Region Hovedstaden
Center for It, Medico og Telefoni

DPIA 2018 Sundhedsplatformen

Baggrund og status
Epic supportadgange til Sundhedsplatformen, logopfølgning m.m.

SP Dialogforum

Vicedirektør Pia Kopke

Hvad er en DPIA?

- En DPIA (Data Protection Impact Assessment) udarbejdes i forbindelse med indførelse af nye eller væsentlige ændringer af systemer, der behandler persondata. Det sker i relation til Sundhedsplatformen ligesom for alle andre systemer
- Kravet om gennemførelse af DPIA blev introduceret med EU forordningen (GDPR) 25. maj 2018
- Regionerne fik lavet en PIA på Sundhedsplatformen i 2016 og en DPIA i 2018
- Regionerne bestiller og betaler selv for at få lavet DPIA'erne som en del af det samlede interne tilsyn
- Når vi arbejder med risici vedrørende persondatabeskyttelse eller informationssikkerhed sigter vi mod at reducere risici til et fornuftigt niveau – det er ikke et mål at fjerne enhver risiko, fordi dette i mange tilfælde ville kræve, at vi helt nedlægger digitale arbejdsgange eller pålægger vores brugere helt urimelige begrænsninger i deres tilgang til de digitale værktøjer

Når ledelsen skal fastlægge en strategi for risikohåndteringen skal følgende hensyn tilgodeses og balanceres:

- Regionens samlede informationssikkerhed
- Kvalitet i patientbehandling eller anden kerneforretning
- Økonomi og ressourcer
- Effektivitet i opgaveløsningen

Region Hovedstadens Informationssikkerhedspolitik

Epic medarbejderes adgange

»Meget, meget problematisk«: Danske patientdata ender i USA

It-medarbejdere i USA har adgang til alle patientjournaler fra Sundhedsplatformen. Myndighederne har svigtet, mener eksperter.

Politiker efter ny sag om Sundhedsplatformen: »Hvad i alverden laver mine sundhedsoplysninger et mystisk sted i USA?«

Fem partier kritiserer, at danske patienters sundhedsdata kan tilgås fra USA, og kræver handling fra den kommende sundhedsminister.

- **FAKTA**
- Data ligger i Danmark i de to regionernes egne datacentre og ejes af Region Hovedstaden og Region Sjælland
- Amerikanske myndigheder kan ikke tilgå danske sundhedsdata i regionernes datacentre
- Et begrænset antal epic-medarbejdere kan på anmodning fra danske supportmedarbejdere *tilgå* oplysninger med henblik på at assistere i en konkret support sag
- Epic-medarbejderne er underlagt de samme regler som alle andre og er reguleret af både en EU standardkontrakt og en databehandleraftale. Al færden i Sundhedsplatformen logges.
- Epic skal årligt undergå en gennemgribende kontrol af et eksternt revisionsfirma og levere en revisionserklæring efter internationale standarder til regionerne

Opfølgning på sundhedspersonalets opslag

Dybt uansvarligt:
Sundhedspersonale kan uopdaget snage i patienternes data i hovedstaden

»Jeg ved, at der er nogle, der logger ind og kigger på operationsprogrammet for at finde kendte mennesker«

Patienter er ikke tilstrækkeligt beskyttet mod snagen i deres privatliv, når de er indlagt på et hospital i hovedstaden, vurderer eksperter. Region Hovedstaden erkender utilstrækkelig kontrol.

- **FAKTA**
- I Region Hovedstaden har vi implementeret logning af al adgang til patientjournaler og dertil en manuel stikprøvekontrol, hvor afdelinger i regionen udtages til kontrol mindst én gang årligt
- I forhold til den automatiserede logopfølgning har vi fulgt erfaringerne fra Region Sjælland tæt og er nu klar til at implementere
- Vi har valgt at køre en grundig intern proces, hvor medarbejderne varsles og samarbejdsorganisationerne inddrages
- De første lograpporter baseret på den automatiserede logopfølgning vil blive udsendt til hospitalerne primo oktober

Samlede risici fra DPIA 2018

Overblik: Her er Sundhedsplatformens 13 største trusler mod privatlivet - plus en hemmelig

Advokatfirma har gennemgået truslerne mod privatlivet under Sundhedsplatformen.

- **FAKTA**
- Den hemmelige risiko vedrører de konkrete kontroller der er indgår i den manuelle logopfølgning. Teksten er undtaget af hensyn til ikke at svække de kontroller, der gennemføres

- Regionerne bestiller og betaler selv for at få lavet DPIA'erne som en del af det samlede interne tilsyn. De identificerede risici vurderes og prioriteres af ledelsen og der udarbejdes på denne baggrund endeligt DPIA risikobillede
- På baggrund af det samlede risikobillede prioriteres aktiviteter til håndtering i regi af en samlet handlingsplan for informationssikkerhed på Sundhedsplatformen
- Handlingsplanen følges tæt og rapporteres til Strategisk Driftsledelse (SDL) som en del af den faste ledelsesrapportering om informationssikkerhed i Sundhedsplatformen
- Handlingsplanen drives af regionernes forum for informationssikkerhed- og persondatabeskyttelse i Sundhedsplatformen (FIPS) som referer til SDL

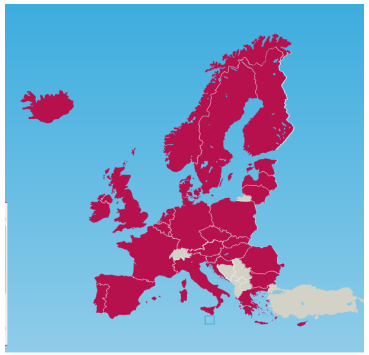
Hvad er Datatilsynets rolle?

- Administrationen er ikke bekendt med, at Datatilsynet har startet en sag om epic medarbejdernes supportadgang til Sundhedsplatformen
- Datatilsynet gennemførte i oktober 2018 et almindeligt tilsyn på Sundhedsplatformen.
- Tilsynet blev gennemført i begge regioner og vedrørte blandt mange emner også rammerne for samarbejdet med Epic, herunder det forhold at Epic er en leverandør fra et tredjeland
- Regionerne afventer fortsat den afsluttende rapport fra Datatilsynet

Tidslinje

- 2018.10.16: Regionerne modtager den samlede DPIA 2018 rapport fra Bech-Bruun
- 2018.10.24: Strategisk Driftsledelse (SDL) behandler DPIA 2018 første gang
- 2018.10.29: Datatilsynet gennemfører tilsynsbesøg i Region Hovedstaden
- 2018.10.31: Datatilsynet gennemfører tilsynsbesøg i Region Sjælland
- 2018.11.15: Strategisk Driftsledelse (SDL) godkender (skriftligt) endeligt risikobillede
- 2018.12.12: SDL godkender samlet handlingsplan for informationssikkerhed 2019
- 2019.03.01: SP Bestyrelsen orienteres om DPIA 2018
- 2019.03.21: Strategisk Driftsledelse (SDL) modtager status via den faste ledelsesrapportering

Hvad er op og ned i forhold til tredjelande?



- Når en leverandører udenfor EU behandler personoplysninger på vegne af den dataansvarlige skal en række forhold være opfyldt
- Med GDPR (EU forordningen) introduceredes nye krav til den instruks, der indgår i databehandleraftalen (tidligere baseret på sikkerhedsbekendtgørelsen)

EU STANDARDKONTRAK

DATABEHANDLERAFTALE

KONTROL MED DATABEHANDLER

EU standardkontrakt og databehandleraftale underskrives	Epic leverer den første eksterne revisionserklæring udarbejdet af PWC	GDPR EU forordningen træder i kraft	DPIA 2018 modtages	Datatilsynet Gennemfører tilsynsbesøg	Epic leverer den anden eksterne revisionserklæring udarbejdet af PWC	Revideret databehandleraftale sendes til Epic
Maj 2016	23 maj 2018	25. maj 2018	Oktober 2018	Oktober 2018	Maj 2019	Juni 2019

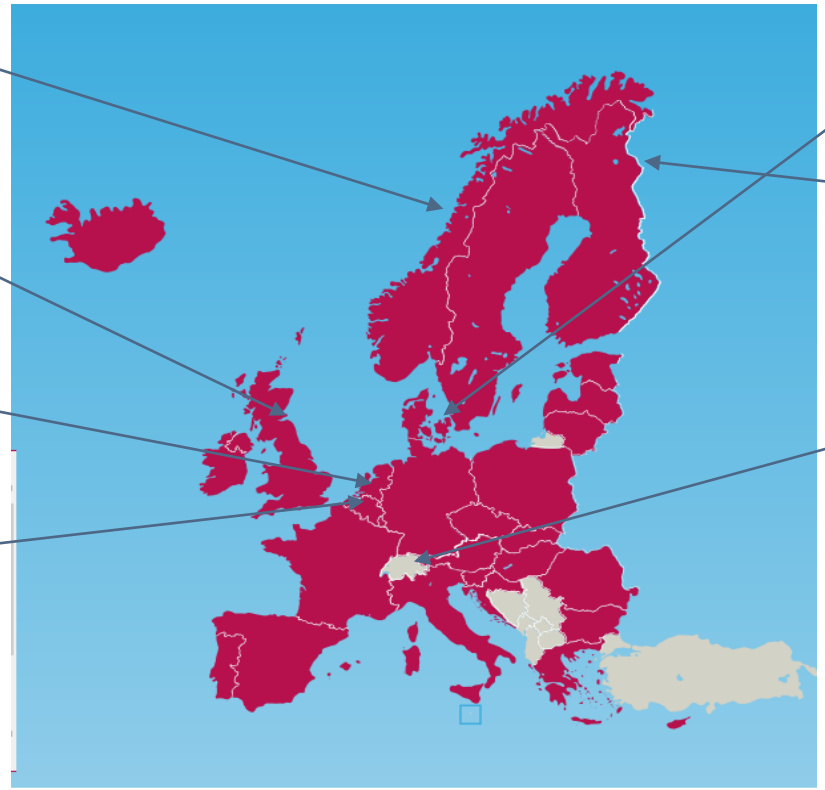
Epic’s europæiske samarbejder

Norge

Storbritannien

Holland

Belgien



Danmark

Finland

Schweiz

Røde risici i DPIA 2018

RISIKO

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.
[…] 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.

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.

AKTION OG STATUS

- Med indførelsen af EU's databeskyttelsesforordning (GDPR) udgik "sikkerhedsbekendtgørelsen," som tidligere udgjorde grundlaget for den instruks, der gives til en databehandler sammen med selve databehandleraftalen
- Samtidig blev der indført krav om mere risikobaserede instrukser, der er målrettet den konkrete databehandler

- SDL har på denne baggrund igangsat en konkretisering af den eksisterende databehandleraftale med Epic

- Den konkretiserede databehandleraftale er planlagt afsendt til Epic i juni og forventes underskrevet snarest

Røde risici i DPIA 2018

RISIKO

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.

AKTION OG STATUS

- Før DPIA 2018 skulle EPIC hver 6. måned kontrollere de tildelte autorisationer (supportadgange)
- Herudover gennemgik regionerne årligt epic-medarbejdernes adgange
- På baggrund af DPIA 2018 har SDL strammet op på proceduren for Epic's medarbejderes adgang. Epic medarbejderne får nu tildelt adgang for 3 måneder ad gangen og deres adgang lukkes automatisk, hvis ikke både regionerne og Epic aktivt har bekræftet at medarbejderen forsat skal have adgang

Røde risici i DPIA 2018

RISIKO

Risiko 2.5: Metode for gennemgang af log
Som det fremgår af den oprindelige PIA fra 2016, skal det for Region Hovedstadens vedkommende gentages, at en stikprøvestørrelse på 10 stk. pr. afdeling pr. år må karakteriseres som så lav, at det må anses for tvivlsomt, om dette alene kan anses som en egentlig kvalitativ gennemgang af loggen. […] De få stikprøver skal ses i sammenhæng med den meget lave sandsynlighed for, at en sundhedsperson, der udelukkende tilgår patienter, som vedkommende ikke har en aktuel behandlingsrelation til inden for den pågældendes autorisation (fx hospitalet/afdelingen), vil blive udtrukket i en stikprøvekontrol bestående af så få stikprøver.

AKTION OG STATUS

- Region Hovedstaden er enig i at den manuelle stikprøvekontrol er utilstrækkelig og havde allerede før DPIA 2018 igangsat forberedelserne til implementering af et automatiseret logopfølgningssystem
- Det automatiserede logopfølgningssystem er pt. ved at blive teknisk implementeret og vil fra starten af oktober sende de første rapporter ud
- Region Hovedstadens administration har valgt at køre en grundig internt proces, hvor medarbejdere bliver varslet og samarbejdsorganisationerne er inddraget