BECH-BRUUN

Aarhus · Oktober 2018

Sagsnr. 062926-0007 mif/cbt/lpos
Dok.nr. 20051880.1

SUNDHEDSPLATFORMEN
Data Protection Impact Assessment (DPIA)

Opfølgende DPIA på baggrund af den oprindelige PIA fra 2016

Sundhedsplatformen
Lyngbyvej 20
2100 København Ø

Dato
1. oktober 2018

Version 1.0

De dataansvarlige

Navn	Region Hovedstaden
Adresse	Kongens Vænge 2, 3400 Hillerød
CVR-nummer	29190623

og

Navn	Region Sjælland
Adresse	Alléen 15, 4180 Sorø
CVR-nummer	29190658

Mellem Region Hovedstaden og Region Sjælland er der indgået en aftale om fælles dataansvar.

Ekstern bistand

Nærværende konsekvensanalyse vedrørende databeskyttelse (DPIA) udgør resultatet af et samarbejde mellem de dataansvarlige

og

Bech-Bruun
Værkmestergade 2
8000 Aarhus C

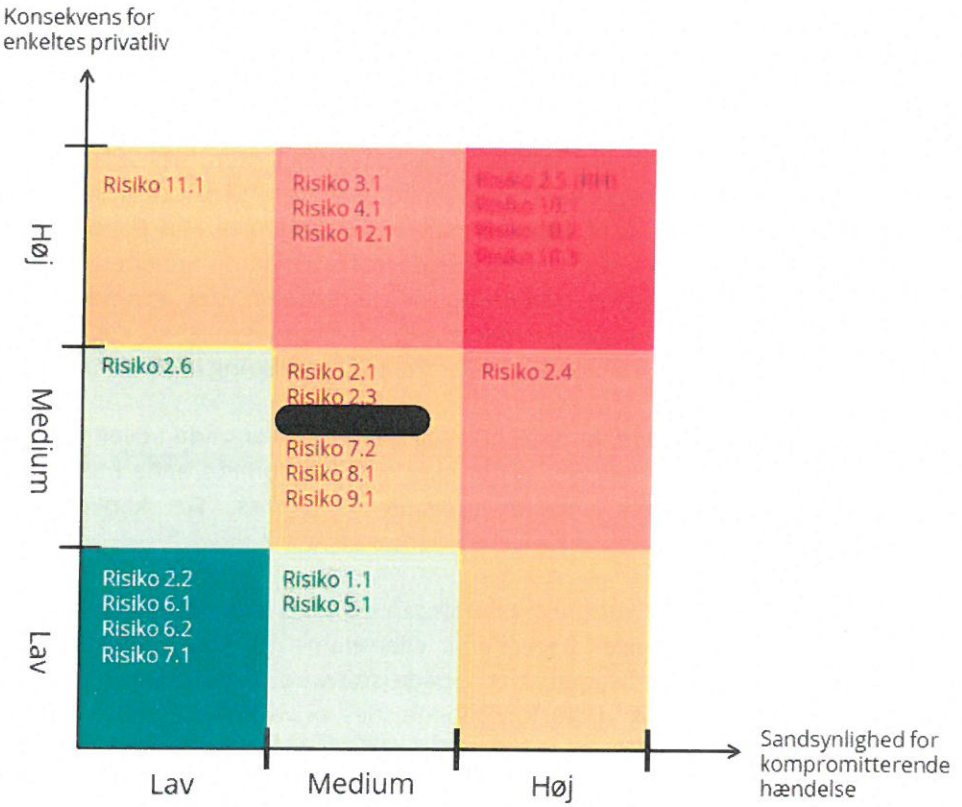
Indholdsfortegnelse

1. Sammenfatning ... 5
2. Introduktion ... 7
2.1 Baggrunden for denne konsekvensanalyse ... 8
2.2 Emnet for denne konsekvensanalyse ... 9
3. Processen for DPIA i relation til Sundhedsplatformen ... 10
3.1 Metode og terminologi ... 10
3.1.1 Metode ... 10
3.1.2 Terminologi ... 11
3.1.3 Risikotemaer og identificerede risici ... 11
3.1.4 De registreredes synspunkter ... 11
3.2 Gennemgåede dokumenter ... 12
4. Generel beskrivelse af Sundhedsplatformen og kortlægning af overordnede datastrømme ... 13
4.1 Generel beskrivelse af Sundhedsplatformen ... 13
4.1.1 Lovgivningen bag behandling af personoplysninger i Sundhedsplatformen ... 14
4.2 Kortlægning af overordnede behandlingsaktiviteter og datastrømme ... 15
5. Risikotemaer ... 17
5.1 Fordeling af dataansvar mellem Region Hovedstaden og Region Sjælland ... 17
5.2 Rettigheder og autorisationer ... 18
5.2.1 Tildeling af rettigheder og autorisationer ... 18
5.2.2 Break the Glass/Bump the Glass ... 19
5.2.3 Gennemgang af loggen ... 20
5.3 Konvertering af data fra eksisterende systemer til Sundhedsplatformen ... 25
5.4 Samtykke til yderligere behandling af patienternes personoplysninger i forbindelse med indlæggelse ... 28
5.5 Overførsel af oplysninger fra parakliniske systemer ... 29
5.6 Oversigtsskærme ... 29
5.7 Min Sundhedsplatform (patientportalen - MyChart) ... 30
5.8 Datastrømme i Sundhedsplatformen ... 31
5.9 Uddannelse ... 32
5.10 Fejlretning og support i EPIC ... 34
5.10.1 Sherlock ... 34
5.10.2 Ekstern adgang til Sundhedsplatformen ... 34
5.11 Opfølgning på fejlregistreringer i Sundhedsplatformen (datakvalitet) ... 37
5.12 Beskyttelse af ansattes personoplysninger (medarbejdervinklen) ... 38
6. Konsekvensanalyse (Impact Assessment) ... 39
6.1 Afvejning af risici ... 39
6.1.1 Grafisk illustration af risikoafvejningen ... 41
6.2 Prioritering af risici med størst risiko for krænkelse af privatlivet ... 43
7. Evaluering af risici og beskrivelse af foranstaltninger, der imødegår disse ... 44

8. Afsluttende bemærkninger 49
8.1 Accepteret residualrisiko/restrisiko 49
8.2 Offentliggørelse af konsekvensanalysen 49
8.3 Opfølgende DPIA 49

1. Sammenfatning

Bech-Bruun har i overensstemmelse med kravene i databeskyttelsesforordningens artikel 35, foretaget en konsekvensanalyse (DPIA – udtrykkene DPIA og konsekvensanalyse anvendes i flæng, se mere vedr. terminologi i afsnit 3.1.2) i forhold til behandlingen af personoplysninger i Sundhedsplatformen. Resultaterne af analysen kan sammenfattes i nedenstående risiko-matrix.



Der er særligt grund til at fremhæve en række konkrete risici fra analysen, som indebærer en høj risiko og dermed har en sandsynlig negativ påvirkning på behandlingen af personoplysninger i Sundhedsplatformen. Der findes en fuldstændig liste over risikotemaer og tilknyttede risici i afsnit 6

De største risici (det røde område) i relation til behandling af personoplysninger i Sundhedsplatformen er centreret omkring Region Hovedstadens gennemgang af

loggen via stikprøver samt EPIC's adgang til en fuld version af produktionsoplysninger fra Sundhedsplatformen i USA baseret på et vagt overførselsgrundlag, som skal konkretiseres yderligere i praksis.

Der er endvidere grund til at fremhæve en række forhold i figuren (det orange og gule område), som også indebærer risici i den "høje ende" i relation til behandling af personoplysninger. Risikoområderne med kombinationen høj/medium sandsynlighed og konsekvens drejer sig om uklarhed om den løbende gennemgang af rapporter vedr. funktionaliteten "Break the Glass", "gamle" IT-systemer der fortsat er i drift, indhentning af samtykke fra patienter og beskyttelse af personoplysninger om de ansatte, som benytter Sundhedsplatformen i forbindelse med deres arbejde. Området medium sandsynlighed kombineret med medium konsekvens indeholder den største samlede gruppe af risici. Det drejer sig om udvidelse/ændring af den oprindelige rettighedsmodel, som blev udarbejdet forud for "go live" i 2016, begrænsning af funktionaliteten "Break the Glass", Region Sjællands funktionalitet til loggennemgang, adgangen til Min Sundhedsplatform via apps, fastlæggelse af de overordnede datastrømme i Sundhedsplatformen samt behovet for yderligere uddannelse af de personer, der anvender Sundhedsplatformen. Endelig vedrører risikoområdet lav sandsynlighed kombineret med høj konsekvens manglende procedurer for kvalitetssikring af data (datakvalitet).

Alle risici i det røde, orange, gule og lysegrønne område i ovenstående figur skal mitigeres, så risikoen for at der sker en kompromitterende hændelse og konsekvensen for den enkeltes privatliv reduceres. De konkrete mitigationsanbefalinger kan ses af figuren nedenfor i afsnit 7.

Det anbefales, at Sundhedsplatformen endvidere indfører en proces, hvor det løbende sikres, at nye integrationer eller elementer i Sundhedsplatformen (fx nye applikationer og integrationer – både software og hardware), som sandsynligvis indebærer en høj risiko for patienternes privatlivsbeskyttelse, underlægges en selvstændig konsekvensanalyse. Da registrerede i Sundhedsplatformen primært udgør patienter, pårørende og brugere af Sundhedsplatformen, bør fremtidige konsekvensanalyser hver for sig målrettes de enkelte typer af registrerede.

Det anbefales endvidere i afsnit 8.3, at der senest i 2020 gennemføres en fornyet DPIA-proces med henblik på opfølgning af de i denne DPIA identificerede risici. Der bør senest 1. april 2019 kontrollere, at der er igangsat mitigering af de risici, som er identificeret i nærværende analyse.

2. Introduktion

En konsekvensanalyse vedrørende databeskyttelse (Data Protection Impact Assessment, DPIA) er kort fortalt en analyse af konsekvenser for privatlivet i forbindelse med behandling af personoplysninger og efterfølgende iværksættelse og kontrol af beskyttelsen af privatlivets fred.

Det overordnede formål med at gennemføre en DPIA er at identificere og mitigere risici ved behandling af personoplysninger på de områder, som analysen omfatter. Risici i relation til behandling af personoplysninger kan opstå fra mange forskellige både interne og eksterne kilder. En DPIA vedrører primært de konsekvenser, som kompromittering af personoplysninger kan have for de registrerede samt sandsynligheden for, at en sådan indtræder. En DPIA kan også omhandle de konsekvenser, som kompromitteringen kan have for den organisation, som analysen omfatter.

Ifølge databeskyttelsesforordningens artikel 35 er det et krav at gennemføre samt kunne dokumentere gennemførelse af en DPIA, når behandlingen af personoplysninger sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder på baggrund af behandlingens karakter, omfang, sammenhæng og formål. Det er i den forbindelse værd at bemærke, at det alene er et krav, at der skal være sandsynlighed for, at behandlingen indebærer en høj risiko – den høje risiko ved en given behandling behøver således ikke at være dokumenteret.

Det fremgår i den forbindelse af bestemmelsen, at gennemførelse af en DPIA navnlig er påkrævet i forbindelse med behandling af følsomme oplysninger (herunder helbredsoplysninger) i stort omfang. Det følger dog af databeskyttelsesforordningens præambelbetragtning nr. 91, at det ikke bør være obligatorisk at gennemføre en DPIA på alle områder, fordi de pågældende behandlinger ikke skal anses for omfattede. Præambelbetragtningen nævner bl.a. en læges eller sundhedspersonales behandling af personoplysninger om patienter. Dog følger det af Justitsministeriets betænkning om databeskyttelsesforordningen[1], at ordlyden i databeskyttelsesforordningens artikel 35, stk. 3, som ligger til grund for præambelbetragtning nr. 91, skal fortolkes indskrænkende, så det ikke er alle former for behandling af personoplysninger fortaget af læger eller sundhedspersoner, der undtages fra obligatorisk gennemførelse af en DPIA. Dette skal sammenholdes med, at der i Sundhedsplatformen behandles helbredsoplysninger om en betyde-

[1] Justitsministeriet, Betænkning nr. 1565 om Databeskyttelsesforordningen (2016/679) – og de retlige rammer for dansk lovgivning, del I, bind 1, side 528 ff.

lig del af Danmarks befolkning, og at systemet alene af den grund må anses for omfattende.

Det følger af databeskyttelsesforordningens artikel 35, stk. 1, 2. pkt., at en enkelt konsekvensanalyse kan omfatte flere lignende behandlingsaktiviteter, der indebærer lignende høje risici.[2] Som bestemmelsen må fortolkes, kan Region Hovedstaden og Region Sjælland derfor foretage en fælles konsekvensanalyse grundet det fælles dataansvar på Sundhedsplatformen, selvom der mellem regionerne kan bestå mindre lokale forskelle i implementeringen og anvendelsen af Sundhedsplatformen.

Databeskyttelsesforordningen indeholder følgende minimumskrav til en DPIA (jf. art. 35, stk. 7):

1. En *systematisk beskrivelse* af de planlagte former for behandling og formålene med behandlingen.[3]
2. En *vurdering* af om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene
3. En *vurdering* af risiciene for de registreredes rettigheder og frihedsrettigheder
4. De *foranstaltninger* der påtænkes for at *imødegå* de pågældende *risici*, herunder garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af databeskyttelsesforordningen under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

Kan de risici, som behandles i konsekvensanalysen, ikke mitigeres, følger det af databeskyttelsesforordningens artikel 36, at Datatilsynet skal høres forinden behandlingens iværksættelse. Det er ikke Bech-Bruuns vurdering, at Sundhedsplatformen afstedkommer risici, som ikke er mulige at begrænse ved implementering af særlige mitigerende foranstaltninger, herunder ændringer af arbejdsgange.

2.1 Baggrunden for denne konsekvensanalyse

Region Hovedstaden gennemførte over sommeren og efteråret 2016 en PIA (Privacy Impact Assessment) i forhold til behandlingen af personoplysninger i Sund-

[2] Justitsministeriets betænkning nr. 1565, s. 526

[3] Bestemmelsen indeholder endvidere et krav om at den systematiske beskrivelse indeholder eventuelle legitime interesser, som forfølges af den dataansvarlige. Da der er meget lav sandsynlighed for, at behandling af personoplysninger baseres på den såkaldte interesseafvejning i databeskyttelseslovens art. 6, stk. 1, nr. 7, er den sidste del af kravet udeladt her.

hedsplatformen. Denne PIA blev foretaget forud for idriftsættelsen af Sundhedsplatformen på hospitaler i Region Hovedstaden og Region Sjælland. Formålet var at kortlægge de konsekvenser for privatlivet, som behandlingen af personoplysninger (herunder specielt helbredsoplysninger) i Sundhedsplatformen medfører og i den forbindelse at identificere og mitigere de risici, som optræder i denne forbindelse.

Da Sundhedsplatformen i dag er implementeret og har været i drift i en periode på hospitalerne i Region Hovedstaden og Region Sjælland, er det besluttet at gennemføre en opfølgende DPIA, der med udgangspunkt i de risikotemaer, der blev konstateret under den forudgående PIA i november 2016, skal hjælpe regionerne til at identificere og mitigere de risici, som aktuelt findes i forbindelse med behandling af personoplysninger i Sundhedsplatformen.

Denne opfølgende DPIA er ikke båret af det forhold, at behandlingsaktiviteternes risiko eller anvendelsen af Sundhedsplatformen nødvendigvis har ændret sig siden 2016, så at regionerne er forpligtede til at udarbejde en fornyet DPIA i medfør af databeskyttelsesforordningen. Der er således ikke tale om en DPIA udarbejdet på grundlag af bestemmelsen i databeskyttelsesforordningens art. 35, stk. 11.

På baggrund af denne rapport vil Region Hovedstaden og Region Sjælland inden for rammerne af de gennemførte interviews og udvalgte risikotemaer være i stand til at dokumentere, hvor i Sundhedsplatformen de aktuelt væsentligste risici findes, ligesom det vil være muligt for regionerne at iværksætte den efterfølgende proces med at mitigere de identificerede risici.

2.2 Emnet for denne konsekvensanalyse

Emnet for denne konsekvensanalyse er Sundhedsplatformens implementering og drift på hospitaler i Region Hovedstaden og Region Sjælland.

3. Processen for DPIA i relation til Sundhedsplatformen

DPIA'en er gennemført over perioden juli – september 2018.

Nærværende rapport er en sammenfatning af – og udgør dermed dokumentation for – de forhold og tiltag, som er identificeret og vurderet i forbindelse med gennemførelsen af DPIA'en. Dokumentationen har både til formål at udgøre grundlaget for den fremadrettede interne risk management af de identificerede forhold (se yderligere i afsnit 0) samt den eksterne dokumentation i forbindelse med dialogen med Sundheds- og Ældreministeriet og i forbindelse med Datatilsynets eventuelle kontrol af, om behandlingen af personoplysninger i Sundhedsplatformen sker i overensstemmelse med den relevante lovgivning.

Gennemførelsen af en DPIA for Sundhedsplatformen bliver yderligere kompliceret af, at behandlingen af personoplysninger i Sundhedsplatformen skal overholde både sundhedsloven, databeskyttelsesforordningen og databeskyttelsesloven og derfor hører under både Sundhedsministeriet og Datatilsynet.

Rapporten indeholder anbefalinger vedrørende de mitigerende handlinger, som bør gennemføres for at imødegå de identificerede risici, herunder sikkerhedsforanstaltninger og mekanismer, der kan sikre beskyttelse af personoplysningerne i Sundhedsplatformen, jf. afsnit 0.

Region Hovedstaden og Region Sjælland har i fællesskab udpeget de personer, som skulle deltage i interviews med henblik på udarbejdelse af den generelle beskrivelse af Sundhedsplatformen, kortlægning af de overordnede datastrømme og opfølgning på de identificerede risikotemaer under den oprindelige PIA fra 2016.

3.1 Metode og terminologi

3.1.1 Metode

Denne DPIA er udformet med henblik på at opfylde de krav, som databeskyttelsesforordningens artikel 35 stiller til indholdet af en konsekvensanalyse vedrørende databeskyttelse. Hovedfokus for denne DPIA er derfor den juridiske compliance med databeskyttelsesforordningen.

Da den første konsekvensanalyse på behandling af personoplysninger på Sundhedsplatformen blev udarbejdet i 2016, fandtes der ikke en international anerkendt metode til udarbejdelse af DPIA samtidig med, at databeskyttelsesforordningen ikke var trådt i kraft. Nærværende konsekvensanalyse er udarbejdet i

overensstemmelse med anbefalingerne i den internationale standard, ISO 29134 "Information technology - Security techniques - Privacy impact assessment - Guidelines".

Konsekvensanalysen bygger endvidere på lovgivningen og de medio 2018 tilgængelige fortolkningsbidrag, herunder Artikel 29-gruppens vejledning "Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679" samt Datatilsynets vejledning vedrørende "Konsekvensanalyse".

3.1.2 Terminologi

Konsekvensanalysen fra 2016 anvendte terminologien PIA (dækkende begrebet Privacy Impact Assessment) i forhold til den gennemførte analyse. Nærværende opfølgende analyse anvender DPIA (Data Protection Impact Assessment). Dette skyldes, at DPIA er den terminologi, som anvendes i databeskyttelsesforordningen.

Enkelte steder i analysen anvendes begrebet PIA. Dette skyldes alene, at det på de pågældende steder er fundet mest naturligt at anvende terminologien fra 2016.

3.1.3 Risikotemaer og identificerede risici

Nærværende konsekvensanalyse udføres overordnet set i forhold til Sundhedsplatformen. Analysen er indsnævret via identifikation af en række risikotemaer, som er overordnede behandlingsaktiviteter eller aktiviteter tilknyttet Sundhedsplatformen.

En del af disse risikotemaer blev identificeret i forbindelse med den oprindelige PIA i 2016. For disse risikotemaer har udgangspunktet været en revurdering af de identificerede risici og regionernes implementering af mitigerende foranstaltninger (på daværende tidspunkt primært Region Hovedstaden, som var først med 'go live'). I forbindelse med nærværende analyse er identificeret nye risikotemaer og underliggende risici, herunder også nye underliggende risici til allerede identificerede risikotemaer.

3.1.4 De registreredes synspunkter

Databeskyttelsesforordningens artikel 35, stk. 9 indeholder krav om, at den dataansvarlige - hvis det er relevant - skal indhente de registreredes eller deres repræsentanters synspunkter.

Dette er ikke fundet relevant i forhold til nærværende analyse, og der er derfor ikke sket høring af repræsentanter for brugere eller patienter i Sundhedsplatformen som led i udarbejdelsen af denne opfølgende DPIA.

3.2 Gennemgåede dokumenter

Følgende dokumenter er gennemgået i forbindelse med gennemførelse af DPIA'en:

- Statsrevisorernes beretning om Sundhedsplatformen, juni 2018
- Samtykke til at udveksle helbredsoplysninger af 13. marts 2018 (Region Hovedstaden)
- Min Sundhedsplatform - procedurer for patienters og pårørendes adgang, oprettelse af adgang m.v. inkl. bilag, version 8 af 25. maj 2018 (Region Hovedstaden)
- Aktindsigt i patientjournaler, version 13 af 12. oktober 2017 (Region Hovedstaden)
- Vejledninger til sikkerhedslog (Region Sjælland)
- Aftale om fælles dataansvar, november 2017
- De vedtagne brugeradgange pr. 27. november 2017
- Rettighedsmodel (senest revideret i november 2017)
- Kontrolinstruks for logopfølgning
- Vejledning om brug af oversigtskærme
- Nyt uddannelseskoncept (Region Hovedstaden)
- Nyt uddannelseskoncept (Region Sjælland)
- Informationspjece fra CMIT, "Beskyt vores information", 2015
- Sikkerhedstest 2018
- Brugerundersøgelse på Sundhedsplatformen, forår 2018
- Håndtering af Sherlock
- Referat fra forretningsudvalgsmøde vedrørende konklusionerne fra Rigsrevisionens rapport.
- Oversigt over eksterne interaktioner i Sundhedsplatformen

4. Generel beskrivelse af Sundhedsplatformen og kortlægning af overordnede datastrømme

Den generelle beskrivelse af Sundhedsplatformen og kortlægningen af de overordnede datastrømme har til formål at give et indblik i, hvad formålet med behandlingen af personoplysninger i Sundhedsplatformen er, samt hvordan behandlingen af personoplysninger foregår i Sundhedsplatformen på et overordnet plan. I den forbindelse er det væsentligt at etablere et overordnet billede af Sundhedsplatformens integrationer til andre IT-systemer, specielt inden for sundhedssektoren.

4.1 Generel beskrivelse af Sundhedsplatformen

Sundhedsplatformen er en fælles, elektronisk patientjournal, som blev implementeret løbende i perioden 2016-2017 på hospitaler og sygehuse i Region Hovedstaden og Region Sjælland. Sundhedsplatformen er et samarbejde mellem Region Hovedstaden og Region Sjælland og er det hidtil største danske IT-projekt indenfor sundhedssektoren.

Det første hospital i Region Hovedstaden (Herlev-Gentofte Hospital) gik i drift med Sundhedsplatformen (omtales som "Go Live") som sundhedsjournal for sine patienter den 21. maj 2016. De øvrige hospitaler og sygehuse i Region Hovedstaden og Region Sjælland er sidenhen overgået til at anvende Sundhedsplatformen som sundhedsjournal for deres patienter.

Sundhedsplatformen erstatter op til 30 forskellige tidligere anvendte IT-systemer. Alle informationer om patienten bliver samlet i den elektroniske patientjournal, som både patienten og sundhedspersonalet har adgang til. Patienten får således mulighed for at følge sin behandling før, under og efter behandlingsforløbet, og det relevante sundhedspersonale får hurtigt og nem adgang til information om patienten og overblik over behandlingsforløbet på tværs af de to regioners hospitaler og sygehuse. I august 2018 var der for Region Hovedstaden oprettet 44.343 brugere i Sundhedsplatformen. For Region Sjælland var tallet 21.920 brugere. Det samlede antal brugeradgange udgjorde således cirka 66.000.

Sundhedsplatformen er designet til at indeholde sundhedsoplysninger om 2,5 mio. danskere.

Sundhedsplatformen er baseret på et IT-system fra den amerikanske softwareleverandør EPIC, som leverer sundheds-it til mere end 1.100 hospitaler over hele verden.

På trods af at Sundhedsplatformen erstatter mere end 30 IT-systemer, er det samlede IT-mæssige setup på hospitalerne fortsat yderst kompliceret, da Sundhedsplatformen integreres med mere end 90 IT-systemer inden og uden for sundhedssektoren.

Sundhedsplatformen indeholder for en stor dels vedkommende helbredsmæssige oplysninger om de borgere, som er i kontakt med de hospitaler og sygehuse, som anvender Sundhedsplatformen. Sundhedsplatformen indeholder herudover en lang række oplysninger om patienterne, som både er af ren privat karakter, eller som af andre årsager er fortrolige. Sundhedsplatformen indeholder også oplysninger om de ansatte på de hospitaler/sygehuse, som har implementeret Sundhedsplatformen. Denne registrering af oplysninger sker via de ansattes oprettelse som brugere i Sundhedsplatformen og i forbindelse med logning af brug af Sundhedsplatformen samt registrering af behandlingsaktiviteter, som involverer den pågældende ansatte. I særlige tilfælde er der mulighed for, at Sundhedsplatformen kan afsløre oplysninger om strafbare forhold om ansatte, hvis fx en loggennemgang viser, at en ansat går ind og kigger på en patient på en anden afdeling uden at have et aktuelt behandlingsforhold til den pågældende patient og dermed ikke handler i overensstemmelse med den relevante lovgivning. På tilsvarende vis kan Sundhedsplatformen indeholde oplysninger om behandlingsfejl og forsømmelser blandt ansatte.

4.1.1 Lovgivningen bag behandling af personoplysninger i Sundhedsplatformen

Databeskyttelsesforordningen og databeskyttelsesloven indeholder en særlig beskyttelse af personoplysninger, herunder særlige kategorier af personoplysninger (følsomme personoplysninger), som udover helbredsmæssige oplysninger kan være fx oplysninger om religiøs eller seksuel overbevisning samt genetiske og biometriske data.

Overordnet følger det af databeskyttelseslovens § 7, stk. 3, at der blandt andet kan ske behandling af følsomme personoplysninger, hvis behandlingen er nødvendig med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt.

Sundhedsloven (kapitel 9) er lex specialis i forhold til databeskyttelsesloven i forbindelse med sundhedspersoners indsamling og videregivelse af patienters helbredsoplysninger, oplysninger om øvrige rent private forhold og andre fortrolige oplysninger. De øvrige forhold, fx sikkerhedsforanstaltninger, i forbindelse med behandling af oplysninger om patienter samt behandling af oplysninger om an-

satte reguleres i henhold til bestemmelserne i databeskyttelsesforordningen og databeskyttelsesloven.

Det betyder, at sundhedsloven, databeskyttelsesforordningen og databeskyttelsesloven i forening sætter rammerne for den behandling af oplysninger om patienter og ansatte, som sker i Sundhedsplatformen.

Samspillet mellem den nationale og europæiske lovgivning vedrørende databeskyttelse er dog underlagt det forhold, at databeskyttelsesforordningen er supranational, hvorfor sundhedsloven og databeskyttelsesloven skal fortolkes EU-konformt. Databeskyttelsesforordningen indeholder en lang række skærpelser af kravene til lovlig behandling af personoplysninger i forhold til de tidligere danske regler på området, herunder de regler som var gældende, da den oprindelige PIA blev gennemført i 2016. Databeskyttelsesforordningen indebærer blandt andet, at de to regioner, som er fælles dataansvarlige for behandlingen af patienternes personoplysninger i Sundhedsplatformen, er forpligtede til at iværksætte en række procedurer for blandt andet at sikre, at patienterne får den information, de har krav på, hvad enten der er tale om oplysningsforpligtelser, der initieres af regionerne selv eller på patientens anmodning. Princippet om transparens medfører endvidere, at der skal ske dokumentation af datastrømme i Sundhedsplatformen.

4.2 Kortlægning af overordnede behandlingsaktiviteter og datastrømme

En kortlægning af behandlingsaktiviteter og datastrømme med personoplysninger[4] er en beskrivelse af processer med personoplysninger, hvor personoplysninger kommer ind i Sundhedsplatformen eller flyttes mellem forskellige enheder i henholdsvis Region Hovedstaden og Region Sjælland. Det kan fx være spørgsmål som: Hvordan indsamles oplysningerne? Kommer de fra patienten selv eller fra andre? Hvad er lovhjemlen til at indsamle oplysningerne? Er lovhjemlen patientens samtykke, eller har patientens praktiserende læge ret eller pligt til at videregive oplysningerne til hospitalet/sygehuset? Hvad er formålet med den konkrete behandling af personoplysninger – aktuel behandling af patienten eller forskning og statistik?

Der er tale om et meget omfattende arbejde, både hvad angår kortlægningen af datastrømme internt i Sundhedsplatformen og ikke mindst i forhold til Sundhedsplatformens eksterne integrationer til kliniske systemer samt administrative, farmaceutiske og special-kliniske systemer. Under den oprindelige PIA i 2016 blev der identificeret mere end 90 datastrømme alene mellem eksterne systemer og Sundhedsplatformen.

[4] Udtrykket mapping anvendes også i denne forbindelse

Databeskyttelsesforordningen indeholder et krav om, at Region Hovedstaden og Region Sjælland som dataansvarlige skal overholde princippet om accountability og i den forbindelse blandt andet være i stand til at påvise, at behandling af personoplysninger er i overensstemmelse med databeskyttelsesforordningen. Regionerne er dermed forpligtede til at udarbejde en forholdsvis detaljeret oversigt over behandlingsaktiviteter i Sundhedsplatformen for at overholde databeskyttelsesforordningens krav om accountability. Region Hovedstaden forventer dette arbejde afsluttet med udgangen af 2018. Region Sjælland har udarbejdet en oversigt, der omfatter hele sundhedsområdet i regionen.

Det centrale ved de overordnede datastrømme i Sundhedsplatformen er, at der er tale om et meget stort antal datastrømme med følsomme oplysninger om potentielt 2,5 mio. danskere, oplysninger om ansatte i de to regioner, som anvender Sundhedsplatformen, samt integrationer mellem Sundhedsplatformen og en lang række eksterne IT-systemer.

5. Risikotemaer

Nedenstående risikotemaer vedrørende behandling af personoplysninger på Sundhedsplatformen er udvalgt ud fra oplysningerne i de gennemførte interviews samt ud fra konkrete persondataretlige problemstillinger vedrørende Sundhedsplatformen.

Risikotemaerne er fastsat ud fra en drøftelse mellem regionerne og Bech-Bruun samt den information, som er fremkommet i forbindelse med interviews. Det betyder, at det principielt vil være muligt at finde risikotemaer vedrørende behandling af personoplysninger, som ikke analyseret i denne rapport.

Risikotemaerne beskrevet i afsnit 5.1- 5.7 stammer fra den oprindelige PIA-proces fra 2016 og har derfor været genstand for fornyet opfølgning og juridisk vurdering i denne DPIA 2018.

Risikotemaerne beskrevet i afsnit 5.8 - 5.12 er derimod identificeret som nye under denne DPIA 2018 vedrørende Sundhedsplatformen.

De identificerede risici, som aktuelt består, og som DPIA har givet anledning til at fremhæve, er beskrevet i umiddelbar tilknytning til de enkelte risikotemaer.

5.1 Fordeling af dataansvar mellem Region Hovedstaden og Region Sjælland

Det er beskrevet i den oprindelige PIA fra 2016, at Region Hovedstaden og Region Sjælland har valgt at etablere fælles dataansvar i forbindelse med behandling af patienters personoplysninger i Sundhedsplatformen. Denne konstruktion sikrer, at Region Hovedstaden og Region Sjælland også i praksis har et fælles ansvar for opgaven vedrørende behandling af patienter og ansattes personoplysninger i Sundhedsplatformen, og at denne opgave sikres i samme omfang, uanset om en patient/ansat er tilknyttet den ene eller den anden region.

Det fælles dataansvar mellem Region Hovedstaden og Region Sjælland er etableret. Endvidere har regionerne – i overensstemmelse med anbefalinger fra Datatilsynet – udarbejdet en række fælles politikker til konkret udmøntning af det fælles dataansvar, fx politik for dokumentation for lovlig behandling af personoplysninger og politik for oplysningspligt og besvarelse af indsigtsanmodninger.

Risiko 1.1: *Fordeling af dataansvar*
På trods af den indgåede aftale om fælles dataansvar vil et fælles dataansvar medføre en forøget risiko for kompromittering af personoplysninger i Sundhedsplatformen alene af den grund, at et større antal personer har potentiel adgang til oplysningerne – også selv om det kræver, at de går ud over deres autorisation.

Fordelingen af dataansvaret aktualiserer derfor behovet for udarbejdelsen af interne procedurer mellem regionerne, som ikke er indbyrdes modstridende.

5.2 Rettigheder og autorisationer

Tildelingen af rettigheder og autorisationer på Sundhedsplatformen (rettighedsmodellen for adgang til slutbrugernes oplysninger) er underlagt de regulatoriske krav i både sundhedsloven og databeskyttelseslovgivningen, herunder principperne i den tidligere gældende vejledning til sikkerhedsbekendtgørelsen, der blev udstedt i medfør af den nu ophævede persondatalov. Sundhedslovens § 42a afgrænser bl.a. sundhedspersoners adgange til og videregivelse fra elektroniske patientjournaler og regulerer, hvordan sundhedspersoner kan anvende medhjælpende sundhedspersoner i deres arbejde, fx hvis en læge bruger en sygeplejestuderende som medhjælp.

5.2.1 Tildeling af rettigheder og autorisationer

Som beskrevet i den oprindelige PIA fra 2016 tildeles rettigheder og autorisationer på Sundhedsplatformen i henhold til den rettighedsmodel, der er lavet i overensstemmelse med reglerne i sundhedsloven.

Sundhedsplatformens oprindelige rettighedsmodel var grundlæggende set mere restriktiv end de krav, som følger af sundhedslovens § 42a, da det fx kun er læger, som vil få den brede adgang til alle patientoplysninger i Sundhedsplatformen.

Rettighedsmodellen indebærer også, at der er nogle medarbejdergrupper, som ikke kan få brugeradgange til Sundhedsplatformen. Det fremgår af PIA 2016 "NOTAT: Ingen brugeradgange for kvalitetsmedarbejdere og risikomanagere", at kvalitetsmedarbejdere og risikomanagere, der håndterer sagsbehandling af utilsigtede hændelser, ikke kan få adgang til patientoplysninger i Sundhedsplatformen, fordi der ikke er hjemmel til dette i sundhedsloven, da de pågældende medarbejdere ikke er autoriserede sundhedspersoner i autorisationslovens forstand. Det understreges i notatet, at sundhedspersoner, der arbejder med kvalitetsarbejde eller utilsigtede hændelser, og som kan tilgå patientjournaler i medfør af deres rolle som sundhedspersoner, ikke må bruge denne brugeradgang til opslag i forbindelse med fx kvalitetsarbejde eller håndtering af utilsigtede hændelser. Det er i 2018

oplyst, at der pågår et arbejde med at revidere adgangen for kvalitetsmedarbejdere og risikomanagere, da deres arbejdsbetingede behov nødvendiggør mere end en kiggeadgang.

Siden Go Live på Sundhedsplatformen den 21. maj 2016 og frem til udarbejdelse af PIA 2016 var det nødvendigt at justere nogle af de smallere brugeradgange til Sundhedsplatformen samt at skræddersy brugeradgange i forhold til de praktiske behov i de enkelte afdelinger på de to hospitaler, som anvendte Sundhedsplatformen på daværende tidspunkt. Det var muligt at justere brugeradgangene i den oprindelige rettighedsmodel, fordi den oprindelige rettighedsmodel i Sundhedsplatformen var mere restriktiv end kravene i sundhedsloven.

Rettighedsmodellen er senest revideret i november 2017. Ud fra den fremsendte rettighedsmatrix er det ikke muligt at se, hvilke adgange som fx går på tværs af regioner, hospitaler og afdelinger.

Konkret tildeles rettigheder automatisk ud fra rettighedsmodellen, når medarbejderen oprettes i systemet under den faggruppe og det speciale, som den pågældende medarbejder tilhører. Har en medarbejder behov for yderligere adgang, kan vedkommendes leder anmode om, at denne adgang tildeles. Dette er eksempelvis tilfældet med fysioterapeuter og ergoterapeuter, som konkret kan have behov for en tværgående adgang.

I forbindelse med ændring eller manuel tildeling af brugeradgange er de ansvarlige medarbejdere i Sundhedsplatformen opmærksomme på, at der ikke må gives adgang til flere personoplysninger end nødvendigt.

5.2.2 Break the Glass/Bump the Glass

Det overordnede formål med funktionaliteten "Break the Glass" i Sundhedsplatformen er at sikre fortrolighed og at beskytte adgangen til patientdata.

"Break the Glass" er et regelsæt, som definerer, hvilke oplysninger i Sundhedsplatformen en given medarbejder må tilgå. Regelsættet er oprindeligt udarbejdet i forhold til den faggruppe, som den pågældende medarbejder er tilknyttet, og hvilke rettigheder, som den pågældende medarbejder dermed skal have, til at slå op i Sundhedsplatformen.

Den konkrete betydning af funktionaliteten " Break the Glass" er, at en medarbejder, som forsøger at tilgå patientoplysninger, som ligger udenfor den pågældendes autorisation, bliver mødt af et skærmbillede, hvoraf det fremgår, at medarbejderen er på vej udenfor sin autorisation. En medarbejder, som har adgang til

det organisatoriske niveau "hospital", vil fx blive mødt af "Break the Glass", hvis medarbejderen forsøger at tilgå en patient på et andet hospital.

Hvis medarbejderen ikke forsøger at tilgå oplysningerne og annullerer handlingen, vil der blive foretaget en registrering af, at den pågældende har forsøgt at "Bump the Glass". Hvis medarbejderen har en aktuel behandlingsrelation til en patient udenfor medarbejderens autorisation, har medarbejderen mulighed for at bryde barrieren ved at oplyse om årsagen til, at barrieren brydes (fx behandling eller faglig vurdering) samt at indtaste sit password. Hver gang en medarbejder bliver mødt af "Break the Glass" og angiver en årsag, genereres work bench-rapporter på henholdsvis de seneste 24 timer og de seneste 7 dage. Derudover genererer Systemforvaltning i Sundhedsplatformen rapporter, der er mere dybdegående, jf. yderligere nedenfor i afsnit 5.2.3 om gennemgang af loggen.

Det har siden PIA 2016 vist sig, at Break the Glass/Bump the Glass har været sat op, således at en lang række hændelser, som har været helt legale, er blevet logget som muligt misbrug. Et eksempel har været, at Break the Glass/Bump the Glass grundet antallet af udslag har gjort anvendelsen af Sundhedsplatformen vanskelig for vikarer, som arbejder i forskellige afdelinger, og derfor har et legitimt behov for at tilgå Sundhedsplatformen flere steder.

Grundet de mange falske rapporteringer har både Region Hovedstaden og Region Sjælland valgt andre løsninger som rapporteringsværktøj, hvilke beskrives nedenfor i afsnit 5.2.3. Break the Glass/Bump the Glass bruges derfor primært i awareness-øjemed.

5.2.3 Gennemgang af loggen

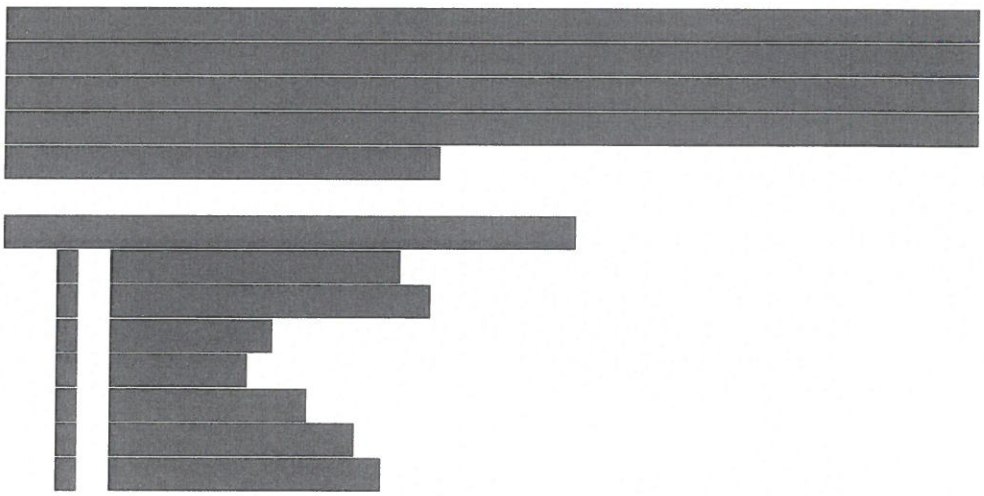
Som anført ovenfor er en væsentlig forudsætning for vurderingen af, om medarbejderne handler i overensstemmelse med de tildelte roller og autorisationer, at der løbende foretages kontrol af dette.

Kravet om logning og efterfølgende gennemgang af loggen var tidligere et krav, som fulgte direkte af sikkerhedsbekendtgørelsens § 19. Overgangen til databeskyttelsesforordningen har medført, at sikkerhedsbekendtgørelsen er ophævet. Det fremgår af Datatilsynets vejledning om behandlingssikkerhed, at er en eller flere af de foranstaltninger, der var en del af sikkerhedsbekendtgørelsen, efter en konkret vurdering fortsat relevante, vil det være oplagt at fortsætte med at gøre brug af dem. Det kunne fx være kravene om autorisation, kontrol med afviste adgangsforsøg eller logning. Regionerne har foretaget en sådan vurdering og har på denne baggrund valgt at fortsætte brugen af logning på Sundhedsplatformen.

Region Hovedstaden:
Kontrolinstruksen for intern gennemgang af logoplysninger ("kontrolinstruksen") er oprindeligt udarbejdet af Region Hovedstaden i samarbejde med Region Sjællands medarbejdere. Kontrolinstruksen er tidsmæssigt delt op i to faser. I den første fase er kontrollen baseret på stikprøver. Den anden fase påbegyndes, når der er indsamlet erfaringer fra den egentlige drift af Sundhedsplatformen. I den anden fase skal det vurderes, om det er muligt at implementere kontrolforanstaltninger, som i højere grad end stikprøver er målrettet mistænkelig adfærd. I relation til PIA 2016 blev det overvejet, om den tredjepartsløsning, der var implementeret i Region Sjælland, kunne implementeres generelt i Sundhedsplatformen. Status medio 2018 er, at Region Hovedstaden arbejder på at anskaffe en løsning svarende til den, som Region Sjælland anvender. Se nærmere herom nedenfor.

Koncernledelsen i Region Hovedstaden besluttede i 2016, at "Break the Glass/Bump the Glass"-rapporter kom direkte ud til de enkelte hospitalsafdelingsledelser, som havde ansvaret for at analysere oplysningerne på listerne samt iværksætte eventuelle nødvendige personalemæssige konsekvenser, hvis en stikprøvekontrol viste, at en medarbejder havde foretaget sig noget uden for den pågældendes autorisation.

Det fremgår af den oprindelige kontrolinstruks vedr. Sundhedsplatformen (PIA 2016), at det endnu var uafklaret, hvilken konkret dokumentation for gennemførelsen af kontroller, som det ville være relevant at anvende og gemme. Det fremgik endvidere af kontrolinstruksen, at rapporteringen af kontrollens resultat skulle ske til systemejer og informationssikkerhed i et kort notat, da der endnu ikke var valgt en egentlig standard for rapportering.



[redacted]

Ved siden af den manuelle stikprøvekontrol har de registrerede mulighed for via logfunktionen i Min Sundhedsplatform at følge med i, hvilke personer som tilgår patientens journal. I dette tilfælde er kontrollen således efterfølgende og initieres konkret ved, at den registrerede aktivt stiller spørgsmålstegn med en registrering på loggen. I sådanne tilfælde foretages en målrettet kontrol som alternativ til den ovenfor beskrevne screeningsprocedure. Rapporter fra Break the Glass/Bump the Glass udgør fortsat et vigtigt instrument i en sådan målrettet kontrol.

Region Sjælland:
Region Sjælland har siden PIA 2016 implementeret et IT-system, som kan håndtere hændelser, således at systemet kan reagere på ulogiske handlinger blandt alle medarbejdere med adgang, fx hvis en medarbejder på afdeling A er inde og kigge på en patient fra afdeling B, eller hvis en medarbejder søger i patientjournalen på en patient, der bor på samme vej, som den pågældende medarbejder. Baseret på sine erfaringer med typiske misbrugstilfælde har Region Sjælland udarbejdet nogle 'mistanketyper', således at systemet blandt andet danner rapporter ved ethvert opslag af naboer, familiemedlemmer eller kollegaer.

[redacted]Hændelser defineres som et opslag på en specifik patient inden for én dag.

Systemet har afløst den manuelle stikprøvekontrol, som Region Hovedstaden fortsat udfører.

[redacted]

Det er Region Sjællands vurdering, at systemet har haft en opdragende effekt på personalet, idet antallet af hændelser er faldet.

Risiko 2.1: *Udvidelse/ændring af oprindelig rettighedsmodel*
Den oprindelige rettighedsmodel er senest revideret og udvidet i november 2017, så tildelingen af rettigheder er mere avanceret, så der på nuværende tidspunkt er større risiko for tildeling af rettigheder i strid med reglerne i sundhedsloven. I den forbindelse bør manuel tildeling af rettigheder som udgangspunkt begrænses til et minimum. Der bør endelig være løbende kontrol af, om tildelingen af adgange sker i overensstemmelse med rettighedsmodellen, herunder kravene i sundhedslovgivningen.

Risiko 2.2: *Adgang for kvalitetsmedarbejdere og risikomanagere*
Da kvalitetsmedarbejdere og risk managers kan have tungtvejende arbejdsbetingede behov for adgang til Sundhedsplatformen, kan det udgøre en risiko for blandt andet datakvaliteten, såfremt disse faggrupper ikke har den nødvendige adgang til Sundhedsplatformen. Der pågår i 2018 et arbejde med at revidere adgangen for disse medarbejderkategorier.

Risiko 2.3: *Anvendelse af funktionaliteten "Break the Glass"*
"Break the Glass" er ikke en absolut adgangsbegrænsning i Sundhedsplatformen, hvilket indebærer at det er muligt for medarbejdere at skaffe sig adgang til personoplysninger, som ikke er omfattet af deres autorisation. I den forbindelse skal det dog bemærkes, at der foretages logning hver gang Break the Glass aktiveres.

Da brugere af Sundhedsplatformen har oplevet, at "Break the Glass" har været sat *for* strengt op, således at der har været genereret for mange falske positive rapporter, kan disse falske rapporter i sig selv skulle underlægges en særlig varsom behandling, idet de er egnet til at skabe mistanke om dadelværdige og strafbare forhold hos de ansatte, som unødvendigt fremgår i rapporten.

[redacted]

[redacted]

Risiko 2.6: *Valg af dokumentation og format for rapportering af logkontrol*
I forhold til PIA 2016 har Region Hovedstaden vedtaget en "Kontrolinstruks for SP Logopfølgning", som indeholder en relativt detaljeret beskrivelse af, hvordan logopfølgning skal dokumenteres og herunder hvilket format det skal ske i. Det er i den forbindelse væsentligt, at der løbende følges op på, om alle elementer i instruksen følges, da værdien af logopfølgning generelt ellers reduceres. Den vedtagne instruks reducerer selvsagt den risiko, som er påvist i forbindelse med PIA 2016, men det er væsentligt at understrege, at dette ikke har nogen betydning i forhold til parametrene i ovenfor nævnte Risiko 2.5

5.3 Konvertering af data fra eksisterende systemer til Sundhedsplatformen

Det fremgår af den oprindelige PIA fra 2016, at det tidsmæssige aspekt i processen vedrørende konvertering af data fra eksisterende IT-sundhedssystemer til Sundhedsplatformen indebar, at det ikke var alle de data, der var planlagt konverteret, som reelt blev konverteret til Sundhedsplatformen. Det betød, at nogle oplysninger, der er relevante for en række eksisterende og fremtidige behandlingsforløb, fortsat lå i de "gamle" IT-systemer med den konsekvens, at sundhedspersoner var nødsaget til at konsultere to eller flere systemer i forbindelse med patientbehandlingen.

Overgangen til Sundhedsplatformen indebærer, at tidligere anvendte systemer, som erstattes af Sundhedsplatformen, som udgangspunkt bør lukkes (sunsettes). Dette er motiveret af sikkerhedshensyn samt sikringen af datakvaliteten, fordi der ikke føres parallelle systemer, som forudsætter yderligere brugerviden.

Leverandøren af Sundhedsplatformen, EPIC, er ikke involveret i lukningen af tidligere anvendte systemer. Derimod foregår lukningen i de enkelte regioner, som hver for sig udarbejder et projekt for hvert system. Da sunsetting ikke har været en del af implementeringen af Sundhedsplatformen, skal der udarbejdes budgetansøgninger for hvert projekt. Dette betyder, at besparelseshensyn kan påvirke lukningen af tidligere anvendte systemer, både hvad angår tidspunkt og metodevalg.

Alt efter det enkelte system har det i regionerne krævet forskellige metoder at håndtere overgangen til Sundhedsplatformen. Nogle behandlinger har kunnet afvikles i de gamle systemer, således at de er blevet arkiveret, og efterfølgende behandlinger er iværksat i Sundhedsplatformen uden, at det har været nødvendigt, at der skulle ske overlapning mellem systemerne. Navnlig længerevarende patientrelationer, som var oprettet i det gamle system, og som skal overføres til Sundhedsplatformen, har derimod krævet særlige tiltag. For Region Hovedstaden og Region Sjælland er der tale om individuelle løsninger for hvert system.

Da journaldata som udgangspunkt skal opbevares i 10 år ifølge journalføringsbekendtgørelsen, skal løsningen samtidig muliggøre opbevaring og adgang til de data, som befandt sig i det system, som skal lukkes.

Region Hovedstaden:
Implementeringen af Sundhedsplatformen indebar, at Region Hovedstaden skulle lukke omkring 30 systemer. Status medio 2018 er, at 23 af disse systemer ikke længere er i drift.

Enkelte systemer har været så store, at det ikke har været muligt at overføre eksisterende data til Sundhedsplatformen. Et eksempel er Antikoagulation-systemet (AK-systemet). Derfor foranstaltes alternative løsninger, så eksisterende data kan tilgås, mens indtastningen af nye data sker i Sundhedsplatformen.

Fødejournalen er et andet eksempel på et system, som det fra dag til dag ikke var muligt at overføre til Sundhedsplatformen, da patienterne i fødejournalen kendetegnes ved at være i systemet i længere tid. Efter lukningen af fødejournalen har det som alternativ foranstaltning været nødvendigt at lave pdf-filer, som er lagt ind i OnBase med henblik på at gøre dem tilgængelige i en klinisk kontekst.

Anderledes har det for EPM-systemet fx været nødvendigt at bevare en læseadgang til medicinmodulet, da alternativet ville være at anskaffe et nyt system for visning af data.

Mere enkelt har det været muligt at lukke andre systemer, fordi der ikke har været indtastet nye data efter overgangen til Sundhedsplatformen. Data fra disse systemer er overført til den historiske patientjournal.

Da de tidligere anvendte systemer er underlagt opsigelsesperioder, har der været incitamenter til at holde systemerne kørende i deres opsigelsesperiode.

Det har været en udfordring, at data fra flere mindre systemer er blevet overgivet i svært anvendelige formater, fx uden kryptering i tabelform. Årsagen antages at

være samarbejdsvanskeligheder mellem Region Hovedstaden og tidligere leverandører grundet overgangen til Sundhedsplatformen. Derfor ligger data flere steder samlet i oversigtsform. Skulle disse data ordnes, ville det formentlig være billigere at anvende det forladte system. Disse erfaringer har tydeliggjort behovet for exit-bestemmelser i IT-kontrakterne.

Region Sjælland:
Region Sjælland er på tilsvarende vis ved at lukke tidligere anvendte systemer. Det er prioriteret først at lukke OPUS-miljøerne ned, hvorefter en række mindre systemer prioriteres. Regionen har indgået aftale med en ekstern leverandør, som indeholder en samlet løsning vedrørende sunsetting af systemer.

Risiko 3.1: *Gamle IT-systemer i (fortsat) hel eller delvis drift*
Som udgangspunkt behandles ikke andre og flere personoplysninger i Sundhedsplatformen end i tidligere systemer. Som fælles brugergrænseflade skal Sundhedsplatformen derfor som udgangspunkt samle adgangen til personoplysningerne ét sted.

Mængden af data i tidligere anvendte systemer har imidlertid medført, at det har været og er en tidskrævende og vanskelig proces at overføre eksisterende oplysninger til Sundhedsplatformen.

Den fortsatte fulde eller delvise drift af gamle IT-systemer medfører, at brugerne af Sundhedsplatformen i visse tilfælde skal benytte flere systemer, eller at data fra tidligere anvendte systemer opbevares i alternative løsninger. Hvor der alene er kiggeadgange til tidligere anvendte systemer, kan forståelse af information i det ene system forudsætte kendskab til det andet. En sådan sideløbende brug af flere systemer er ikke forudsat efter implementeringen af Sundhedsplatformen.

Når sundhedspersoner udover Sundhedsplatformen skal konsultere ét eller flere "gamle" IT-systemer, er der en risiko i forbindelse med behandling af personoplysninger, fordi det er sundhedspersonen, som selv skal samle oplysninger, som ellers ville blive vist samlet, hvis de var blevet konverteret til Sundhedsplatformen. Denne risiko intensiveres, når personoplysningerne i enkelte tilfælde kan foreligge som rådata i form af usorterede og ukrypterede data alt efter den løsning, som er valgt i forbindelse med sunsetting af det gamle system. Således kan personoplysninger overses, ligesom de kan ske at blive tillagt forkert værdi, hvilket alt sammen kan have betydning for datakvaliteten og patientsikkerheden.

Gamle systemer er blandt andet holdt kørende ud fra det hensyn, at der i opsigelsesperioden alligevel er betalt for, at systemet står til regionernes rådighed. Den efterfølgende finansiering og udarbejdelse af projekter for sunsetting indebærer

en risiko for, at gamle systemer holdes i drift uhensigtsmæssigt længe, hvilket i sig selv udgør en sikkerhedsrisiko, uagtet at de trufne sikkerhedsforanstaltninger på systemniveau har været forsvarlige.

5.4 Samtykke til yderligere behandling af patienternes personoplysninger i forbindelse med indlæggelse

I forbindelse med indlæggelse på hospitaler og sygehuse, som anvender Sundhedsplatformen, får patienterne mulighed for at samtykke til udveksling af helbredsoplysninger i 15 forskellige relationer, som ligger uden for den aktuelle behandlingssituation. Konkret er der tale om, at patienten kan samtykke til, at hospitalet må informere patientens pårørende (skal angives konkret) om helbredsforhold og aktuel behandling, at hospitalet kan indhente helbredsoplysninger til egen læge eller speciallæge, at hospitalet må indhente oplysninger om tidligere behandlinger fra fx andre hospitaler, egen læge eller sociale myndigheder, samt at hospitalet må videregive helbredsoplysninger, fx til andre hospitaler, egen læge, sociale myndigheder eller kvalitetssikringsarbejde i regionen. Bagsiden af den blanket, hvorpå patienten samtykker, indeholder en kort gennemgang af reglerne vedrørende udveksling af helbredsoplysninger.

Når patienten gives mulighed for at samtykke til så mange forhold på samme tidspunkt, er det meget vigtigt, at patienten forstår, hvad samtykke til hvert enkelt forhold indebærer og ikke mindst kan have af konsekvenser for den pågældende.

Region Hovedstaden har i marts 2018 opdateret samtykkeerklæringen til udveksling af helbredsoplysninger.

Risiko 4.1: *Indhentelse af lovligt samtykke*
Når patienterne har mulighed for at samtykke til mange forskellige former for behandling af deres personoplysninger i forbindelse med indlæggelse, er der en risiko for, at patienten samtykker til former for behandling af sine personoplysninger, som den pågældende reelt ikke kan gennemskue konsekvensen af. Det kan have den konsekvens, at samtykket ikke anses for tilstrækkeligt informeret, og dermed ikke lever op til kravene i sundhedsloven og databeskyttelsesforordningen.

Det er ikke oplyst, at regionerne på trods af opdateringen af samtykkeerklæringen har iværksat øvrige procedurer eller tiltag, der tilgodeser, at patienter ofte udgør en sårbar gruppe, som ikke er i stand til at overskue konsekvenserne af et samtykke.

5.5 Overførsel af oplysninger fra parakliniske systemer

Overførsel af oplysninger fra parakliniske systemer til Sundhedsplatformen finder sted i de situationer, hvor en praktiserende læge fx anmoder om screening af en blodprøve. Denne anmodning indebærer en videregivelse af oplysninger fra én sundhedsperson (den praktiserende læge) til en anden sundhedsperson (den person, som ansvarlig for gennemførelse af den pågældende test). Den modtagende sundhedsperson er forpligtet til at journalføre sin respektive behandling af patientens helbredsoplysninger i det journalsystem, som fx anvendes på laboratoriet. Den efterfølgende integration mellem det det parakliniske system og Sundhedsplatformen skal ikke anses som en videregivelse i sundhedslovens forstand, da en elektronisk patientjournal er en samling af oplysninger om patienten fra en række patientjournaler.

Denne DPIA-proces har ikke givet anledning til yderligere bemærkninger vedrørende dette emne.

Umiddelbart vil registrering af oplysninger fra fx laboratorietests i ét yderligere IT-system (Sundhedsplatformen) indebære en forøgelse af risikoen for kompromittering af de pågældende oplysninger. Denne risiko opvejes dog af, at Sundhedsplatformen har en bedre beskyttelse af oplysningerne samtidig med, at de sundhedspersoner, som anvender Sundhedsplatformen i forbindelse med aktuel patientbehandling, ikke skal indsamle oplysningerne fra flere IT-systemer.

Risiko 5.1: *Overførsel af oplysninger fra parakliniske systemer*
Der er hverken identificeret en forøgelse eller en formindskelse af denne risiko siden den oprindelige PIA i 2016.

5.6 Oversigtsskærme

Sundhedsplatformen indeholder en funktion - den såkaldte prelogin visning - som gør det muligt at se nogle skærmbilleder uden anvendelse af individuelt brugernavn og password. De oplysninger, som fremgår af oversigtsskærme med prelogin visning, er oplysninger om patientens fornavn og forbogstav for efternavn. Det er usikkert, om oversigtsskærme i prelogin visning indeholder oplysninger om patientens fødselsdato, eller om der kun er tale om køn og alder.

Regionerne er opmærksomme på at begrænse mængden af personoplysninger på oversigtsskærme til et minimum.

I forbindelse med implementering af Sundhedsplatformen på oversigtsskærmene og opsætning af disse, viste det sig, at det ikke var praktisk muligt at logge ind med personligt brugernavn og password fra prelogin visning. De to funktioner er derfor adskilt, så der ikke er mulighed for andre funktioner end prelogin på oversigtsskærme, idet personligt login foregår på selvstændige maskiner, hvor brugeren automatisk logges af efter 3 minutters inaktivitet.

Oversigtsskærme, der viser overordnede oplysninger, er placeret på hospitalsafdelinger, fx vagtstuer, og i forbindelse med operationsstuer. Oversigtsskærme placeret på offentligt tilgængelige områder viser ikke oplysninger, som kan identificere patienter. Oversigtsskærme på hospitalsafdelinger og operationsstuer er fysisk placeret i lokaler, hvortil der kun er adgang for sundhedspersonale, så det dermed ikke er muligt for uvedkommende at få adgang til at se oplysningerne, som fremgår af skærmen. Sikkerhedsforanstaltningerne udgør skiltning, ligesom vagtstuer kan aflåses. I forbindelse med implementering af oversigtsskærme er der indført en politik for, hvordan oversigtsskærmene fysisk skal placeres og hvilke sikkerhedsforanstaltninger, der skal træffes, fx montering af et privacyfilter og skiltning.

Risiko 6.1: *Indhold på oversigtsskærme*
Risikoen vedr. visning på prelogin oversigtsskærme må vurderes at være reduceret i forhold til PIA 2016.

Risiko 6.2: *Uvedkommendes adgang til oversigtsskærme*
Skærme med personoplysninger er ikke altid placeret bag aflåste døre, men der er implementeret øgede sikkerhedstiltag (fx diskretionslinjer eller privacy screens på skærmene) med henblik på at minimere risikoen for, at uvedkommende forsætligt eller uagtsomt kan få adgang til personoplysningerne. Risikoen må derfor vurderes at være reduceret i forhold til PIA 2016

5.7 Min Sundhedsplatform (patientportalen - MyChart)

Min Sundhedsplatform (www.minsundhedsplatform.dk) er en del af Sundhedsplatformen og er en portal på internettet, hvor patienter på de hospitaler/sygehuse, som anvender Sundhedsplatformen, kan kommunikere med sundhedspersonalet, få indblik i dele af deres sundhedsoplysninger, se prøvesvar, udfylde spørgeskemaer, få adgang til egne børns sundhedsjournaler og har mulighed for at modtage påmindelser fra de afdelinger, som patienten er tilknyttet.

Min Sundhedsplatform er også tilgængelig som applikation til mobile enheder via App Store og Google Play.

Patienterne logger på "Min Sundhedsplatform" via NemID.

Forældre med forældremyndighed over børn under 15 år kan få oprettet adgang til barnets "Min Sundhedsplatform". Forældrenes adgang udløber automatisk, når barnet fylder 15 år. Det fremgår af "Vilkår og betingelser", at forældrene skal udfylde og underskrive en erklæring for at kunne tilgå "Min Sundhedsplatform" for børn over 15 år.

Patienten kan give fuldmagt til, at andre kan se den pågældendes oplysninger på "Min Sundhedsplatform". Fuldmagterne afgives på papir og underskrives i hånden ved personligt fremmøde på et hospital/sygehus og legitimering overfor sundhedspersonalet. Fuldmagten er begrænset til 1 år og skal herefter fornyes. Der arbejdes på, at fuldmagterne kan gives elektronisk og underskrives med NemID.

Via "Min Sundhedsplatform" har patienterne mulighed for at se, hvilke sundhedspersoner og fuldmagtshavere, som de seneste 180 dage har tilgået deres patientjournal på Sundhedsplatformen.

Det skal bemærkes, at bestemmelserne i dokumenterne "Vilkår og betingelser og "Datasikkerhed" er delvist overlappende.

Denne DPIA-proces har ikke givet anledning til yderligere bemærkninger vedrørende dette emne.

Risiko 7.1: *Uklarhed i vilkår for brug af Min Sundhedsplatform*
PIA 2016: Vilkårene for anvendelse af "Min Sundhedsplatform" er uklare, fordi nogle af bestemmelserne både fremgår af vilkårene og politikken vedrørende datasikkerhed samtidig med, at det ikke er klart, om forældre til børn over 15 år skal have en fuldmagt for at få adgang til barnets version af "Min Sundhedsplatform".
DPIA 2018: Det bør undersøges, om vilkårene for brugen af app'en er blevet opdateret i overensstemmelse med kravene i databeskyttelsesforordningen.

Risiko 7.2: *Min Sundhedsplatform som applikation*
Min Sundhedsplatform er gjort tilgængelig som applikation til mobile enheder via App Store og Google Play. Jo flere indgange til Sundhedsplatformen, desto større er risikoen for, at der sker et sikkerhedsbrud.

5.8 Datastrømme i Sundhedsplatformen

De overordnede datastrømme blev identificeret og kortlagt som risikotema i den oprindelige PIA fra 2016, afsnit 4.2. Der henvises til beskrivelsen under dette punkt.

Siden foretagelsen af den oprindelige PIA i 2016 er Sundhedsplatformen udbredt til samtlige hospitaler og sygehuse i Region Hovedstaden og Region Sjælland, hvilket har medført en markant stigning i datastrømmene i Sundhedsplatformen. Dette skal imidlertid sammenholdes med det forhold, at flere tidligere anvendte systemer er lukket ned, hvorfor der langt hen ad vejen er tale om ændrede datastrømme vedrørende samme forhold.

Risiko 8.1: *Overordnede datastrømme i Sundhedsplatformen*
Som det fremgår af den oprindelige PIA fra 2016 skal risikoen ved behandling af patienters personoplysninger i forbindelse med de overordnede datastrømme i Sundhedsplatformen findes i det potentielle omfang af de personoplysninger, som vil blive behandlet i Sundhedsplatformen. Den potentielle behandling af følsomme helbredsoplysninger om 2,5 mio. borgere samt om medarbejdere i Region Hovedstaden og Region Sjælland, som er tilknyttet de cirka 66.000 udstedte brugeradgange til Sundhedsplatformen, udgør i sig selv en risiko, idet et eventuelt sikkerhedsbrud vil kunne kompromittere en stor mængde datasubjekter/patienter, hvis personoplysninger tidligere var fordelt på en række andre systemer. Risikoen skal dermed ses i sammenhæng med omfanget af integrationer mellem Sundhedsplatformen og eksterne IT-systemer. Kombinationen af følsomme oplysninger og mængden af registrerede oplysninger forøger risikoen.

Sundhedsplatformens størrelse gør i sig selv, at det kan være vanskeligt for enkeltpersoner at overskue dataflowet og på denne baggrund iagttage databeskyttelsesreglerne. Det er på denne baggrund væsentligt, at der sikres metoder til løbende monitorering af behandlingsaktiviteterne. Både Region Hovedstaden og Region Sjælland har i forbindelse med databeskyttelsesforordningens ikrafttrædelse 25. maj 2018 valgt at gennemføre omfattende kortlægningsprojekter med henblik på at skabe dette overblik.

5.9 Uddannelse

Implementeringen af Sundhedsplatformen på de enkelte hospitaler og sygehuse skete over en periode i 2016-2017, hvor Sundhedsplatformen løbende blev videreudviklet med nye funktioner og forbedringer i takt med, at disse fandtes nødvendige, ligesom det var et bevidst valg fra Region Hovedstadens side, at medarbejderne først blev undervist i mere avancerede funktioner i Sundhedsplatformen, når medarbejderne havde opbygget en vis basal erfaring i brugen af systemet. Som påpeget i Rigsrevisionens Beretning om Sundhedsplatformen fra 2018 vedrørende den tidligste implementering af Sundhedsplatformen på Herlev-Gentofte Hospital har der været variationer mellem de versioner af Sundhedsplat-

formen, som medarbejderne blev undervist i, og dem, som medarbejderne sidenhen skulle anvende.

Samlet set er der i Sundhedsplatformen oprettet cirka 66.000 brugeradgange, som benyttes af de ansatte i de to regioner. Hertil ansættes hver måned knap 500 nye medarbejdere hos Region Hovedstaden og cirka 235 hos Region Sjælland. Blandt disse nyansatte udgør størstedelen sundhedsfagligt personale, hvoraf kun en delmængde i forvejen er certificeret i Sundhedsplatformen.

Derfor er der et stort behov for både grundcertificering og løbende uddannelse af de ansatte, som anvender Sundhedsplatformen.

Regionerne har iværksat flere undervisningstiltag vedrørende brugen af Sundhedsplatformen samt generel undervisning og uddannelse inden for IT-sikkerhed og behandlingen af personoplysninger.

Både Region Hovedstaden og Region Sjælland har indført uddannelseskoncepter. Koncepterne er opdelt i forskellige basis- og specialespor målrettet enkelte stillingstyper og underliggende specialeområder. Endvidere udbydes funktionskurser ad hoc på de ansattes forespørgsel.

Regionerne har derudover udgivet en række vejledninger og procedurebeskrivelser for forskellige områder af Sundhedsplatformen, som fungerer som opslagsværker for brugerne.

I foråret 2018 blev resultaterne af den gennemførte brugertilfredshedsundersøgelse på Sundhedsplatformen offentliggjort. På spørgsmålet om, hvorvidt brugerne er enige i, at der tilbydes tilfredsstillende uddannelsesmuligheder vedrørende Sundhedsplatformen, fordeler svarende sig som følger:

- 1,97 % svarede helt enige
- 11,86 % svarede overvejende enige
- 26,46 % svarede hverken enige eller uenige
- 25,31 % svarede overvejende uenige
- 22,48 % svarede helt uenige
- 11,93 % svarede ved ikke/ ikke relevant

(n = 10.719)

Besvarelserne er taget til efterretning og vil få betydning for den fremtidige uddannelsesindsats i regionerne.

Risiko 9.1: Behov for yderligere uddannelse
Konklusionerne i Rigsrevisionens rapport om den første udrulning af Sundhedsplatformen på Herlev-Gentofte Hospital samt resultaterne af den gennemførte brugerundersøgelse blandt Sundhedsplatformens brugere viser, at der har været og i hvert fald blandt en stor del af Sundhedsplatformens brugere fortsat vurderes et behov for uddannelse i anvendelsen af Sundhedsplatformen. Uddannelsesbehovet må antages at omfatte både grunduddannelse og løbende efteruddannelse.

Risiciene ved, at Sundhedsplatformen anvendes forkert grundet mangelfuld uddannelse kan bestå i manglende eller fejlagtige registreringer af betydning for datakvaliteten og patientbehandlingen, men også af betydning for IT-sikkerheden.

5.10 Fejlretning og support i EPIC

Da Sundhedsplatformen udgør det foreløbigt største IT-projekt inden for sundhedssektoren i Danmark, har et vist antal tilpasninger måttet påregnes som naturlige som led i leveringen og implementeringen af et IT-system af denne størrelse.

5.10.1 Sherlock

Rapportering af fejl og supportbehov, som ikke kan klares af Region Hovedstaden via platformen ServiceNow sker for begge regioners vedkommende til EPIC via "Sherlock", der er et værktøj, som EPIC har stillet til rådighed.

Det er primært ansatte i Systemforvaltningen, som foretager anmeldelse i Sherlock, da adgangen til Sherlock er betinget af en brugeradgang. Sundhedspersoner har derfor som udgangspunkt ikke mulighed for selvstændigt at oprette supportsager i Sherlock.

Den korrespondance og dermed behandling af personoplysninger, som finder sted via Sherlock, har været genstand for en grundig juridisk vurdering hos regionerne, herunder for at sikre at overførslen kunne ske under iagttagelse af den tidligere gældende krigsregel i persondatalovens § 41, stk. 4, hvorefter der ikke kunne ske lagring af oplysninger om en væsentlig del af den danske befolkning uden for Danmark. Herudover har regionerne sikret det nødvendige overførselsgrundlag via EU-Kommissionens standardaftale for overførsel af personoplysninger til databehandlere i usikre tredjelande, ligesom regionerne har indgået de nødvendige databehandleraftaler med EPIC.

5.10.2 Ekstern adgang til Sundhedsplatformen

Fejlrapportering og support på Sundhedsplatformen skal ikke nødvendigvis ses som to adskilte ting. En supportsag kan bestå i en anmodning, som ikke nødvendiggør adgang til systemet. Afslører en anmodning om support derimod en egentligt systemfejl, forventes det, at EPIC retter fejlen.

Når supportmedarbejdere hos EPIC har behov for adgang til Sundhedsplatformen, er det ofte i tilfælde, hvor regionerne ikke selv besidder de nødvendige kompetencer hertil, fx når der skal justeres i den bagvedlæggende programmering/kodning i Sundhedsplatformen. I implementeringsperioden har det således ofte været nødvendigt at involvere supportmedarbejdere hos EPIC.

EPIC har adgang til Sundhedsplatformen på forskellige niveauer. Overordnet sondres i den forbindelse imellem support- og produktionsmiljøet. Produktionsmiljøet indeholder oplysninger om patienter og personale, da der er tale om den version, som anvendes "live" ude på hospitalerne. Supportmiljøet er derimod et testmiljø, som skal sikre, at der ikke udføres tests i produktionsmiljøet med de drifts- og sikkerhedsmæssige risici, som dette kan indebære. Efter det oplyste er de oplysninger, som anvendes i supportmiljøet et spejl af de oplysninger, som ligger i produktionsmiljøet.

Faste supportmedarbejdere hos EPIC tildeles adgang til både produktions- og supportmiljøet. Adgangen sker fysisk fra EPIC i USA eller i England, hvorfra supportmedarbejderne kan tilgå de forskellige submiljøer.

For så vidt angår adgangen til supportmiljøet med personoplysninger på brugere og patienter, benytter regionerne EU-Kommissionens Standard Contractual Clauses for overførsel af oplysninger fra en dataansvarlig i EU (hhv. Region Hovedstaden og Region Sjælland) til en databehandler i et ikke-sikkert tredjeland (EPIC i USA) som overførselsgrundlag.

Brugerrettigheder til supportmedarbejdere tildeles af Brugeradministrationsteamet. Procedurer for tildelingen af adgang, herunder efter hvilke kriterier dette kan ske, er under udarbejdelse. Det lægges til grund, at SP Systemforvaltningen har autoriseret anmodninger, som indgår hos Brugeradministrationsteamet. Der er generelt givet adgang til de supportmedarbejdere hos EPIC, som har bedt om adgang til produktionsmiljøet.

En udskrift af 28. august 2018 viste, at 152 EPIC-medarbejdere havde adgang til både produktions- og supportmiljøet. Tallet varierer løbende i takt med gennemførelsen af revisioner af tildelte brugeradgange.

Regionerne har oplyst, at adgangen til følsomme personoplysninger generelt er et fokusområde.

Efter afslutningen af en sag markeres den som 'completed'. Der kan søges på historiske sager, men ifølge nye procedurer indført pr. 31. august 2018 vil alle personoplysninger blive slettet fra supportsagen, når opgaven er afsluttet. En supportsag markeres som afsluttet, når sagens ejere er enige herom. Denne status kan efterfølgende ændres. Den risiko, som bestod ved, at personoplysninger blev taget ud af produktionsmiljøet og sideløbende blev opbevaret på supportsagen, må efter det oplyste anses som mitigeret, forudsat at de nye procedurer også har virkning for supportsager, som allerede var afsluttet pr. 31. august 2018.

Der er udarbejdet en revisionserklæring, der er godkendt af administrationen den 16. august 2018. Ifølge regionerne viser rapporten ikke væsentlige anmærkninger. Revisionserklæringen har ikke været en del af dokumentationen i nærværende DPIA-proces.

Risiko 10.1: *Overladelse af personoplysninger til tredjelande*
Supportmedarbejdere hos EPIC i England og USA har adgang til personoplysninger på patienter og ansatte i Sundhedsplatformens produktionsmiljø. At der i USA, som databeskyttelsesretligt udgør et tredjeland, er skabt adgang til personoplysninger vedrørende danske patienter og ansatte udgør i sig selv en risiko.

Grundlaget for overførsel af personoplysninger til EPIC i USA er EU-Kommissionens Standard Contractual Clauses for overførsel af oplysninger fra en dataansvarlig i EU (hhv. Region Hovedstaden og Region Sjælland) til en databehandler i et ikke-sikkert tredjeland (EPIC i USA) (bilag 18 til aftalen med EPIC). Det fremgår af aftalens tillæg 1, at EPIC (dataimportøren) i forbindelse med implementerings-, vedligeholdelses- og supportydelser vil have adgang til relevante personoplysninger, uden at dette er nærmere konkretiseret. Det fremgår videre af aftalens tillæg 2, litra b, at EPIC's medarbejdere bl.a. kan tilgå hhv. Region Hovedstadens og Region Sjællands systemer via en site-to-site VPN.

Der er tale om et meget vagt formuleret overførselsgrundlag, som skal konkretiseres yderligere i praksis, og som ikke giver EPIC en ubetinget adgang til Sundhedsplatformen. I forbindelse med gennemførelse af nærværende DPIA har det ikke været muligt de facto at kontrollere, om EPIC's adgange er nærmere konkretiseret i forhold til adgang til de enkelte miljøer (efter det oplyste pågår et arbejde med beskrivelse af procedurer for tildeling af adgange for EPIC medarbejdere), og om EPIC overholder de betingelser for overførslen, som er fastsat i Standard Contractual Clauses (bilag 18, tillæg 2). I den forbindelse skal det understreges, at

den revisionserklæring, som er udarbejdet vedr. EPIC, ikke har været en del af nærværende DPIA, hvorfor det ikke har været muligt at inddrage forhold herfra.

Risiko 10.2: *Opfølgning på tildelte adgange til produktionsmiljøet*
Gennemgangen af brugeradgange, hvor 152 EPIC-medarbejdere – i supportøjemed – har adgang til en fuld spejlet version af personoplysninger i Sundhedsplatformen, understreger behovet for en løbende og hyppig opfølgning af tildelte brugeradgange. Det følger videre af det netop omtalte tillæg 2, at EPIC bl.a. skal kontrollere de tildelte autorisationer hver 6. måned. Det indebærer en risiko, såfremt personer, som ikke aktuelt har et behov for adgang til produktions- eller supportmiljøet i Sundhedsplatformen, ikke fratages denne adgang. Risikoen intensiveres jo større en sådan eventuel gruppe er.

Risiko 10.3: *Personoplysninger i supportmiljøet*
Det udgør en risiko, når supportmiljøet indeholder personoplysninger, fordi de indtastede data er en spejling af produktionsmiljøet. Dette ikke mindst, når der samtidig er tale om at oplysninger overføres til USA, som er et usikkert tredjeland, jf. risiko 10.1.

5.11 Opfølgning på fejlregistreringer i Sundhedsplatformen (datakvalitet)

Resultatet af brugertilfredshedsundersøgelsen, som blev offentliggjort i april 2018, viser, at 40 % af de adspurgte samlet set enten er meget utilfredse eller utilfredse med Sundhedsplatformen. På spørgsmålet om, hvorvidt den adspurgte finder Sundhedsplatformen brugervenlig, har 67 % svaret, at de enten er overvejende uenige eller helt uenige i, at Sundhedsplatformen er brugervenlig. Når mange brugere finder Sundhedsplatformen vanskelig at anvende og som beskrevet i afsnit 5.9 ikke føler sig tilstrækkeligt uddannet i brugen, kan det ikke udelukkes, at Sundhedsplatformen anvendes på en måde, som giver anledning til fejlregistreringer.

Databeskyttelsesforordningen indeholder et grundlæggende princip om datakvalitet, som har betydning i forhold til fejlregistreringer, fordi fejlregistreringer er ensbetydende med, at personoplysningerne er urigtige i forhold til de formål, hvortil de behandles.

Risiko 11.1: *Manglende procedurer for kvalitetssikring af data*
Der er ikke indført procedurer til identifikation af og opfølgning på fejlregistreringer i Sundhedsplatformen. Dette indebærer en risiko for, at der bliver behandlet urigtige personoplysninger i forhold til behandlingsformålet, så urigtige registreringer bliver lagt til grund som faktum, og at der ikke tages de rimelige skridt til at sikre, at oplysningerne ajourføres.

Som nævnt ovenfor under afsnit 5.9 kan manglende uddannelse og rutiner i anvendelsen af Sundhedsplatformen eller særlige funktioner heraf medføre, at data ikke indtastes rette sted eller slet ikke indtastes, hvilket medfører samme risiko for datakvaliteten og patientbehandlingen, så længe der ikke er indført effektive procedurer, som kan identificere eventuelle fejlregistreringer.

5.12 Beskyttelse af ansattes personoplysninger (medarbejdervinklen)

Sundhedsplatformen anvendes af ansatte bag de cirka 66.000 tildelte brugeradgange på tværs af de to regioner.

I platformen behandles personoplysninger om medarbejderen i form af navn, initialer, medarbejdernummer, titel, anciennitet, ansættelsessted, patientrelationer og muligvis cpr-nummer m.v.

Overskrider medarbejderen sine tildelte adgangsrettigheder, vil logningen heraf medføre behandlingen af oplysninger om et (muligt) strafbart forhold, ligesom eventuelle behandlingsfejl eller forsømmelser vil være registreret i tilknytning til den patient, som rammes af fejlen eller forsømmelsen.

Endelig behandles også oplysninger om medarbejderne, når de som patienter er i kontakt med hospitaler inden for Region Hovedstaden og Region Sjælland.

Risiko 12.1: *Beskyttelse af ansattes personoplysninger*
Behandlingen af personoplysninger på brugere af Sundhedsplatformen udgør en risiko på lige fod med behandlingen af personoplysninger om patienter.

Lognings- og rapporteringsværktøjer kan skabe uberettiget mistanke mod brugere grundet falske positive rapporter. Hvor en sådan mistanke ikke manes til jorden, kan den have ansættelsesretlige konsekvenser for medarbejderen, ligesom vedkommendes anseelse og omdømme kan risikere at lide skade.

En egentlig konsekvensanalyse vedrørende medarbejdervinklen i Sundhedsplatformen udarbejdes ikke i forbindelse med nærværende analyse, da regionerne har oplyst, at den udarbejdes i anden sammenhæng. Det er dog væsentligt at følge op på, at dette faktisk sker, hvilket også er baggrunden for, at risikoen er oplistet her.

6. Konsekvensanalyse (Impact Assessment)

I nærværende afsnit bliver de risici, der er identificeret ovenfor under afsnit 5 i tilknytning til de enkelte risikotemaer, afvejet i forhold til behandlingens konsekvenser for den enkeltes privatliv samt sandsynligheden for, at der sker en kompromitterende hændelse.

Hvor en identificeret risiko alene vedrører den ene region, er risikoen mærket med RH (Region Hovedstaden) eller RS (Region Sjælland)

De identificerede risici prioriteres for at skabe et overblik over områder med størst risiko for krænkelse af privatlivet, jf. ISO29134:2017, s. 17.

6.1 Afvejning af risici

Vurderingen af de risici, der blev identificeret i det foregående afsnit 5, i forhold til behandlingens konsekvenser for den enkeltes privatliv samt sandsynligheden for, at der sker en kompromitterende hændelse, er illustreret i nedenstående figur:

Privacy risiko		Sandsynlighed for kompromitterende hændelse	Konsekvens for den enkeltes privatliv
Risikotema 1 – Afsnit 5.1	Risiko 1.1: Fordeling af dataansvar	Medium*	Lav*
Risikotema 2 – Afsnit 5.2	Risiko 2.1: Udvidelse/ændring af oprindelig rettighedsmodel	Medium*	Medium
	Risiko 2.2: Adgang for kvalitetsmedarbejdere og risk managers	Lav	Lav
	Risiko 2.3: Anvendelse af funktionaliteten "Break the Glass"	Medium*	Medium*
	[redacted]	Høj	Medium
	[redacted]	Høj	Høj
		Medium	Medium

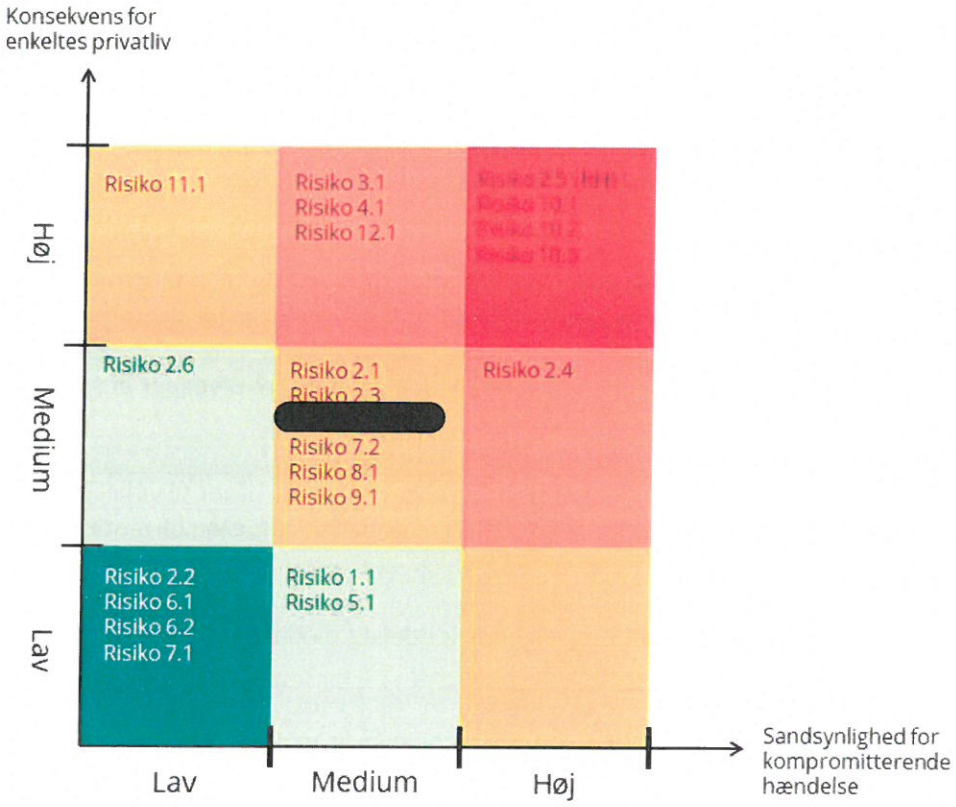
PIA 2016

	Risiko 2.6 (RH): Valg af dokumentation og format for rapportering af logkontrol (RH)	Lav*	Medium
Risikotema 3 – Afsnit 5.3	Risiko 3.1: Gamle IT-systemer i (fortsat) hel eller delvis drift	Medium*	Høj*
Risikotema 4 – Afsnit 5.4	Risiko 4.1: Indhentelse af lovligt samtykke	Medium	Høj
Risikotema 5 – Afsnit 5.5	Risiko 5.1: Overførsel af oplysninger fra paraklinisk systemer	Medium	Lav
Risikotema 6 – Afsnit 5.6	Risiko 6.1: Indhold på oversigtsskærme	Lav*	Lav*
	Risiko 6.2: Uvedkommendes adgang til oversigtsskærme	Lav*	Lav
Risikotema 7 – Afsnit 5.7	Risiko 7.1: Uklarhed i vilkår for brug af Min Sundhedsplatform	Lav	Lav
	Risiko 7.2: Min Sundhedsplatform som applikation	Medium	Medium
Risikotema 8 – Afsnit 5.8	Risiko 8.1: Overordnede datastrømme i Sundhedsplatformen	Medium	Medium
Risikotema 9 – Afsnit 5.9	Risiko 9.1: Behov for yderligere uddannelse	Medium	Medium
Risikotema 10 – Afsnit 5.10	Risiko 10.1: Overladelse af personoplysninger til tredjelande	Høj	Høj
	Risiko 10.2: Opfølgning på tildelte adgange til produktionsmiljøet	Høj	Høj
	Risiko 10.3: Personoplysninger i supportmiljøet	Høj	Høj
Risikotema 11 – Afsnit	Risiko 11.1: Manglende procedurer for kvalitetssikring af data	Lav	Høj

Risikotema 12 – Afsnit	Risiko 12.1: Beskyttelse af ansattes personoplysninger	Medium	Høj	

*Ændret risikovurdering ift. PIA 2016

6.1.1 Grafisk illustration af risikoafvejningen



De under risikotemaerne 1-12 identificerede risici er følgende:
Risiko 1.1: Fordeling af dataansvar
Risiko 2.1: Udvidelse/ændring af oprindelig rettighedsmodel
Risiko 2.2: Adgang for kvalitetsmedarbejdere og risk managers
Risiko 2.3: Anvendelse af funktionaliteten "Break the Glass"
[redacted]
Risiko 2.6 (RH): Valg af dokumentation og format for rapportering af logkontrol

Risiko 3.1: Gamle IT-systemer i (fortsat) hel eller delvis drift
Risiko 4.1: Indhentelse af lovligt samtykke
Risiko 5.1: Overførsel af oplysninger fra parakliniske systemer
Risiko 6.1: Indhold på oversigtsskærme
Risiko 6.2: Uvedkommendes adgang til oversigtsskærme
Risiko 7.1: Uklarhed i vilkår for brug af Min Sundhedsplatform
Risiko 7.2: Min Sundhedsplatform som applikation
Risiko 8.1: Overordnede datastrømme i Sundhedsplatformen
Risiko 9.1: Behov for yderligere uddannelse
Risiko 10.1: Overladelse af personoplysninger til tredjelande
Risiko 10.2: Opfølgning på tildelte adgange til produktionsmiljøet
Risiko 10.3: Personoplysninger i supportmiljøet
Risiko 11.1: Manglende procedurer for kvalitetssikring af data
Risiko 12.1: Beskyttelse af ansattes personoplysninger

I denne DPIA anvendes ovenstående risiko-matrix til at illustrere de ovennævnte identificerede risicis sandsynlighed og konsekvenser for de berørte registrerede.

I denne DPIA anvendes følgende inddeling med tre niveauer af sandsynlighed:

Sandsynlighed	**Beskrivelse**
Lav	Det er usandsynligt, at truslen bliver til virkelighed.
Medium	Der er en rimelig chance for, at truslen bliver til virkelighed.
Høj	Det er sandsynligt, at truslen bliver til virkelighed.

I denne DPIA anvendes følgende inddeling med tre niveauer af konsekvenser:

Konsekvens	**Beskrivelse**
Lav	Personer kan opleve få mindre ulemper, som de kan overkomme uden større indsats (tid brugt på at genindtaste oplysninger, dårlig brugeroplevelse, irritation og lignende)
Medium	Personer kan opleve betydelige ulemper, som de kan overkomme med få besværligheder (ekstra udgifter, manglende adgang til forretningsservice, frygt, mangel på forståelse, stress, mindre fysiske lidelser).
Høj	Personer kan opleve betydelige konsekvenser, som de kun kan overkomme med alvorlige vanskeligheder (økonomiske konsekvenser, fejlkontering af midler, sortlistning eller nedgradering i kreditmuligheder, fysisk skade på aktiver, påvirkning af arbejdssituation, stævning, dårligere helbred og lig-

	nende).

6.2 Prioritering af risici med størst risiko for krænkelse af privatlivet

Nedenstående oversigt er udtryk for en prioritering af de identificerede risici i Sundhedsplatformen, som indebærer den største risiko for krænkelse af privatlivet for de personer, som får deres personoplysninger behandlet i Sundhedsplatformen. Oversigten medtager ikke risici, som i afsnit 6.1 er vurderet til at have en lav sandsynlighed for en kompromitterende hændelse kombineret med en lav konsekvens for den enkeltes privatliv (matrixens mørkegrønne felt), hvorfor listen kun indeholder 18 prioriterede risici i forhold til de 22 identificerede risici.

1. Risiko 2.5 (RH): Metode for gennemgang af log
2. Risiko 10.1: Overladelse af personoplysninger til tredjelande
3. Risiko 10.2: Opfølgning på tildelte adgange til produktionsmiljøet
4. Risiko 10.3: Personoplysninger i supportmiljøet
5. [redacted]
6. Risiko 3.1: Gamle IT-systemer i (fortsat) hel eller delvis drift
7. Risiko 4.1: Indhentelse af lovligt samtykke
8. Risiko 12.1: Beskyttelse af ansattes personoplysninger
9. Risiko 11.1: Manglende procedurer for kvalitetssikring af data
10. Risiko 2.1: Udvidelse/ændring af oprindelig rettighedsmodel
11. Risiko 2.3: Anvendelse af funktionaliteten "Break the Glass"
12. [redacted]
13. Risiko 7.2: Min Sundhedsplatform som applikation
14. Risiko 8.1: Overordnede datastrømme i Sundhedsplatformen
15. Risiko 9.1: Behov for yderligere uddannelse
16. Risiko 2.6 (RH): Valg af dokumentation og format for rapportering af logkontrol
17. Risiko 1.1: Fordeling af dataansvar
18. Risiko 5.1: Overførsel af oplysninger fra parakliniske systemer

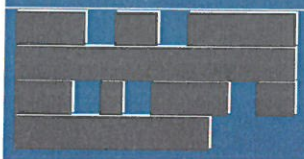
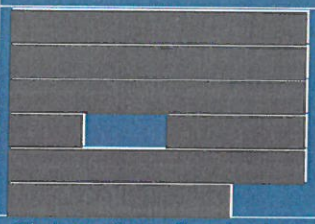
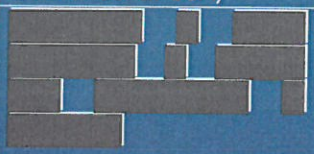
7. Evaluering af risici og beskrivelse af foranstaltninger, der imødegår disse

Denne fase består af risk management med henblik på den nødvendige reduktion af privacy-risikoen tilknyttet de i forrige afsnit prioriterede risici.

Risk management skal følges op af en drøftelse mellem Sundhedsplatformen og Bech-Bruun med en vurdering af, hvad der er det acceptable niveau for den residual-risiko, som ikke umiddelbart kan reduceres i første omgang.

Nedenstående anbefalinger baserer sig på de drøftelser, der har været mellem regionerne og Bech-Bruun. Regionerne anbefales at søge særskilt rådgivning vedrørende implementeringen af risikomitigerende foranstaltninger, ligesom yderligere og alternative foranstaltninger blandt andet fremgår af den internationale ISO 29151:2017, hvortil Datatilsynet henviser i sin DPIA-vejledning.

DPIA 2018: Privacy-risiko	**DPIA 2018: Anbefalede mitigerende foranstaltninger**	**Implikationer for Sundhedsplatformen**	**Igangsatte mitigerende handlinger**
Risiko 2.5 (Region Hovedstaden): Metode for gennemgang af log	Et større antal logs skal gennemgås i forbindelse med stikprøvekontrol. Konstatering af uregelmæssigheder skal følges op af follow-up checks eller øgede kontrolbesøg i en efterfølgende, afgrænset periode.	Generering af øgede ressourcer til arbejde med gennemførelse af stikprøvekontrol. Alternativt overvejelser om IT-system til overvågning af mistænkelig adfærd.	Region Hovedstaden overvejer anskaffelsen af et system svarende til det, som Region Sjælland har indført.
Risiko 10.1: Overladelse af personoplysninger til tredjelande	Overførselsgrundlaget og instruksen til EPIC skal konkretiseres yderligere, så der er en tydelig beskrivelse af, hvilke miljøer den enkelte EPIC-medarbejder har adgang til.	Vurdering af øvrige muligheder for support og fejlretning.	Regionerne har foretaget en grundig juridisk vurdering vedrørende Sherlock.
Risiko 10.2: Opfølgning på tildelte adgange til produktionsmiljøet	Hyppigere opfølgning på tildelte adgange til produktionsmiljøet.	Risikoen for EPIC-medarbejderes uberettigede adgang til helbredsoplysninger om danskere stiger i de situationer, hvor der gives adgang til flere personer	

DPIA 2018: Privacy-risiko	DPIA 2018: Anbefalede mitigerende foranstaltninger	Implikationer for Sundhedsplatformen	Igangsatte mitigerende handlinger
		end absolut nødvendigt.	
Risiko 10.3: Personoplysninger i supportmiljøet	Nedlukning for fuldstændig spejling af oplysninger fra produktions- til supportmiljø.	Øget for manglende compliance med databeskyttelsesforordningen, når oplysninger spejles til supportmiljøet (i kombination med overførsel til USA)	
			
Risiko 3.1: Gamle IT-systemer i (fortsat) hel eller delvis drift	Sikring af at alle planlagte typer af data konverteres fra de tidligere anvendte IT-systemer til Sundhedsplatformen. Prioritering af effektive løsninger til sunsetting af tidligere anvendte IT-systemer, herunder foranstaltninger i form af tilstrækkelige sikkerhedsforanstaltninger og sikring af datakvaliteten i overgangsfasen fra det "gamle" IT-system til Sundhedsplatformen.	Allokering af ressourcer så det sikres, at alle de planlagte typer af data fremadrettet konverteres fra de "gamle" IT-systemer til Sundhedsplatformen.	Region Hovedstaden udarbejder sunsettingprojekter for hvert system. Region Sjælland har indgået aftale med en ekstern leverandør om en samlet sunsettingløsning.
Risiko 4.1: Indhentelse af lovligt samtykke	Sikring af at de sundhedspersoner, som indhenter patienternes samtykke til yderligere	Iværksættelse af og dokumentation for træning/test af de relevante sundhedspersoner. Det	Region Hovedstaden har i marts 2018 opdateret sin samtykkeerklæring.

DPIA 2018: Privacy-risiko	DPIA 2018: Anbefalede mitigerende foranstaltninger	Implikationer for Sundhedsplatformen	Igangsatte mitigerende handlinger
	behandling af deres oplysninger, konkret informerer patienterne om konsekvenser af samtykke i tilstrækkeligt omfang inden afgivelse	vil være hensigtsmæssigt, at de relevante sundhedspersoner gennemgår et e-læringsmodul én gang årligt.	
Risiko 12.1: Beskyttelse af ansattes personoplysninger	Gennemførelse af DPIA målrettet behandlingen af personoplysninger om brugere af Sundhedsplatformen.	Ansatte, der anvender Sundhedsplatformen i deres daglige arbejde er også registrerede i persondataretlig forstand og skal beskyttes som sådan.	
Risiko 11.1: Manglende procedurer for kvalitetssikring af data	Der bør indføres procedurer, som sikrer, at antallet af fejlregistreringer reduceres, så princippet om datakvalitet overholdes.	Behandling af personoplysninger på Sundhedsplatformen sker ikke i overensstemmelse med princippet om datakvalitet, når der er et højt antal fejlregistreringer.	
Risiko 2.1: Udvidelse/ændring af oprindelig rettighedsmodel	Gennemførelse af kontrol så det sikres, at justeringer i adgange ikke påvirker den oprindelige rettighedsmodel	Udpegning af arbejdsgruppe, som har ansvar for gennemførelse af kontrollen	
Risiko 2.3: Anvendelse af funktionaliteten "Break the Glass"	[redacted]	Funktionaliteten "Break the Glass" er fornuftigt ud fra et persondataretligt perspektiv, men det skal sikres, at funktionaliteten indstilles forholdsmæssigt i forhold til rettighedstildelingen.	
[redacted]	[redacted]	[redacted]	

DPIA 2018: Privacy-risiko	DPIA 2018: Anbefalede mitigerende foranstaltninger	Implikationer for Sundhedsplatformen	Igangsatte mitigerende handlinger
Risiko 7.2: Min Sundhedsplatform som applikation	Sikring af effektive foranstaltninger til opdatering af applikationer, så risiko for kompromitering af personoplysninger mindskes ved inddragelse af eksterne leverandører.	Når Sundhedsplatformen flyttes ud på flere platforme, som regionerne har mindre kontrol over, stiger kompromiteringsrisikoen.	
Risiko 8.1: Overordnede datastrømme i Sundhedsplatformen	Sikring af tilstrækkelig dokumentation af de komplicerede datastrømme i Sundhedsplatformen	Planlægning og efterfølgende igangsætning af proces, som sikrer, at der udarbejdes en dækkende dokumentation for datastrømmene i Sundhedsplatformen inkl. integrationer til andre IT-systemer	Region Sjælland har udført en generel analyse af dataflowet. Region Hovedstaden forventer sin analyse af dataflowet afsluttet i efteråret 2018.
Risiko 9.1: Behov for yderligere uddannelse	Intensivering af uddannelsesindsatsen med fokus på grund- og efteruddannelse.	Fejlindtastninger og manglende indtastninger øger risikoen for manglende overholdelse af princippet om datakvalitet.	Regionerne har gennemført en brugertilfredshedsundersøgelse samt indført nye uddannelseskoncepter.
Risiko 2.6 (Region Hovedstaden): Valg af dokumentation og format for rapportering af logkontrol	Beslutning om model for dokumentation og format for rapportering vedrørende kontrol af log.	Uddybning af kontrolinstruks vedrørende intern gennemgang af logoplysninger	
Risiko 1.1: Fordeling af dataansvar	Via bestemmelser i regionernes aftale om fælles dataansvar skal der sikres den bedst mulige beskyttelse af patienter og medarbejderes oplysninger	Det påbegyndte arbejde med etablering af fælles dataansvar i Sundhedsplatformen fortsættes med særligt fokus på sikring af de registreredes rettigheder	Udfyldes af CIMT/KIT

DPIA 2018: Privacy-risiko	DPIA 2018: Anbefalede mitigerende foranstaltninger	Implikationer for Sundhedsplatformen	Igangsatte mitigerende handlinger
Risiko 5.1: Overførsel af oplysninger fra parakliniske systemer	Øget opmærksomhed omkring det forhold at oplysningerne er registreret flere steder	Udarbejdelse for procedure for overførsel af oplysninger fra parakliniske systemer til Sundhedsplatformen (hænger sammen med datastrømme)	Udfyldes af CIMT/KIT

8. Afsluttende bemærkninger

8.1 Accepteret residualrisiko/restrisiko

Regionerne iværksætter på baggrund af de identificerede risici foranstaltninger med henblik på at mitigere de påpegede risici. I det omfang de identificerede risici ikke kan nedbringes til et minimum, skal regionerne forholde sig til, hvorvidt denne resterende risiko (residualrisikoen) kan forsvares uden omlægning af behandlingen, og om Datatilsynet skal høres ifølge databeskyttelsesforordningens artikel 36 som beskrevet under afsnit 2.

8.2 Offentliggørelse af konsekvensanalysen

Region Hovedstaden og Region Sjælland beslutter sammen, i hvilket omfang resultatet af denne konsekvensanalyse publiceres for offentligheden.

Konsekvensanalysen vil som udgangspunkt være omfattet af den aktindsigt, som kan meddeles i medfør af offentlighedsloven.

8.3 Opfølgende DPIA

Da Region Hovedstaden og Region Sjælland fortsat indhøster erfaringer med Sundhedsplatformen og i den sammenhæng løbende foretager forbedringer og udvikling af Sundhedsplatformen, anbefaler Bech-Bruun, at der senest i 2020 gennemføres en fornyet DPIA-proces med henblik på opfølgning af de i denne DPIA identificerede risici samt en analyse af eventuelt nye.