Region Hovedstaden

**Center for It, Medico og Telefoni**

**POLITIKERSPØRGSMÅL**

Journal-nr.: 19043614

Ref.: Katrine Fejerskov Kirkegaard / Berit Nielsen

Dato: 14. august 2019

Spørgsmål nr.: 074-19
Dato: 2. juli 2019
Stillet af: Jacob Rosenberg (I)
Besvarelse udsendt den: 14. august 2019

# Politikerspørgsmål vedr. patient-data i Sundhedsplatformen

**Spørgsmål:**
I lyset af den aktuelle sag i medierne om adgang for amerikanske support-medarbejdere til patientdata i Sundhedsplatformen har jeg følgende spørgsmål:

1. Det er som udgangspunkt ikke tilladt for en dansk sundhedsperson at tilgå en patientjournal for en patient, som man ikke har behandlingsansvar for. Hvis dette forekommer, får patienten besked, og det kan få konsekvenser for den pågældende sundhedsperson. Når en Epic supportmedarbejder i USA åbner en journal for en dansk patient, får patienten ikke besked. Hvorfor får en dansk patient ikke besked, når deres journal tilgås af en udenlandsk medarbejder hos Epic?

2. Rapporten fra Bech-Bruun dateret oktober 2018 indeholder flere anbefalinger til, hvordan en række alvorlige sikkerhedsbrister i Sundhedsplatformen kan løses. Hvilke konkrete initiativer har Regionen iværksat indenfor hver af disse anbefalinger, og hvad er tidsplanen for, at samtlige anbefalinger bliver imødekommet?

3. Medarbejdere hos Epic i USA har og har haft adgang til individuelle patienters ikke-anonymiserede sundhedsdata i Sundhedsplatformen. Kan Region Hovedstaden dokumentere, at data ikke er eller har været gemt på lokale computere eller lokale servere i USA?

4. Kan Region Hovedstaden dokumentere præcist hvilke patienters data, som har været synlige for medarbejdere hos Epic i USA? Dvs. bliver adgangen logget, ligesom den bliver for sundhedsmedarbejdere i Danmark?

5. Kan Region Hovedstaden dokumentere præcist hvem, der har haft adgang til data i USA og hvornår?

6. Kan Region Hovedstaden dokumentere, at man fra USA kun har haft adgang til præcis de data, som er nødvendige og tilstrækkelige for supportformålet?

7. Indeholder supportmiljøet en fuld spejling af produktionsmiljøet, og ligger denne spejling fysisk på regionens servere i Danmark?

8. Har regionen kendskab til, hvorvidt den fulde spejling på noget tidspunkt har været lagret på lokale installationer hos EPIC i USA?

9. Når medarbejdere hos EPIC i USA har logget på Sundhedsplatformen, eksempelvis med lægerettigheder, har det så givet mulighed for adgang til patientdata i andre databaser og derved til patientdata fra andre regioner? Det kan for eksempel være røntgen, laboratorie, medicin, kvalitetsdata og lignende.

10. Det fremgår af en artikel i Politiken (https://politiken.dk/indland/art7267850/Men-firma-bag-Sundhedsplatformen-er-ikke-EU-certificeret), at Epic ikke er med i den såkaldte ”Privacy Shield” ordning. Privacy Shield-ordningen pålægger amerikanske virksomheder nogle pligter, som ikke følger af amerikansk lovgivning, og giver samtidig mulighed for at tage retlige skridt mod de virksomheder, som bryder aftalen. Har Region Hovedstaden tænkt sig at kræve Epic’s deltagelse i Privacy Shield-ordningen?

**Svar:**
**1. Det er som udgangspunkt ikke tilladt for en dansk sundhedsperson at tilgå en patientjournal for en patient, som man ikke har behandlingsansvar for. Hvis dette forekommer, får patienten besked, og det kan få konsekvenser for den pågældende sundhedsperson. Når en Epic supportmedarbejder i USA åbner en journal for en dansk patient, får patienten ikke besked. Hvorfor får en dansk patient ikke besked, når deres journal tilgås af en udenlandsk medarbejder hos Epic?**
**Ad 1)** Alle opslag i Sundhedsplatformen logges og der gennemføres systematisk kontrol af alle opslag. Er der foretaget opslag i en patientjournal af en sundhedsperson uden umiddelbar behandlerrelation sendes lograpporter til den ansvarlige ledelse, som herefter gennemgår opslagene og vurderer, om

der har været et sagligt, arbejdsrelateret formål med opslaget. Hvis det viser sig, at en medarbejder har lavet et opslag uden et sagligt, arbejdsrelateret formål, vil den ansvarlige ledelse konkret vurdere sagen, fastlægge eventuelle sanktioner og indberette hændelsen som et brud på persondatasikkerheden. Først i håndteringen af brud på persondatasikkerheden fastlægges der ud fra en konkret risikovurdering, om det uberettigede opslag skal indberettes til Datatilsynet og om den pågældende patient skal underrettes. Patienten får således kun besked om et uberettiget opslag foretaget af en sundhedsperson i tilfælde, hvor det vurderes at være en risiko for patienten.

Det samme gør sig gældende, hvis opslaget er foretaget af Epic-medarbejdere i USA.

**2. Rapporten fra Bech-Bruun dateret oktober 2018 indeholder flere anbefalinger til, hvordan en række alvorlige sikkerhedsbrister i Sundhedsplatformen kan løses. Hvilke konkrete initiativer har Regionen iværksat indenfor hver af disse anbefalinger, og hvad er tidsplanen for, at samtlige anbefalinger bliver imødekommet?**
**Ad 2)** Administrationen vil understrege, at rapporten påpeger *risici* for, at der kan indtræffe alvorlige sikkerhedsbrister. Der er således ikke sket sikkerhedsbrister.
Som led i det løbende arbejde med udvikling af informationssikkerheden på Sundhedsplatformen, udarbejdes der årligt en samlet og strategisk prioriteret handlingsplan for de større udviklingsaktiviteter, der skal gennemføres i det kommende kalenderår. Handlingsplanen for 2019 har især fokus på håndteringen af risici identificeret i Bech-Bruuns Data Protection Impact Assesment (DPIA) for Sundhedsplatformen fra 2018. Handlingsplanen drives af regionernes Forum for Informationssikkerhed for Sundhedsplatformen, som drøfter handlingsplanen som fast punkt på deres møder.

Administrationen har via handlingsplanen igangsat 9 konkrete initiativer, som udspringer af DPIA 2018, for at sikre håndtering af konkrete risici. Et af disse initiativer er allerede afsluttet, og de øvrige forventes afsluttet i henholdsvis tredje og fjerde kvartal 2019 og første kvartal 2020.

**3. Medarbejdere hos Epic i USA har og har haft adgang til individuelle patienters ikke-anonymiserede sundhedsdata i Sundhedsplatformen. Kan Region Hovedstaden dokumentere, at data ikke er eller har været gemt på lokale computere eller lokale servere i USA?**
**Ad 3)** I den gældende sikkerhedsinstruks står der angivet, at ”*dataimportøren og dataeksportøren skal samarbejde med henblik på at begrænse mængden af personoplysninger, som af dataimportøren kopieres, lagres eller udskrives uden for dataeksportøens systemer, til det minimalt nødvendige for, at dataimportøren kan levere ydelser til dataeksportøren.”*

Dokumentation af, at Epic handler i overensstemmelse med sikkerhedsinstruksen foretages via de årlige revisionserklæringer, som Epic er forpligtet til at levere.
Administrationen modtog den seneste revisionserklæring fra Epic den 16. maj 2019. Revisionserklæringen blev godkendt uden anmærkninger af administrationen den 12. juni 2019.
Administrationen har ikke anledning til at tro, at Epic ikke behandler data i Sundhedsplatformen korrekt og i overensstemmelse med de kontraktuelle krav.

**4. Kan Region Hovedstaden dokumentere præcist hvilke patienters data, som har været synlige for medarbejdere hos Epic i USA? Dvs. bliver adgangen logget, ligesom den bliver for sundhedsmedarbejdere i Danmark?**
**Ad 4)** Alle adgange og opslag logges i Sundhedsplatformen. Dette gælder både for Epic-medarbejdere i USA, interne support-medarbejdere og sundhedspersoner i Danmark. Derfor er datagrundlaget for at gennemgå og følge op på, hvem der har haft adgang til patienternes journal altid til stede.

**5. Kan Region Hovedstaden dokumentere præcist hvem, der har haft adgang til data i USA og hvornår?**
**Ad 5)** Her henviser administrationen til svar på spørgsmål 4. Administrationen skal understrege, at data ikke ligger i USA, men i de to regioners datacentre, som ejes af hhv. Region Hovedstaden og Region Sjælland.

**6. Kan Region Hovedstaden dokumentere, at man fra USA kun har haft adgang til præcis de data, som er nødvendige og tilstrækkelige for supportformålet?**
**Ad 6)** Administrationen udfører i dag logopfølgning på Epic-medarbejderes opslag som en manuel procedure baseret på stikprøvekontroller. Stikprøvekontrollen udføres fire gange årligt. Metoden er tilsvarende den, som administrationen hidtil har brugt i udførslen af manuel logopfølgning på hospitalerne.

**7. Indeholder supportmiljøet en fuld spejling af produktionsmiljøet, og ligger denne spejling fysisk på regionens servere i Danmark?**
**Ad 7)** Ja, supportmiljøet er en kopi af data fra produktionsmiljøet. Supportmiljøet er fysisk placeret på servere i Region Sjælland og Region Hovedstaden.

**8. Har regionen kendskab til, hvorvidt den fulde spejling på noget tidspunkt har været lagret på lokale installationer hos EPIC i USA?**
**Ad 8)** Administrationen henviser her til svar på spørgsmål 3.

**9. Når medarbejdere hos EPIC i USA har logget på Sundhedsplatformen, eksempelvis med lægerettigheder, har det så givet mulighed for adgang**

**til patientdata i andre databaser og derved til patientdata fra andre regioner? Det kan for eksempel være røntgen, laboratorie, medicin, kvalitetsdata og lignende.**
**Ad 9)** Når en Epic medarbejder logger på Sundhedsplatformen i Danmark er det med et personligt bruger-id, der rettighedsmæssigt giver en administratoradgang, der som udgangspunkt giver adgang til supportmiljøet.
Epic medarbejdere har ikke mulighed for at tilgå andre data end de data, der ligger i Sundhedsplatformen, og de har derfor heller ikke adgang til patientdata i andre databaser, herunder patientdata fra andre regioner.

**10. Det fremgår af en artikel i Politiken (https://politiken.dk/indland/art7267850/Men-firma-bag-Sundhedsplatformen-er-ikke-EU-certificeret), at Epic ikke er med i den såkaldte "Privacy Shield" ordning. Privacy Shield-ordningen pålægger amerikanske virksomheder nogle pligter, som ikke følger af amerikansk lovgivning, og giver samtidig mulighed for at tage retlige skridt mod de virksomheder, som bryder aftalen. Har Region Hovedstaden tænkt sig at kræve Epic's deltagelse i Privacy Shield-ordningen?**
**Ad 10)** Privacy Shield-ordningen er en ordning, som virksomheder kan melde sig til og fra uden varsel. Der er tale om nogle meget uklare rammer, som ikke har været testet lovgivningsmæssigt, og det har derfor ikke været en ordning, der har spillet en rolle i de to regioners overvejelser.

Det er vigtigt at understrege, at data ligger i Danmark og ejes af de to regioner – ikke af Epic og ikke i USA. Region Hovedstaden er enige i, at ethvert tredjelands adgang til personoplysninger er en juridisk overførsel af data og udgør en risiko som skal håndteres fornuftigt og reguleres gennem EU standardkontrakter og databehandleraftaler.

Vi har i regionerne etableret det nødvendige juridiske set-up omkring Epic medarbejdernes adgange. Alle data ligger fysisk i Danmark i regionernes egne datacentre. Epic medarbejdernes adgange er og har fra start været reguleret af en EU standardkontrakt og en databehandleraftale. Aftalerne er udarbejdet med ekstern rådgivning fra advokatfirmaet Bech Bruun og følger alle forskrifter.

Vi sikrer derudover, at Epic årligt revideres op mod internationale sikkerhedsstandarder af en ekstern revisionsvirksomhed. Seneste revision blev udført af PwC og kom tilbage uden anmærkninger.