgrænsninger

Nærværende målbillede er en nedskalleret udgave af et målbillede. Målbilledet er i fase 1 udarbejdet i et intensivt forløb med deltagelse af Region Nord, Region Midt, Region H. og Sundhedsdatastyrelsen. Øvrige parter har ikke været direkte involveret, men har fået målbilledet til kommentering. Desuden har målbilledet været præsenteret i rådgivende udvalg for standarder og arkitektur på sundhedsområdet (RUSA). Målbilledet fase 2 – hvor blandt andet afdelingssløringer og de mere tekniske detaljer er blevet fastholdt – er udarbejdet i efteråret 2023. Følgende afsnit er udgået:

- 1.3.1 Eksisterende (sammenhæng til andre målbilleder mv.)
- 1.4.7 Centrale aktører (udgår)
- 2.2 Interessenter og interesser (udgår)
- 2.5 Kvaliteter (udgår)
- 9 Fremtidige versioner af målbilledet (udgår)

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 ens 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

[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.

for at beskytte medarbejdere mod repressalier fra borgere, f.eks. hvis borgeren/patienten har udvist truende adfærd.

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 Eksisterende (udgår)

Sammenhæng med strategier og andre målbilleder.

## 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.

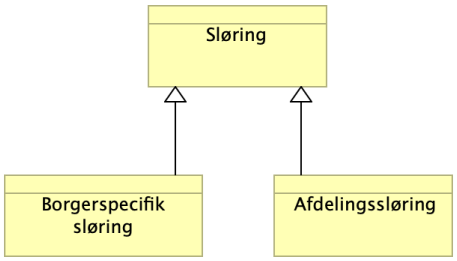
### 1.4.1 Identitetssløring

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 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

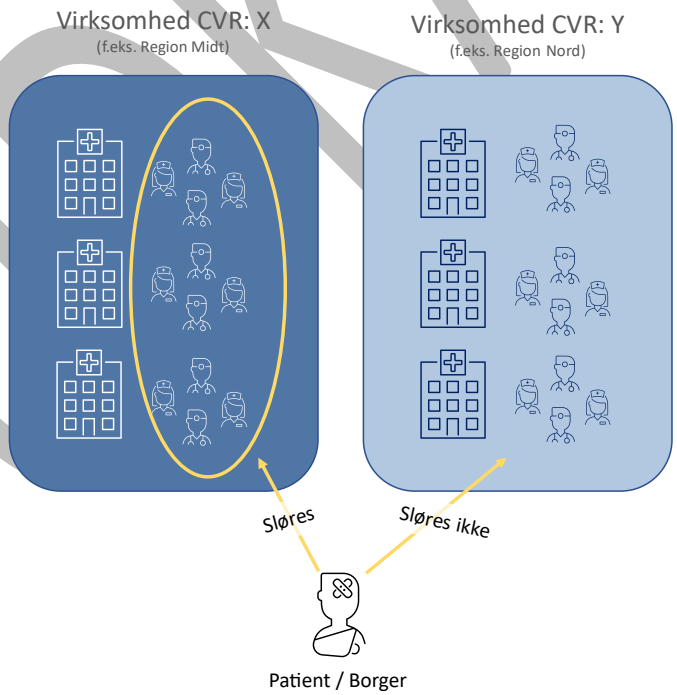



Figur 1: Sløringstyper

### 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 oplever adfærd (f.eks. truende, forfølgende eller på anden vis upassende), som gør medarbejdere i sundhedsvæsenet utrygge ift. deres privatperson eller privatsfære.

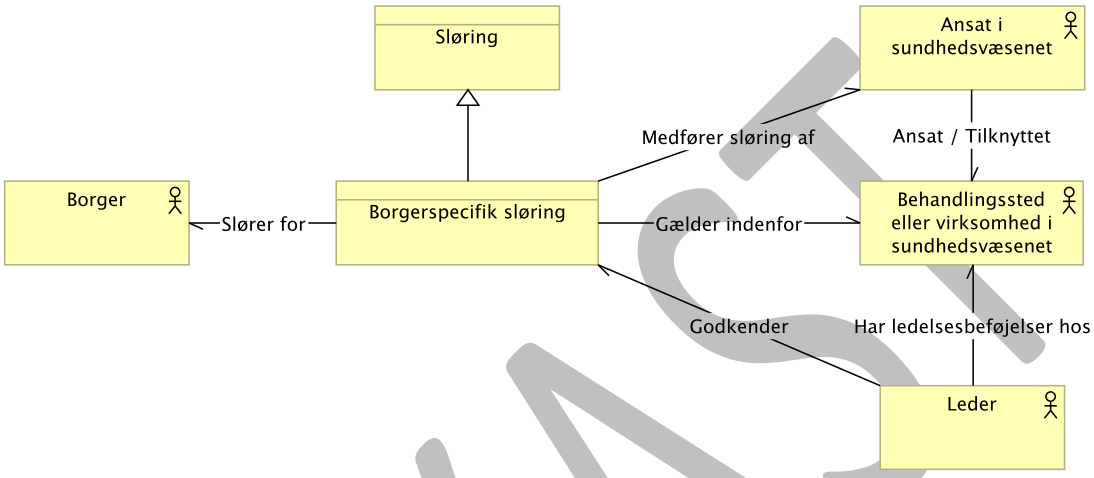
Hvis en ansat registrerer en borgerspecifik sløring vil alle kolleger også optræde som sløret overfor borgeren/patienten. En sløringsregistrering er således lige dele selvbeskyttelse som beskyttelse af kolleger (inden for samme organisation baseret på CVR nummer). En sløring af medarbejdere i en region 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 to år, 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.

#### 1.4.2.1 Sløringsregistrering for borgerspecifik sløring

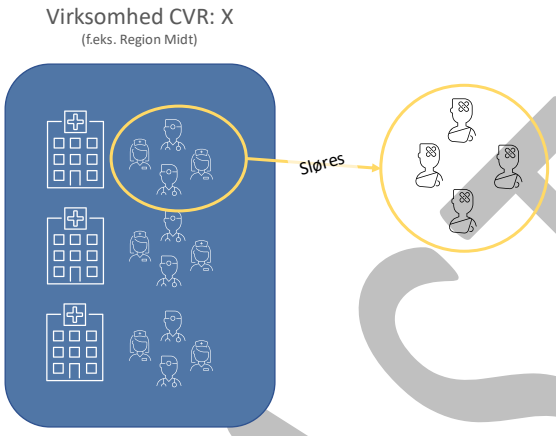
En sløringsregistrering dækker over den tekniske registrering af en sløring. En sløringsregistrering behandles af en leder/administrativ medarbejder hurtigst muligt efter registreringen. Sløringsregistreringen opbevares i et register, som anvendes af borgervendte løsninger til at afgøre, om der skal 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 er tilknyttet 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.

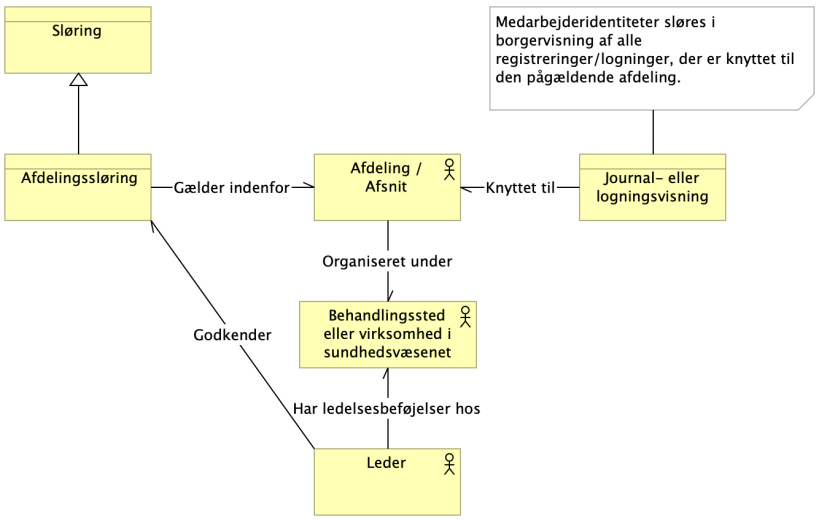
Ansatte, der optræder i visning af journal- eller logningsoplysninger fra den pågældende afdeling eller afsnit, vil blive sløret, uanset hvilken borger/patient der er tale om, og uanset om medarbejderen aktuelt er tilknyttet den pågældende afdeling.

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.

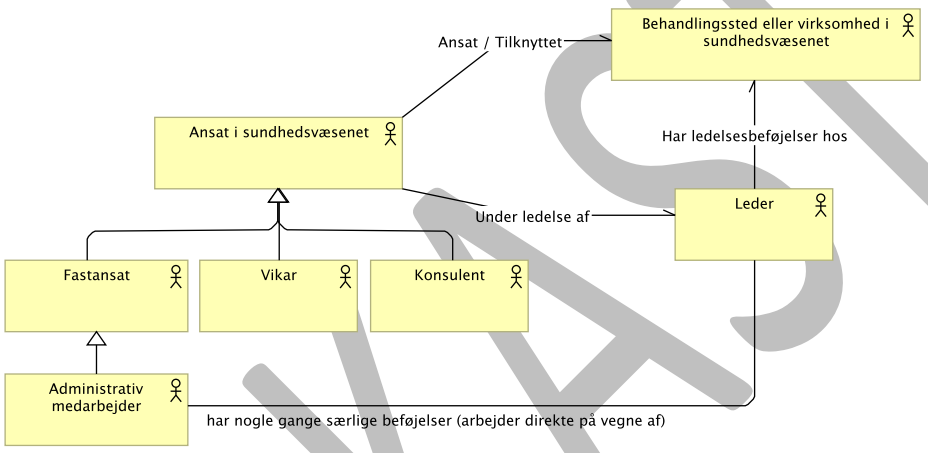
### 1.4.4 Ansættelse, ansatte og ledelse

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 sundhedsprofessionelle (sundhedsfaglige, der arbejder på et behandlingssted), men

[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.

også 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 'sundhedsfaglig'.

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, da henvendelses identifikation altid vil 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 myndigheders ansatte.

### 1.4.7 Centrale aktører (udgår)



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

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

# 2. Strategisk

## 2.1 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/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 201X'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 3.1 '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.

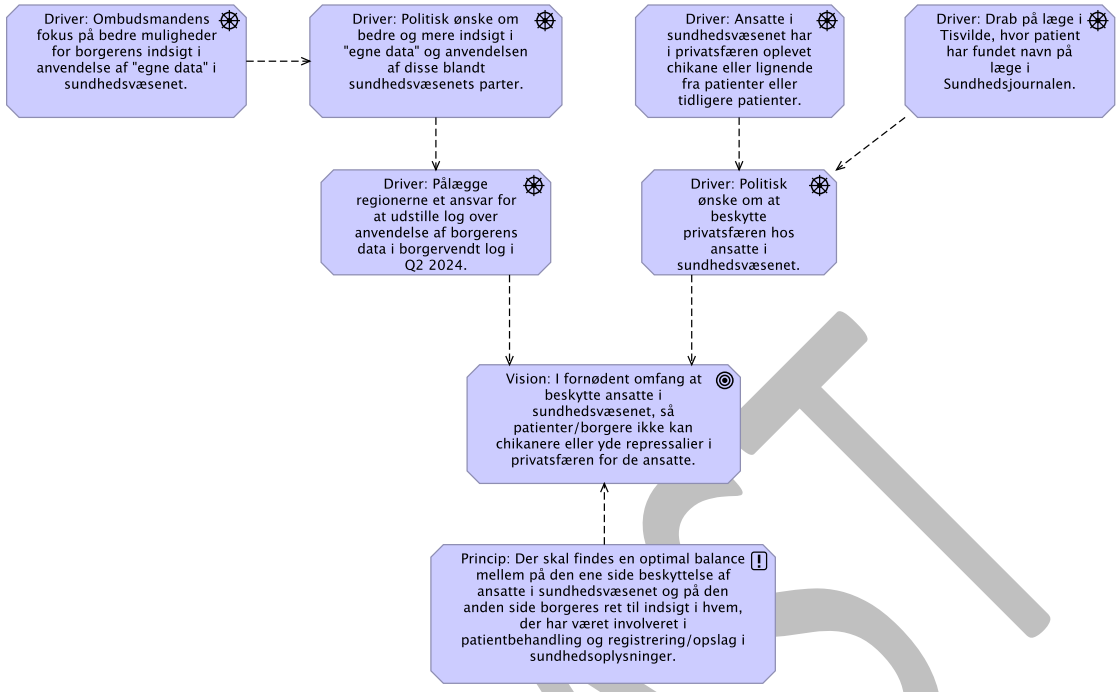
På den anden side, er der eksempler på, at udstilling af de ansattes navne i offentlige digitale løsninger kan bruges til at finde frem til privatadresse og andre oplysninger om de ansatte i sundhedsvæsenet. Under efterforskningen af drabet[8] på en læge i Tisvilde i 2019 blev der fundet udskrifter fra 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 identitetssløring.

## 2.2 Interessenter og interesser (udgår)

Dækkes af User Stories (se Appendiks B – User Stories)

## 2.3 Vision

Visionen med arbejdet er følgende:

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

Med 'i fornødent omfang' indarbejdes ovennævnte princip om, at den almindelige borgers ret til indsigt i navne på de ansatte, der har haft adgang til patientens helbredsoplysninger, ikke skal fratages borgere i almindelighed.

## 2.4 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.

## 2.5 Kvaliteter (udgår)

## 2.6 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.

- **Princip 1:** Der skal skelnes mellem administration af sløringsbehov (sløringsregistreringen), og hvordan der teknisk sløres (pseudonymiseringsteknik). Det betyder, at de to dele er uafhængige og kan udvikles selvstændigt.
- **Princip 2:** Der skal alene sløres i borgervendte visninger f.eks. Sundhedsjournalen (borgerdelen), MinLog (borgerdelen), FMK-online (borgerdelen), Medicinkort appen etc. Sløringsfunktionalitet skal kunne indgå i alle relevante nuværende og kommende borgervendte løsninger.
  Pseudonymer skal ikke registreres i kilderegistre. Identiteter skal udskiftes med pseudonymer, når det er nødvendigt i de borgervendte visninger. De rigtige identiteter skal altid fremgå i visninger for sundhedsfaglige (se 4.4.1 Forretningsproces for sløring).
- **Princip 3:** Formålet med den nationale sløringsservice er et nationalt register, der alene gør det muligt at kommunikere behov for sløringer mellem den registrerende part og andre services, der skal kunne effektuere sløringen af den registrerende parts medarbejdere.

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

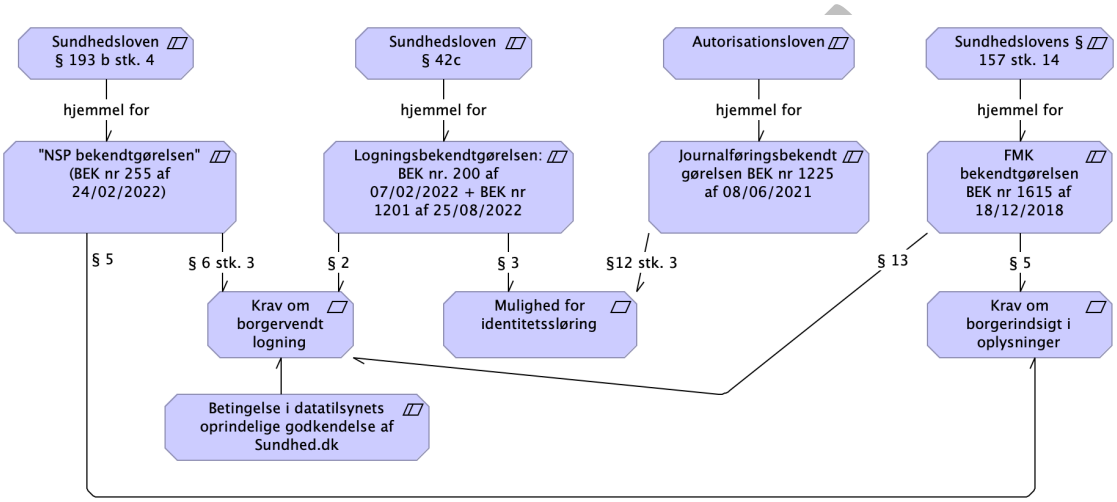
[11] Arkitekturprincipper for Sundhedsområdet. https://sundhedsdatastyrelsen.dk/-/media/sds/filer/rammer-og-retningslinjer/referenceaktitektur-og-it-standarder/arkitekturprincipper_version-2,-d-,0.pdf?la=da

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

- **Princip 4:** En ledelses beslutning om sløring ift. medarbejdere kan ikke give anledning til sløring af medarbejdere ansat i andre CVR-enheder. I regional sammenhæng betyder det, at en registrering om sløring fra en afdeling i Region X vil beskytte alle der er under ledelse af Region X, men ikke medarbejdere i Region Y eller kommunerne etc.).
- **Princip 5:** Ledelsens beslutning om sløring er knyttet til ledelsesret og arbejdsmiljøloven. Det betyder, at sløring gælder alle ansatte, der er under ledelse af den pågældende organisation inkl. vikarer, konsulenter mv.
- **Princip 6**: Det administrative arbejde ved en sløring, dvs. de processer/arbejdsgange, der skal til for at foretage registreringen, tilrettelægges af de enkelte parter.

# 3. Lovgivning

Målbilledet omhandler visning af person-identiteter (ansatte) i borgevendte løsninger. Nedenfor redegøres for de love og bekendtgørelser, der kræver at disse identiteter registreres i journaler og logs. Der er forskellige krav til forskellige løsninger, og dataansvaret ligger ikke hos den samme aktør i de respektive bekendtgørelser. 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.

Overordnet kan det konkluderes, at der er hjemmel til mulighed for identitetssløring i Logningsbekendtgørelsen og Journalføringsbekendtgørelsen, men ikke i FMK- og "NSP"-bekendtgørelsen. Som lovarbejdet pt. er udformet, er det derfor tilladt at identitetssløre i MinLog visninger og i E-journal/Sundhedsjournal borgervisningen, men reelt ikke i andre nationale løsninger herunder FMK-Online og de borgervendte løsninger til "Et samlet patientoverblik".

## 3.1 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 2022 blev denne hjemmel brugt til 'logningsbekendtgørelsen', BEK nr. 200 af 07/02/2022[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, der foretog opslaget. Desuden skal behandlingssted og tidspunkt udstilles. Der stilles krav om at oplysningerne skal fremstilles i en overskuelig og letforståelig oversigt.

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

[14] https://www.retsinformation.dk/eli/lta/2022/200

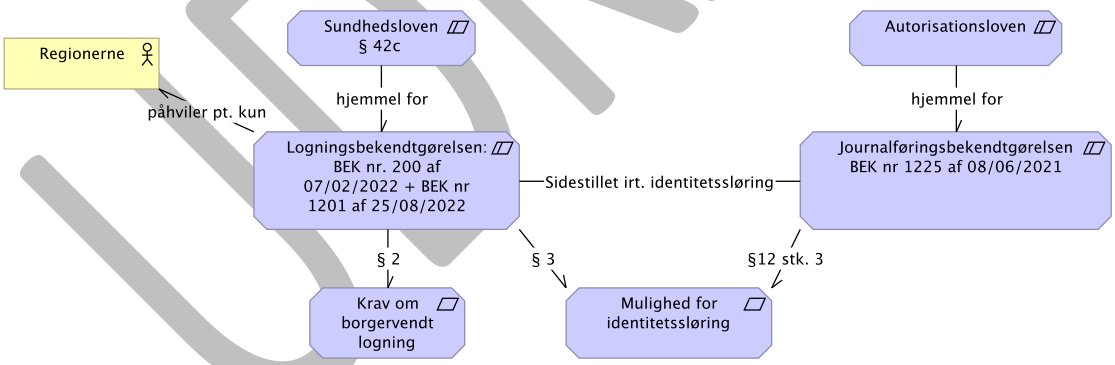
I bekendtgørelsens § 3 kan regionsrådet i den enkelte region beslutte, at patienten i stedet for fornavn og efternavn får adgang til oplysninger om 'anden entydig identifikation' på den person, der har foretaget et opslag.

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, hvor længe den gælder, og hvilken rækkevidde en sløring har. Dog 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 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/opslag i sundhedsoplysninger.

Desuden 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 sundhedsfaglige kan optræde med anden identitet end navn i journaler (eller i borgervendt visning af journaldata).




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

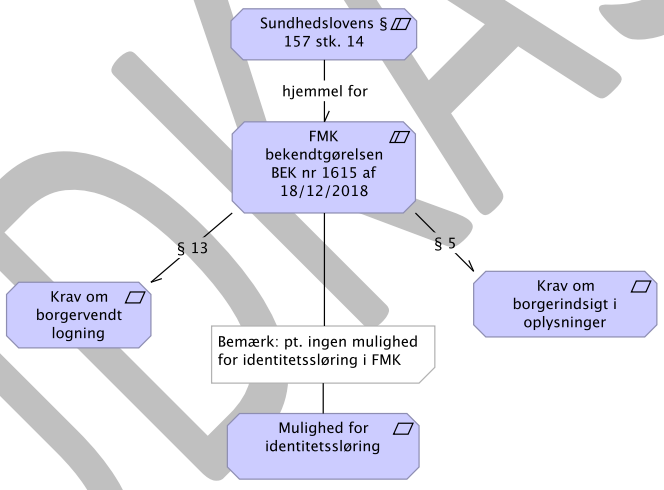
[15] https://www.ft.dk/samling/20211/beslutningsforslag/b35/index.htm

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

## 3.2 FMK-bekendtgørelsen

Fælles Medicin Kort (FMK[17]), der giver borgere og sundhedsprofessionelle 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. 1615 af 18/12/2018[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 sundhedspersonen har et sådant*". Der er ikke i den nuværende udgave af FMK-bekendtgørelsen mulighed for at optræde med anden identitet end navn, og der specificeres ikke nærmere, hvilke oplysninger der som udgangspunkt skal vises i den borgervendte visning på Sundhed.dk.

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). Heller ikke her er der pt. mulighed for identitetssløring.




Figur 10: FMK-bekendtgørelsen stiller krav om borgervendt logning og borgervendt visning. Der er pt. ingen muligheder for identitetssløring i FMK lovarbejdet.



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

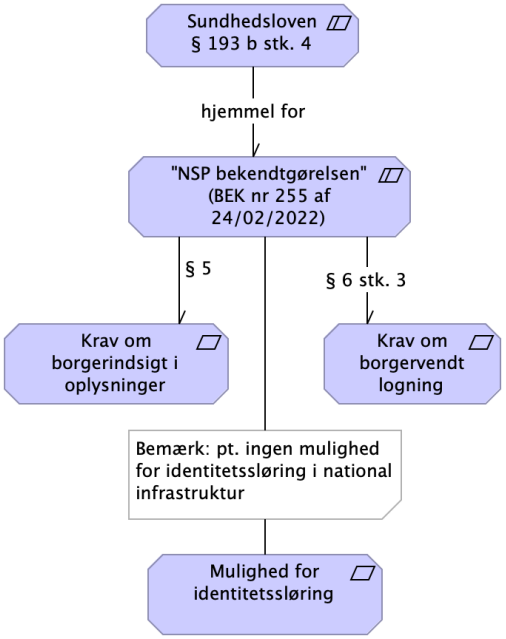
[18] https://www.retsinformation.dk/eli/lta/2018/1615

## 3.3 Bekendtgørelse om drift mv. af den fælles digitale infrastruktur ("NSP bekendtgørelsen")

BEK nr. 255 af 24/02/2022[19] (med hjemmel i Sundhedslovens § 193b) forpligter i § 6 SDS til at logge alle 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.

Der er ikke i den nuværende udgave af NSP-bekendtgørelsen mulighed for at ansatte i sundhedsvæsenet kan optræde med anden identifikation end navn.




Figur 11: "NSP-bekendtgørelsen" stiller krav om både borgerindsigt i oplysninger og borgervendt logning. I begge disse kræves der navn på ansatte, og der er pt. ingen muligheder for identitetssløring.

[19] https://www.retsinformation.dk/eli/lta/2022/255

# 4. Forretningsarkitektur

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

## 4.1 Forretningens krav (fra lovgivning)

Som det fremgår af kapitel 3 er der følgende forretningsmæssige krav til borgervendt logning, borgervendt visning af helbredsoplysninger og mulighed for identitetssløring:

- Regionerne skal jf. logningsbekendtgørelsen sikre at "*en patient, der er fyldt 15 år, i en periode på to år fra opslagstidspunktet får adgang til en overskuelig og letforståelig oversigt over oplysninger om fornavn, efternavn og titel på den, der har foretaget opslag i patientens elektroniske patientjournal, behandlingssted, hvorfra opslaget er foretaget, og tidspunkt for opslaget*".
- I relation til foregående punkt: "*Regionsrådet kan beslutte, 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.*"
- FMK skal udstille en borgervendt visning af borgerens medicinoplysninger, herunder navn på sundhedsfaglige, der har deltaget i medicinhåndteringen.
- FMK skal udstille en borgervendt log, der viser hvilke ansatte i sundhedsvæsenet, der har haft adgang til FMK hvornår.
- Forretningstjenester i "den nationale infrastruktur" (tjenesterne i "et samlet patientoverblik", graviditetsmappen, national PRO tjeneste og 'høremappen') skal ligeledes udstille borgervendt tjeneste til visning af helbredsoplysninger og borgervendt log.
- Parterne på sundhedsområdet skal føre journal over behandling af patienten i det danske sundhedsvæsen. I journalen (eller i visning af journaldata for borgeren) *kan* de ansatte optræde under pseudonym.

## 4.2 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 – i kontekst af identitetssløring – de forskellige aktører forventes at opleve, når de har kontakt med patienter/borgere i det danske sundhedsvæsen. 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 skal være muligt at henvende sig til behandlingsstedet for at få oplyst identiteten bag et pseudonym, og at der skal være klagemuligheder, hvis borgeren mener, at der er sløret uretmæssigt.

### 4.2.1 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 – skal jeg 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.

### 4.2.2 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.

### 4.2.3 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.

## 4.3 Centrale forretningsobjekter (udgår)

## 4.4 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, der søger indsigt i en ansats pseudonym.

### 4.4.1 Forretningsproces for sløring

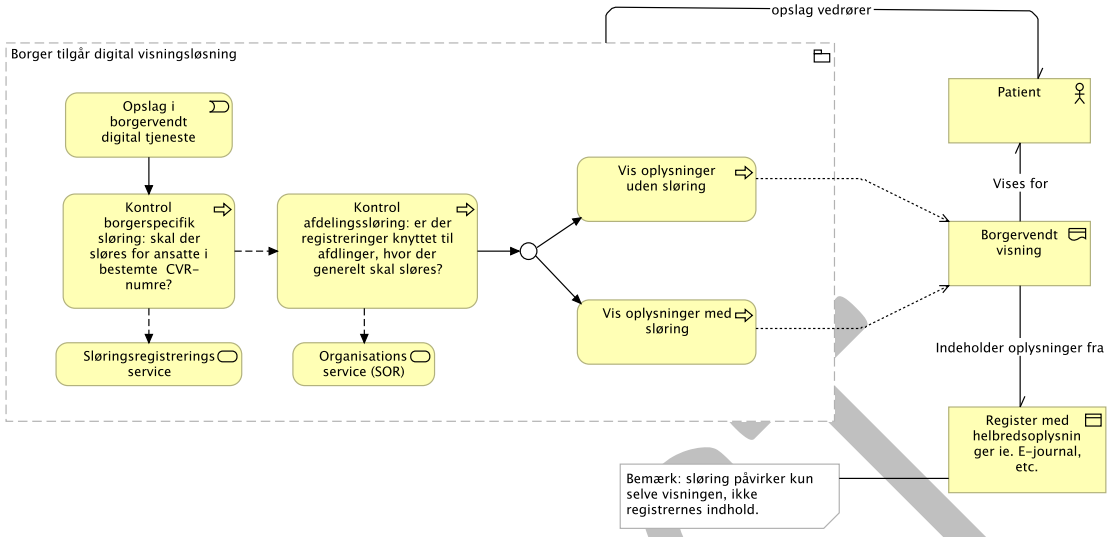
Når en borger tilgår en digital tjeneste som e-journal[20] eller FMK, vil den borgervendte løsning fremover kontrollere, om de medarbejdere, der fremgår i visningen, skal sløres. Det kontrolleres ved at anvende en sløringsregisterservice. Hvis en sløringsregistrering eksisterer, skal borgervisningen udskifte fornavn/efternavn med et pseudonym for de medarbejdere, der arbejder for den organisation, 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 bemyndiget vil en sløring overfor barnet også slå igennem for forælderen/værgen.

**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 sundhedsfaglige stadig kunne se den rigtige identitet, selvom der sløres for borgeren.



[20] Det antages, at der skabes hjemmel til sløring i andre tjenester end borgervendt logning. Dette arbejde er i skrivende stund i gang (september 2023).

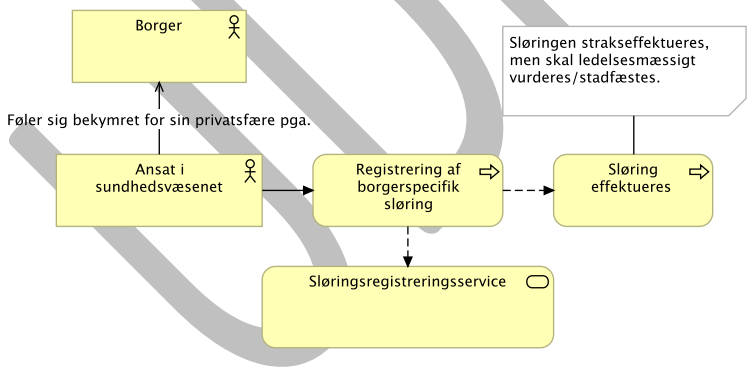



Figur 12: Forretningsproces for sløring i digitale borgervendte løsninger.

### 4.4.2 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 privat person 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 leder-repræsentant på behandlingsstedet (se næste afsnit).

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




Figur 13: Forretningsproces ved ansattes registrering af en (midlertidig) sløring.

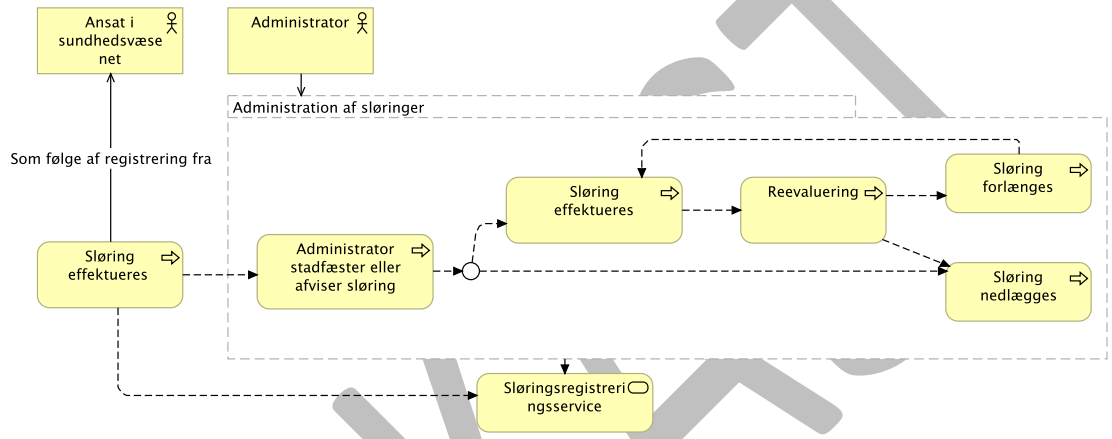
### 4.4.3 Forretningsproces for administration af borgerspecifikke sløringer

Administrationen af en sløring følger et typisk forløb, hvor en sløring kan skifte status (fra ikke-stadfæstet til stadfæstet), kan nå reevalueringsdato, 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.

Den registrerede sløring skal behandles hurtigst muligt af en administrator/leder, så den enten kan blive stadfæstet eller afvist (nedlagt). En sløring vil af forsigtighedshensyn altid være aktiv indtil den eksplicit nedlægges (uanset stadfæstelsesstatus/evalueringsstatus). Fra sløringen når (re)evalueringsdatoen, skal forlængelsen/nedlæggelsen ske hurtigst muligt.

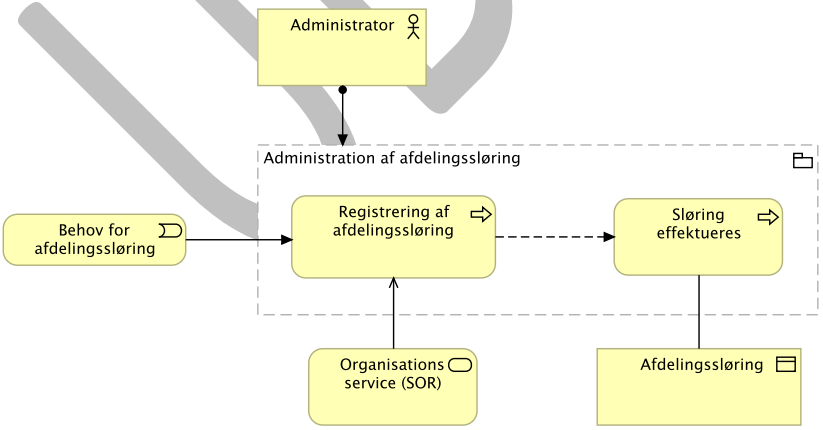
**Bemærk:** Det er op til den registrerende part at have processer og arbejdsgange, der sikrer rettidig stadfæstelse og re-evaluering. Den nationale service har ingen viden om status, kun om udløbstidspunkt.




Figur 14: Administrativ livscyklus for sløringer.

### 4.4.1 Forretningsproces for registrering af en afdelingssløring

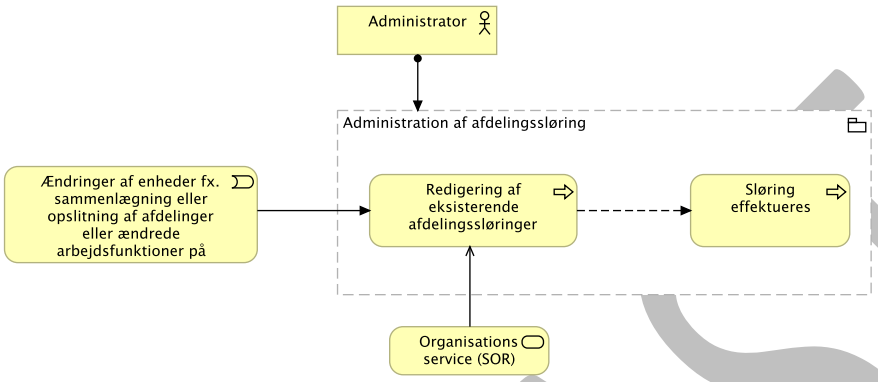
Når en administrator registrerer en afdelingssløring, effektueres den øjeblikkeligt. I modsætning til borgerspecifikke sløringer, har afdelingssløringer som udgangspunkt ikke en udløbsdato.




Figur 15: Registrering af en afdelingssløring. Afdelinger angives i SOR klassifikationen, og det kontrolleres, at den angivne SOR-enhed findes ved oprettelse.

### 4.4.2 Forretningsprocessen for administration af afdelingssløring

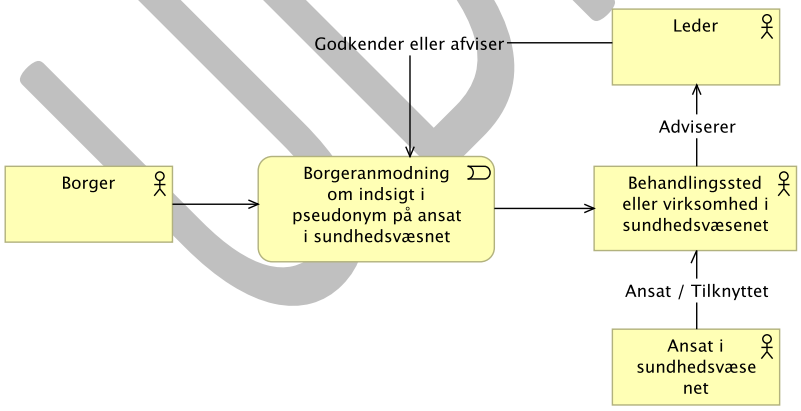
Administrationen af en afdelingssløring effektueres med det samme, og kan kun foretages af en administrator. En ændring affødes typisk af ændringer i enheder, som medfører ændringer i SOR-hierarkiet. Det kunne eksempelvis være ved sammenlægning eller opsplitning af afdelinger.




Figur 16: Administration af en afdelingssløring.

### 4.4.3 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 17: Forretningsproces for borgerhenvendelse ift. udlevering af den rigtige identitet bag et pseudonym.

**Bemærk:** 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. Se mere om aktindsigt i afsnit 1.4.6.

### 4.4.4 Forretningsregler for sløring af relaterede personer

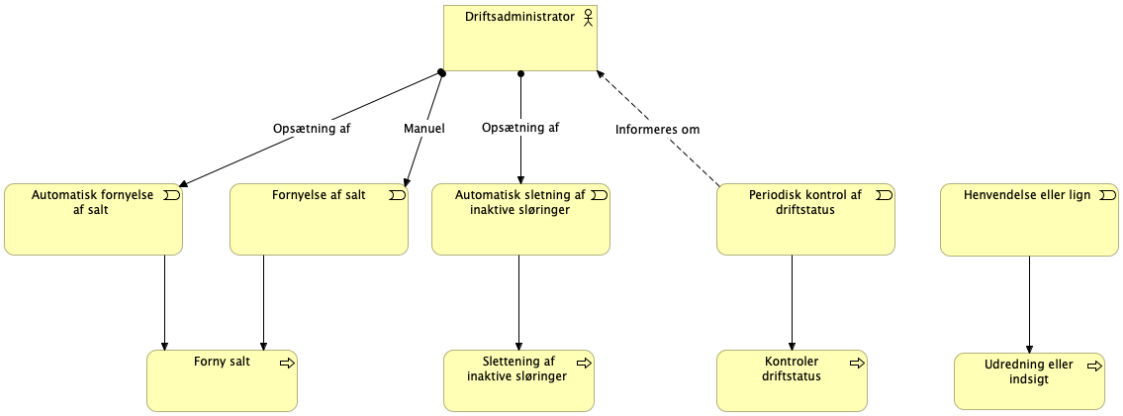
Hvis en nærtstående, f.eks. en forælder eller en værge har optrådt truende eller på anden vis skaber utryghed for en ansat i sundhedsvæsenet, kan den ansatte registrere en sløring overfor vedkommende. Hvis forælderen eller værgen herefter tilgår log- eller journaloplysninger, uanset om det er egne eller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

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

### 4.4.5 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.
- Sikkerhedselementerne skal også ved behov kunne fornyes manuelt
- Inaktive sløringer slettes fra servicen automatisk
- Selve servicen sløringsregistreringsservicen skal være tilgængelige 24/7 og derfor får administrator en alarm hvis servicen ikke er tilgængelig.




Figur 18: Forretningsprocesser for vedligehold for driftsadministrator samt andre henvendelser.

## 4.5 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 2 år. Ved reevaluering af en borgerspecifik sløring kan denne for hver evaluering forlænges i op til 2 år.<br><br>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 den borgervendte præsentation (digitalt eller analogt). |
| **BSS-5** | Ingen sletning ved dødsfald. | Såfremt en borger dør, skal der ikke aktivt slettes data i registret. Data slettes automatisk jf. forretningsregel **Ø-2** nedenfor. |
| **BSS-8** | 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-9** | Sløring for nærtstående. | Er der lagt sløring på en person gælder følgende ved andres adgang til dennes oplysninger:<br><br>Forældre: der skal sløres.<br><br>Værge: der skal sløres.<br><br>Bemyndiget: der skal sløres. |

| | | |
|---|---|---|
| **BSS-10** | Rækkevidde af sløringer, kun egen organisation. | En organisation kan kun oprette sløringer for egen organisation (CVR nummer). |

## 4.6 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.<br><br>Pseudonymer skal knyttes til den enkelte borger, så den samme ansatte optræder med forskellige pseudonymer overfor forskellige borgere.<br><br>Pseudonymer beregnes af visningsløsningerne, men skal være ens på tværs af løsninger.<br><br>Pseudonymer skal ikke være entydige over tid, men bør være entydige i visningsøjeblikket (på tværs af løsninger). |
| **Ø-2** | Opbevaring af logs i 5 år og opbevaring af registerdata i 5 år efter inaktivering. | Opsamlede log-data skal slettes 5 år efter logning.<br><br>Registrerede sløringsdata skal slettes 5 år efter in-aktivering (5 år efter slutgyldighedstidspunkt). |
| **Ø-3** | Elementer til sikring af pseudonymers entydighed og sikkerhed skal løbende fornys´. | For at sikre pseudonymet over tid, ændres elementerne løbende med et passende interval. Desuden er det muligt at aktivere manuel fornyelse, ved et tab af kontrol over det aktive salt. |
| **Ø-4** | Hjælp borgeren | Hvis der sløres identiteter overfor en borger, skal der – hvis der findes datagrundlag for det – vises informationer om arbejdsfunktion og rolle for den slørede medarbejder, samt ved logninger årsag til opslag. |

# 5. Informationsarkitektur

## 5.1 Informationsarkitektur for borgerspecifikke sløringer

En sløringsregistrering for en borgerspecifik sløring kan foretages af en hvilken som helst sundhedsansat, og påvirker borgervisningen af samtlige af de sundhedsansattes identiteter, der er ansat under det samme CVR-nummer som den registrerende part. Som følge af **Princip 1** i afsnit 2.6, skelnes der mellem den administrative del – sløringsregistreringen – og den tekniske sløring – pseudonymiseringen – som gennemgås i afsnit 5.3.

### 5.1.1 Information anvendt til en borgerspecifik sløring

Til en sløringsregistrering anvendes følgende information:

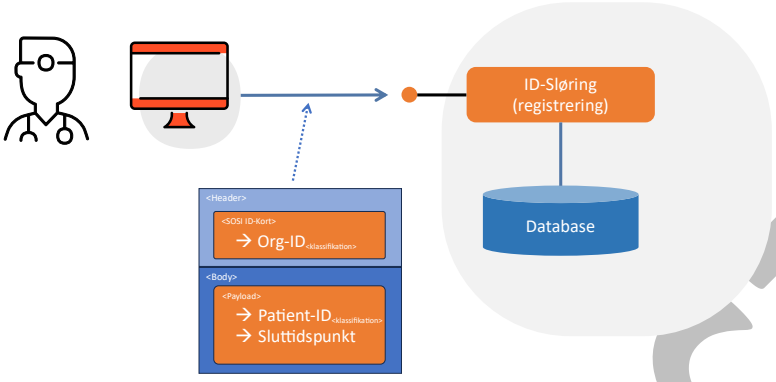
- Patient-ID (CPR, eCPR og på sigt evt. andre identifikationsklassifikationer)
- Organisations-ID (pt. CVR-nummer)
- Slutgyldighedstidspunkt

Borger identifikation 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 skal kontrolleres, når der er et autoritativt register til rådighed, her eksempelvis CPR eller eCPR registre. Hvis patient-ID'et ikke findes i det autoritative register, skal servicen fejle på en måde så den ansatte er klar over at sløringenregistrering ikke er sket.

Organisations-ID (CVR-nummeret) anvendes til at afgøre, hvilke ansatte der skal sløres. I første version af sløringsservicen vil organisations-ID'et være det CVR-nummer, der sendes med i SOSI ID-kortet (niveau 3 eller 4), når en ansat registrer sløringen. Da SOSI ID-kortet 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: det er kun whitelistede organisationer, der kan oprette sløringer (for egen organisation).

Slutgyldighedstidspunkt angiver den dato+tid hvor sløringen skal bortfalde. Det er et krav at registrere slutgyldighedstidspunkt, og slutgyldighedstidspunktet kan maksimalt være 2 år efter registreringstidspunktet. Skal sløringen opretholdes efter sluttidspunktet, skal sløringen genregistreres (se forretningsregel **BSS-3** i afsnit 4.5).

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 / eCPR.




Figur 19: Informationer der medsendes ved registrering af en sløring. Organisations-ID (CVR-nummeret) aflæses fra adgangsbilletten (SOSI ID-kort), patient-ID og sluttidspunkt medsendes som egentlige parametre.

### 5.1.2 Ændring af borgerspecifik sløringsregistrering

Når der registres en sløring, bruges sløringsadministrations-API'et (se afsnit 5.4.1) 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.

Afslutning/Sletning af sløringer sker ved at registrere en "ny" sløring for patienten med slutgyldighedstidspunkt til "nu". Sløringen vil reelt ikke være ny, men vil overskrive sluttidspunktet.

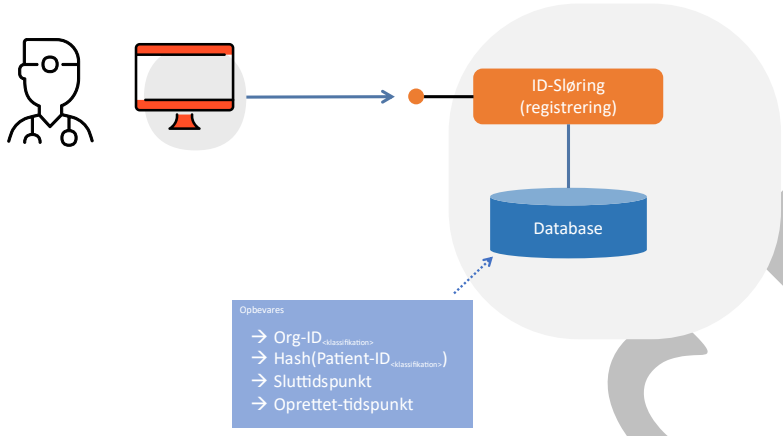
Tilsvarende for reevalueringer, der resulterer i en forlængelse af en sløring. Dette registreres også som en "ny" sløring med nyt slutgyldighedstidspunkt (maks. 2 år fra nyt registreringstidspunkt).

### 5.1.3 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 i den nationale NSP 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 relativt 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:

- 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 20: Oplysninger der opbevares per sløringsregistrering.

## 5.2 Informationsarkitektur for afdelingssløring

En afdelingssløring er som ovenfor nævnt en proaktiv sløring, der ikke er knyttet til den enkelte borger, men hvor det vurderes, at de ansatte med tilknytningen til afdelingen har behov for særlig beskyttelse. Afdelingssløring oprettes som ved at registrere et SOR-id[21] 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.

## 5.3 Pseudonymisering

Pseudonymisering af den sundhedsansatte sker på baggrund af en algoritme som alle borgervendte løsninger skal anvende. Pseudonymerne udregnes lokalt i den borgervendte løsning ved hjælp af UUIDv5. Pseudonymet udregnes på baggrund af tre inputs:

- Patient-ID/Borger-ID (typisk CPR)
- For- og efternavn på den sundhedsansatte
- Et tilfældigt "salt"

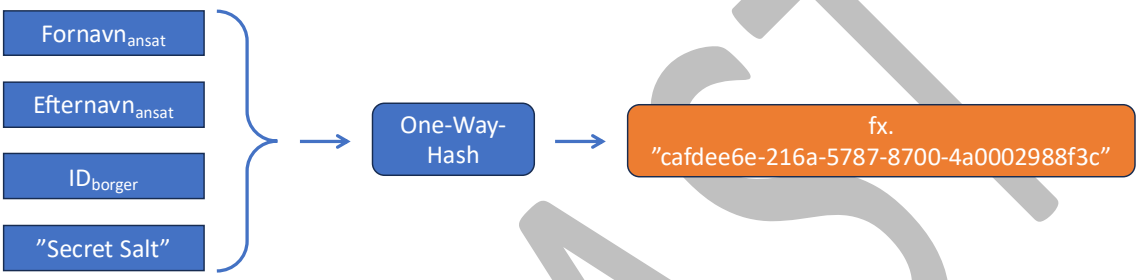
På den måde sikres det, at pseudonymet så vidt muligt er entydigt på tværs af løsninger. Derudover giver det borgeren mulighed for at sammenholde opslag i forskellige borgervendte løsninger på et givet opslagstidspunkt.

Borgerens ID (patient-ID) vil i langt de fleste tilfælde være et CPR-nummer, men der kan være tilfælde hvor andre vil være aktuelle. For- og efternavn på den sundhedsansatte er den laveste

[21] I den tekniske udformning vil det også i den første fase blive tilladt at registrere afdelinger i Sygehus- afdelingsklassifikationen (SHAK), men det forventes at denne mulighed senere vil bortfalde.

fælles nævner for den information, der fremgår på sundhedsansatte 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 sundhedsansattes identitet, så borgere ikke kan finde frem til den faktiske identitet ved at beregne pseudonymer for alle sundhedsfaglige ('brute force' beregning på lækket CPR-register med navne samt viden om algoritmen[22]).




Figur 21: Psedonymberegningsalgoritmen binder pseudonymer til borgeren og sikret med et "secret salt".

### 5.3.1 UUIDv5

UUID er en Universal Unique Identifier, der returnerer en 36-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. Denne egenskab anvendes til at sikre at alle parter beregner det samme pseudonym på tværs af løsninger, 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-namespaces, der per definition er 6ba7b812-9dad-11d1-80b4-00c04fd430c8.
- Tekststreng: "Fornavn+Efternavn+PatientID+'Secret Salt'"

"Secret Salt" gennemgås i afsnit 5.3.2.

For yderligere tekniske detaljer henvises til Guiden på NSP-hjemmesiden.

### 5.3.2 "Secret Salt"

Saltet er den tilfældige værdi, der medregnes i pseudonymet, og har til formål at øge beskyttelsen af den bagvedliggende information, altså den sundhedsansattes identitet. Saltets længde

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

har betydning for robustheden. Hvis saltet bliver for kort, kan det gættes (beregnes) hvis angriberen har adgang til blot få pseudonymer og viden om algoritmen. Hvis saltet bliver 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 periodisk udskiftes. 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 5.4.2 og 5.4.3.

Generelt er det i 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[23] 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.

## 5.4 Logiske snitflader

### 5.4.1 Sløringsadministrations-API

Sløringsadministrations API'et er det kald som foretages, når en sundhedsansat vil registrere en sløring. API'et har til formål at muliggøre, at:

- en sundhedsfaglig 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. Hvis der findes et autoritativt register for ID'et (f.eks. CPR / eCPR) skal der kontrolleres at ID'et findes i registret. og fejles, hvis der ikke gør. Der medsendes også det tidspunkt, der skal være slutgyldighedsdatoen for registreringen. Denne kan fejle hvis datoen angives i forkert format.

For afdelingssløringer vil der være følgende API:

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

**createOrgBlurring(orgID, orgClassification) —> id**

Opretter en ny afdelingssløring.

**listOrgBlurringsForCVR() —> {orgID, orgClassification}***

Returnerer listen af registrerede afdelinger hørende til CVR-nummeret (fra SOSI ID-kortet)

**listAllActiveOrgBlurrings() —> {orgID, orgClassification}***

Returnerer listen af aktive afdelingssløringer (skal anvendes i effektueringssammenhæng)

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

Inaktiverer en afdelingssløring.

### 5.4.2 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 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 den angivne PatientID.

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 6.3.3 for uddybende information.

### 5.4.3 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 SOR-enheder, der (altid) skal sløres for, kan rekvireres 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.

### 5.4.4 Salt-API'et

Salt API'et skal bruges af modtagerne af IDWS tokens (f.eks. MinLog servicen), forud for beregning af pseudonymer. API'et består af en enkelt funktion, der returneret de 16 bytes der udgør saltet.

getCurrentSalt() → [byte]

### 5.4.5 Driftsadministrations API

API´et har flere funktioner som driftspersonaltet 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 af i 5 år efter udløbsdato af hensyn til sporbarhed og support. Herefter slettes sløringsregistreringen, så databasen ikke fyldes op med irrelevante sløringer. Dertil anvendes driftsservicen:

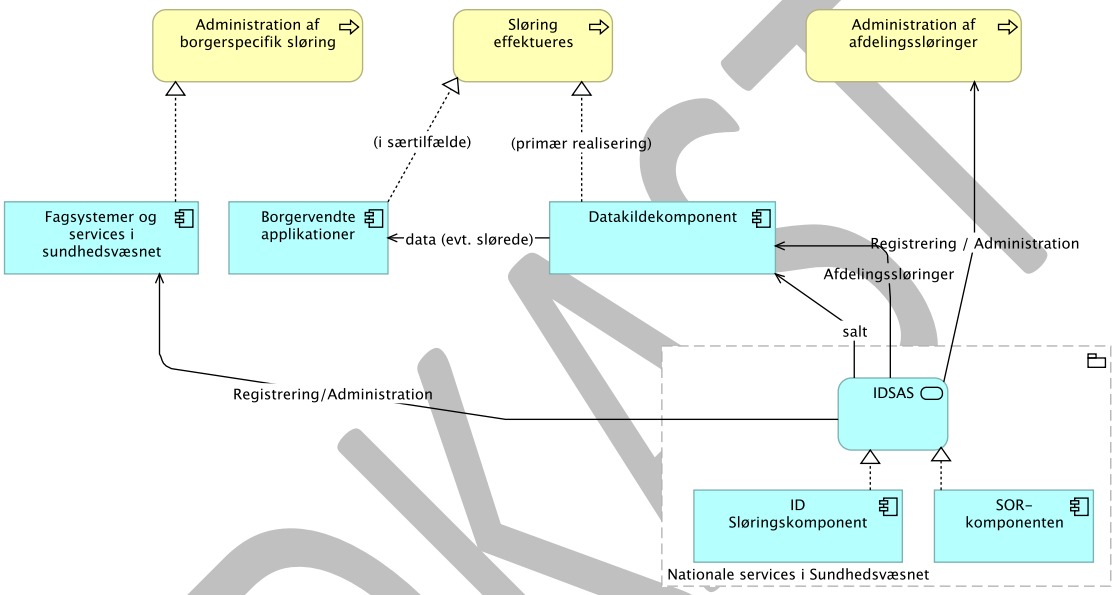
Cleanup-blurrings()

For at driftsadministratorerne kan sikre sig at ID-sløringsservicen er kørerne som forventet, er der udviklet en statusrapporteringservice som meddeler, hvis der er ændringer til status for servicen denne service kaldes, "HealthServlet". Hvis der meldes fejl, vil en driftsadministrator blive notificeret og vil kunne rapportere et incident og at genoprette servicen.

# 6. Applikations- og infrastrukturarkitektur

## 6.1 Applikationer og services vist i komponenter

Applikationsmæssigt realiseres administration af borgerspecifikke sløringer (forventeligt) i de registrerende parters fagsystemer. Sløringer effektueres gennem pseudonymisering i datakilderne[24] til de borgervendte løsninger, men kan i særtilfælde effektueres i de enkelte borgervendte applikationer.



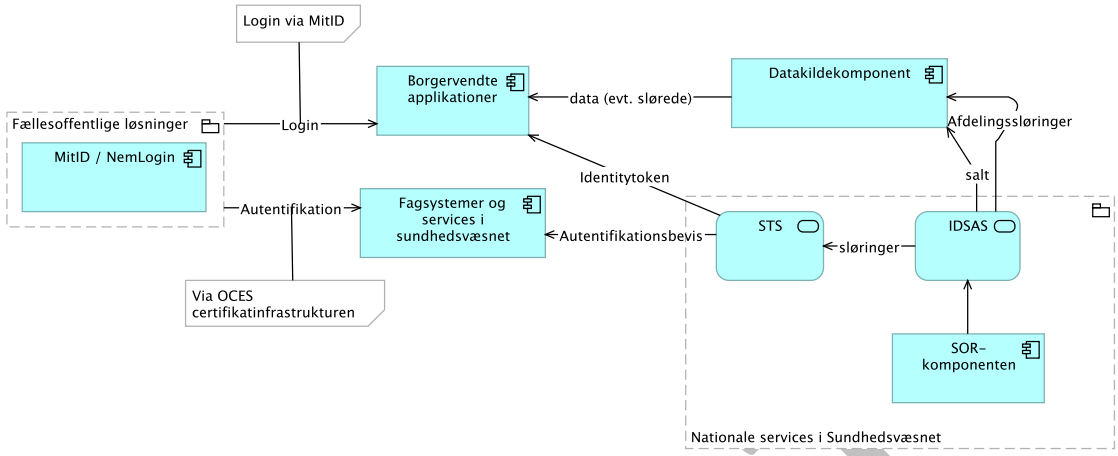

Figur 22: Overordnet komponentunderstøttelse af de væsentligste forretningsprocesser.

## 6.2 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 (OCES) i relation til sikker identifikation af bruger 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.

[24] 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 23 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 sundhedsfagliges 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. Sløringsservicen udstilles som en national service, med forventningen om, at flere parter vil få brug for at anvende den i fremtiden.

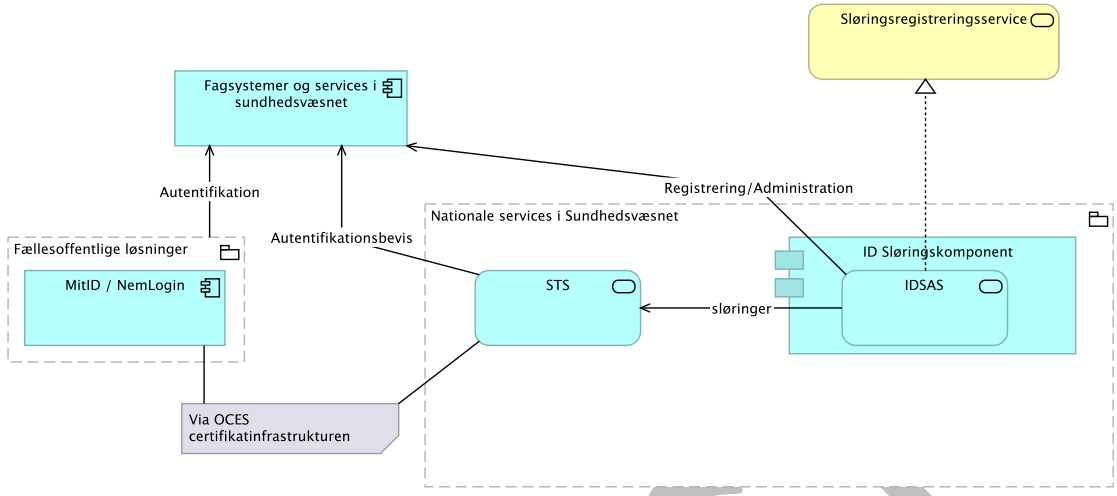
## 6.3 Applikationsflows

### 6.3.1 Administration af borgerspecifikke sløringer

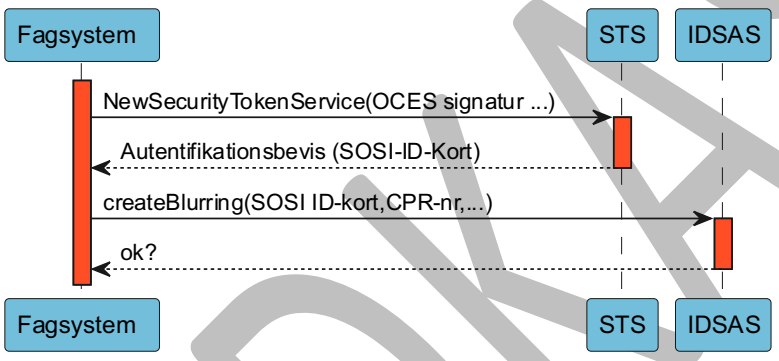
Det logiske forretningsflow for dette gennemgås i afsnit 4.4, men det konkrete applikationsflow er noget anderledes, især som følge af sikkerhedshåndtering.

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*. Den logiske snitflade er uddybet i afsnit 5.4.1.




Figur 24: Applikationssammenhæng for registrering og administration af borgerspecifikke sløringer.




Figur 25: Simpelt flow for registrering/administration af borgerspecifikke sløringer.

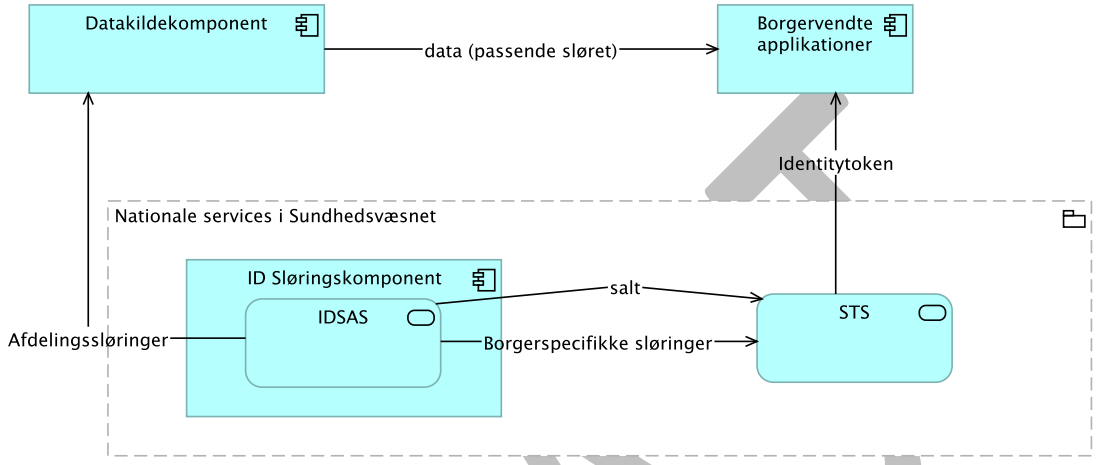
### 6.3.2 Effektueret sløring: borgervisning

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.

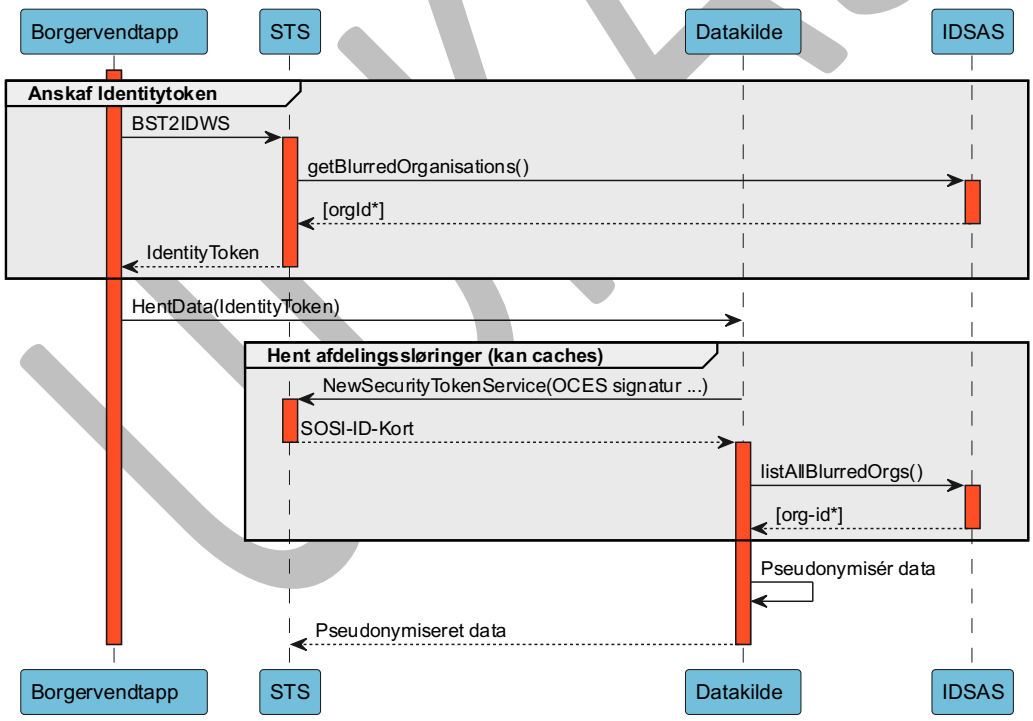
Før en OIOIDWS service kan kaldes skal der derfor fremskaffes et identitytoken. Det rekvireres hos STS'en på NSP, hvor den borgervendte løsning "veksler" et bootstrap token (der blev udstedt da borgeren oprindeligt loggede ind) til et identitytoken. STS'en vil bruge IDSAS komponenten (*GetBlurredOrganisations)* 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, indgår. Datakildeservicen skal selv producere pseudonymer, og dertil skal den bruge

det "salt" som kommer med adgangsbilletten. IDSAS-komponenten udstiller[25]. Endvidere skal datakildeservicen kende de organisations-koder som der skal afdelingsløres for. De rekvireres (periodisk) hos IDSAS-komponenten. Denne liste forventes at være relativt stabil, og kan evt. caches. Figur 26 illustrerer forskellige anvenderes adgang til IDSAS-komponenten.




Figur 26: Applikationssammenhæng for effektuering af sløring




Figur 27: Flow for effektuering af sløring inkl. rekvirering af Identitytoken

[25] Indbygges evt. senere i identity-tokenet.

### 6.3.3 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 sundhedsfagliges 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.

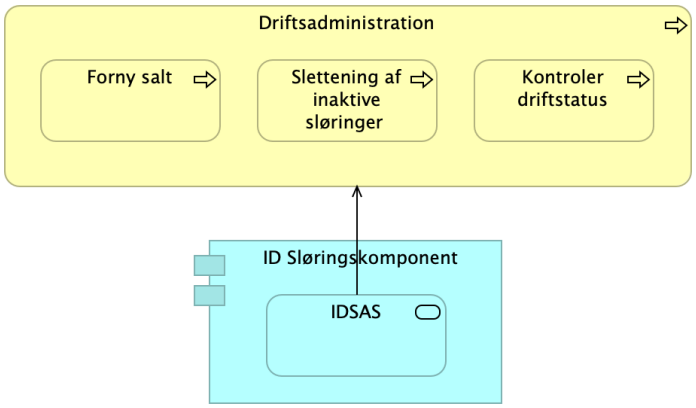
Når IDSAS-komponenten efterfølgende er reetableret vil STS´en igen udstede billetter med målrettede sløringsinformationer.

### 6.3.4 Driftadministration

Driftsadministrationen består af tre dele:

- Fornyelsen af salt, det forventes at dette udføres ca. hver 30 dag
- Check om sløringsservicen er tilgængelig, og alarmere administrator hvis der er problemer
- Oprydning af inaktive (udløbne) sløringer, det forventes at jobbet startes en gang om ugen

Det er ID sløringskomponenten der understøtter driftsadministrationen med de tre API'er der gennemgås i 5.4.5.




Figur 28 Applikationsunderstøttelse af drifts administration

# 7. Sikkerhed

Målbilledet for national ID-sløring omhandler udpegningen af individer, der overfor sundhedspersoner har optrådt truende, chikanerende eller på anden måde upassende. Disse individer fratages midlertidigt rettigheden til at se ellers tilgængelige informationer om hvem, der deltaget i behandlingen, i digitale løsninger. Borgeren har dog stadig mulighed for at henvende sig til behandlingsstedet for at søge om indsigt. Borgeren har også stadig ret til aktindsigt.

Oplysninger om hvem der er frataget disse rettigheder, er i sig selv ret følsomme. Det udtaler sig nemlig om personens karakter, og denne viden kan misbruges og fejlanvendes. Behovet for ekstra sikkerhed afspejles i udformningen af den tekniske løsning, hvor det blandt andet kun er 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 sundhedsfaglige (hvor det jo er de sundhedsfaglige 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.

## 7.1 Logning

Normalvis anvendes MinLog på NSP til at registrere og opbevare registrering af adgang til borgens data. Borgeren kan på denne måde følge op på, hvilke sundhedspersoner der har haft adgang til borgerens helbredsoplysninger, og hvornår. En sløringsregistrering skal *ikke*[26] registreres i MinLog, da det ikke ønskes at der gives eksplicit information til borgeren om, at en sundhedsfaglig har registreret en sløring. Herudover må informationen om en oprettet sløring anses for ikke at være helbredsoplysninger, og derfor ikke skulle registreres i MinLog.

## 7.2 Autenticitet, Tilgængelighed, Integritet, Uafviselighed og Fortrolighed

Den generelle diskussion af sikkerhed tager udgangspunkt i referencearkitekturen for informationssikkerhed på sundhedsområdet[27]. Heri opereres med følgende fem dimensioner ved sikkerhed:

[26] MinLog er borgervendt logning. Der sker forskellige andre tekniske logninger, af hensyn til sporbarhed, support mv.

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

| 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. |
| 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:

- Anvendere af sløringsregistreringsservicen kan kun fås med et gyldigt DGWS-adgangsbillet (SOSI ID-kort), som udstedes på baggrund af autentifikation med de fællesoffentlige loginmidler hos MitID / OCES. Derudover kan kun systemer der er whitelistet til IDSAS på NSP'en anvendes til at registrere en sløring. Servicen sikrer, at der kun kan sløres inden for det CVR-nummer, som det kaldende sytem eller den kaldende bruger (sundhedsfaglige) kommer fra.
  Borgere autentificeres med privat MitID

Kun driftsadministratorer kan få direkte adgang til 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.

**Tilgængelighed**

For at servicen er tilgængelig skal følgende være etableret:

- En sundhedsdatanetaftale og tilsvarende tilslutning
- En NSP serviceaftale
- Den organisation som skal kalde sløringsservicens CVR-nummer whitelistes, så det kun kan kaldes af en whitelistet organisation.
- Selve servicen skal være tilgængelig ("oppe").

Er disse etableret, 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. I forhold til sikring imod ondsindede cyber-angreb, skal der jf. strategien for cyber- og informationssikkerhed i sundhedssektoren[28] afholdes regelmæssige sikkerhedsaudits for at forudse disse, og der skal etableres passende høj beskyttelse af de centrale komponenter for at forebygge angreb mod dem. Endvidere skal der være effektiv overvågning, så cyber-angreb opdages hurtigt, og der skal være klare velafprøvede processer og procedurer for en hurtig reetablering af driften for at håndtere angreb.

Endelig er der i designet indarbejdet enkelte værn mod nedbrud som følge af afhængigheder. Et godt eksempel er at der bag registreringsservicen er et afkoblingspunkt, så et midlertidigt udfald i NSP netværksinfrastrukturen ikke medfører stop af registreringer i det kliniske led. Hvis IDSAS er utilgængelig vil STS'en ikke udstede IDWS biletter, og borgere kan derfor ikke tilgå de løsninger, der kræver STS-billetter.

**Integritet**

Integritet sikres gennem den anvendte infrastruktur. Ved at anvende et IDWS bootstrap token bindes informationen om organisationer der skal sløres overfor borgeren til den tjeneste, hvor sundhedspersoner skal sløres.

**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". Da dette ikke kan etableres i de første versioner, er det besluttet at opbevare borgernes ID'er (CPR-numre) som sikre hashes, så en tilfældig lækage ikke afslører de registreredes identitet.



[28] ] 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

# 8. Governance

Udgår af dette minimålbillede.

# 9. Fremtidige versioner af målbilledet (udgår)

# 10. Appendiks A – Begrebsliste

| Foretrukken term | Accepteret term | Definition | Evt. borgervendt forklaring/kommentar/kilde |
|---|---|---|---|
| Afdelingssløring | Generel sløring | En sløring af de ansattes identitet ved borgervisning af helbredsoplysninger fra udvalgte afdelinger/underenheder. Alle ansatte, der optræder i registreringer/logninger fra slørede afdelinger, sløres. | |
| Aktindsigt | | Adgang til at se dokumenter, der indgår i sagsbehandlingen hos en offentlig myndighed.<br>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, som har registreret en sløring. | |
| Behandlingssted | | Organisation med egen ledelse der udfører sundhedsfaglig behandling og foretager sundhedsfaglige optegnelser i et afgrænset informationssystem | NBS[29] |

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

| Foretrukken term | Accepteret term | Definition | Evt. borgervendt forklaring/kommentar/kilde |
|---|---|---|---|
| Borger | | Person der har pligter og rettigheder i forhold til en kommune, region eller stat | NBS |
| Borgerspecifik sløring | Specifikke sløringer | En sløring knyttet til en specifik borger, der eks. har udvist truende adfærd eller lignende overfor sundhedsfaglige. | |
| Identitetssløring | | Identitetssløring er den generelle betegnelse for sløringen af sundhedsansattes identitet. Der findes to måder, hvorpå en identitetssløring kan ske: ved en afdelingssløring og ved en borgerspecifik sløring. | |
| Pseudonym | | Påtaget identifikation, se "Anden entydig identifikation". | |
| Sløringsregistrering | | En registrering af en sløring. | |
| Sundhedsprofessionel | | Sundhedsaktør der er tilknyttet en sundhedsproducerende enhed. | NBS |
| IDSAS | | Identitetssløring af ansatte i sundhedsvæsenet | |
| STS | | Sikkerhedsservices på NSP omfatter STS (Security Token Service) og Billetomveksling. | |
| NSP | | National service platform | |

# 11. 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 ved, at en patient ikke har adgang til information der henviser til mig/os som privatperson. |
| 2 | at kunne skjule min og mine kollegers identitet, hvis jeg føler mig truet/udsat, af min patient … | … så jeg f.eks. kan henvende mig til rette vedkommende og forhøre mig om tidligere forløb. |
| 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 reevaluering … | … 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 føle 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 på 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 (se 1) … | … 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 lovmedholdelige … | … 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 jeg (og mine kolleger) ikke længere er sløret. |
| 18 | at kunne oprette en afdelingssløring (proaktiv sløring for bestemte afdelinger) ... | … så sundhedsfaglige der optræder i registreringer fra den type afdelinger automatisk bliver sløret. |
| 19 | at kunne kommunikere proaktive sløringer på en let forståelig måde ... | … så sundhedsfaglige kan føle sig trygge og så sundhedsfaglige ikke opretter unødige personspecifikke sløringer. |