Personvernkonsekvensvurdering (DPIA)
Kortversjon for legekontor for PraksisNett sin IT infrastruktur

Artikkel 35-1 i Personvernforordningen (GDPR) sier:

> «Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer.» (Behandlingsansvalig = legekontoret).

Dette dokumentet er utformet for at legekontoret, som er behandlingsansvalig for IT system på legekontoret, skal kunne svare på relevante spørsmål relatert til GDPR.

Dette dokumentet redegjør for hvilken ekstra risiko for eksponering av pasientinformasjon og brudd på pasientens rettigheter fastlegen utsetter sine pasienter for ved å være del av PraksisNett sin IT løsning. For å understøtte fastlegers vurdering har forskjellige aspekter ved IT løsningen vært analysert for risiko av ulike aktører; internt ved NSE, eksternt av HEMIT, og av personvernteamet på Universitetssykehuset i Nord-Norge (UNN), som er databehandler for IT infrastrukturen. Alle dokumentene er vedlagt denne kortversjonen av DPIA. På basis av fremlagt dokumentasjon har personvernombudet ved UNN vurdert at løsningen *ikke* utgjør en uakseptabel risiko for personvernet. Personvernombudets anbefaling er dermed at løsningen kan tas i bruk.

Dataflyt og prosessering av pasientinformasjon i PraksisNett sin IT infrastruktur

PraksisNett sin IT infrastruktur inneholder tre typer dataressurser. Dette er:

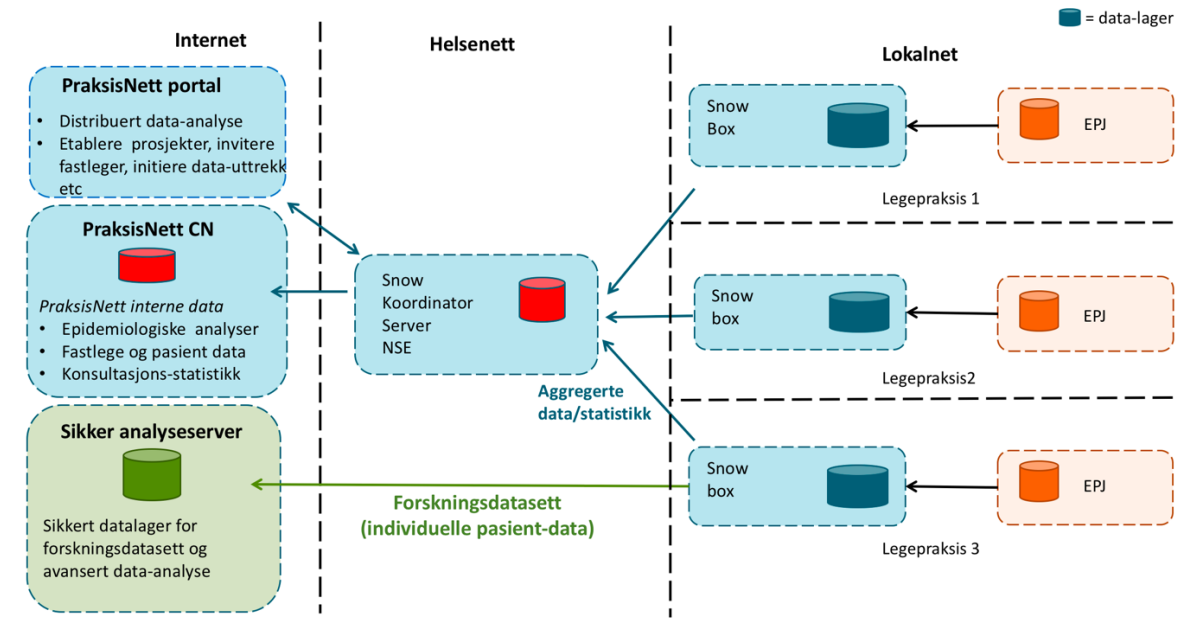
1. Forskningsdatasett som lagres på Snow-boksen (blå tønner i Figur 1)
2. Aggregerte og anonyme data generert fra alle deltagende fastlegekontor (røde tønner i Figur 1)
3. Komplette pseudonymiserte datasett som lagres i en sikker analyseserver (grønn tønne i Figur 1).

De oransje tønnene i Figur 1 er EPJ-databasen (”lagring fra journalsystemet”) som brukes daglig av fastlegen for å dokumentere pasientbehandlingen. Før data kan trekkes ut og benyttes til forskning må fastlegen godkjenne uttrekk og lagring av EPJ-data på Snow-boksen. Data om pasienter og fastleger som trekkes ut fra EPJ-systemet pseudonymiseres[1] før de lagres på Snow-boksen av en programvare-komponent som installeres på EPJ-serveren. Denne kalles Data Reuse Component (DRC). Pasienter kan kun re-identifiseres av pasientens fastlege, eller den som fastlegen har gitt tillatelse.

Aggregerte data lagret i de røde tønnene lages på følgende måte: Data lagret i Snow-boksen aggregeres først lokalt, deretter på tvers av alle Snow-boksene. De aggregerte dataene lagres deretter på Snow koordinatorserveren. Herfra gjør PraksisNett informasjon som er relevant for forskere tilgjengelig. Dette er typisk informasjon *om* tilgjenglige datavariable (metadata),

[1] Pseudonymisering innebærer at alle identifikatorer, som personnummer, navn, helsepersonell-nummer etc. erstattes med genererte identifikator som gjør det umulig å finne identiteten til personen uten tilgang til koblingsnøkkelen.

data om antall fastleger og pasienter, antall konsultasjoner og epidemiologiske data om pasientene. Datasettene kan også analyseres med verktøy for distribuert statistisk data-analyse, mens de ligger lagret på Snow-boksene. Ved distribuert statistisk analyse trekkes kun aggregerte data ut fra Snow-boksene. Distribuert statistisk analyse er nødvendig for å administrere forskningsprosjekt, ivareta sykdomsovervåking (som overvåkning av influensa, etc.) og for å kunne gi fastlegene personlig tilbakemelding på praksis.



Figur 1. Dataflyt i PraksisNett sin IT infrastruktur.

Generering av rekrutteringslister fra pasientdata

For at pasientdata skal kunne brukes til forskningsformål må det innhentes samtykke fra pasienten. Samtykke må innhentes både for prosessering av informasjonen og for deltagelse i et forskningsprosjekt. Alle forskningsprosjekt lager rekrutteringslister for fastlegene ved å matche inklusjon og eksklusjonskriteriene med EPJ-informasjonen om pasientene som er lagret på Snow-boksen. Pasienter som har reservert seg mot forskning vil ikke inviteres. Basert på rekrutteringlistene genererer IT-løsningen individuelle invitasjonsbrev som fastlegen kan sende til pasientene i det aktuelle prosjekt.

Overføring av pasientdata til en sikker analyseserver.

Når datainnsamlingen i et forskningsprosjekt er i gang overføres de pseudonymiserte datasettene jevnlig til en sikker analyseserver. Kun pasienter som har samtykket vil få sine pasientdata overført til den sikre analyseserveren. Her får forskeren tilgang til forskningsdatasettet og kan gjøre avansert data-analyse av det komplette datasettet.

Hvem har tilgang til dataene?

Når EPJ-dataene overføres til Snow-boksen pseudonymiseres identifikatorene til både pasient og fastlege. De pseudonymiserte dataene vil være tilgjengelig for alle som har tilgang til Snow-boksen på legekontoret, samt for de som har systemadministrasjonsansvaret for Snow-boksen. Systemadministratorene er de personene som ivaretar drift på oppdrag fra UNN som er databehandler. Dette gjelder også personell hos Medrave software AB, for de som har Medrave-verktøyet installert på Snow-boksen. På den sikre analyseserveren vil forskere og personell som ivaretar systemadministrasjon ha tilgang til de pseudonymiserte datasettene. De som har ansvar for systemadministrasjon av Snow-boksen må også ha mulighet til å logge seg inn på EPJ-serveren for å installere og administrere DRC-programvare for uttrekk av EPJ-data. DRC-programvaren sørger for at kravene fra GDPR oppfylles på best mulig måte.

Er alle mottakere av pasientinformasjonen identifisert og dokumentert?
PraksisNett sitt IT-system vil være en ny kanal for tilgang til pasientinformasjon og to typer pasientinformasjon vil bli prosessert i PraksisNett; pseudonymiserte datasett og fullt identifiserte datasett. For at noen skal få tilgang til fullt identifiserbar informasjon gjennom dette IT-systemet må vedkommende autentisere seg gjennom HelseID, fastlegen må ha godkjent bruk av pasientinformasjon, og personen må være autorisert av PraksisNett. Fastlegen kan autorisere andre ved legekontoret til å få tilgang til sine pasienters pasientinformasjonen. Tilgang til og prosessering av pasientinformasjonen loggføres.

Pseudonymisert pasientinformasjon
Alle fastleger som har godkjent bruk av pasientinformasjon til et forskningsprosjekt vil få tilgang til pseudonymisert pasientinformasjon som tilhører forskningsprosjektet. Også autorisert støttepersonell ved et legekontor kan få tilgang til pseudonymisert pasientinformasjon i forskningsprosjektet.

Hvilken tilleggs-risiko introduserer Praksisnett løsningen?
Risikoanalysene som er gjennomført har alle konkludert med at systemet medfører lav risiko. I tillegg vil risikoreduserende tiltak iverksettes. Se nedenfor. PraksisNett bruker en dedikert server – Snow-boksen – som sin infrastruktur. Snow-boksen introduserer en risiko for at noen tar med seg den fysiske boksen med pasientinformasjonen, eller at noen hacker seg inn på Snow-boksen via nettet. Snow-boksen introduserer en risiko for å belaste EPJ-serveren ved uttrekk av data og at interne medarbeidere på et legekontor eller systemadministratorer får tilgang til pasientinformasjon via IT-løsningen installert på Snow-boksen. DRC-programvaren som kjører på EPJ-serveren introduserer en risiko for å påvirke EPJ-systemet. Dette er hoved-risikomomentene løsningen introduserer. For en ytterligere gjennomgang av risikomomenter henviser vi til gjennomførte risikoanalyser. Disse er også oppsummert i et vedlegg til det komplette DPIA-dokumentet.

Hva er risikoen for at data kan bli misbrukt?
Risikoanalysene som er gjennomført har alle konkludert med at systemet medfører lav risiko. Et viktig tiltak som legekontoret må bidra med er å lage rutiner for gjennomgang av PraksisNett sine informasjonssikkerhetsrapporter som vil sendes legekontoret jevnlig.

Hvilke tiltak er iverksatt for å redusere risiko?

1. Snow-boksen er utstyrt med en av/på knapp. Dersom legekontoret ønsker å stoppe prosessering av pasientinformasjon kan de slå av Snow-boksen, koble fra strøm, eller ta ut nettverkpluggen til serveren. Alle disse handlingene vil effektivt stoppe prosessering av pasientdataene.
2. Pseudonymisering. For å redusere risiko for eksponering av identifiserbar pasient-informasjon er alle data pseudonymisert. Snow-boksen vil ikke inneholde opplysninger om identiteten til pasienter eller helsepersonell. Dette vil lagres på EPJ-serveren.
3. Fysisk sikring av Snow-boksen. Snow-boksen må sikres fysisk på samme måte som EPJ-serveren. EPJ-serveren vil være et mer fristende mål om noen skulle få fysisk adgang siden den vil inneholde komplette data med full identitet på pasienter og helsepersonell, mens Snow-boksen kun vil inneholde pseudonymiserte data.
4. Sentralisert overvåkning. All aktivitet på Snow-boksen vil automatisk logges til et sentralisert overvåkningssystem. Personer som forsøker å hacke seg inn på en Snow-boks over nettet vil ikke kunne hindre at forsøk på pålogging og vellykket pålogging blir synlig i overvåkningssystemet. Overvåkningssystemet vil jevnlig rapportere til legekontoret om aktiviteten på Snow-boksen. Forsøk på hacking vil derfor med stor sannsynlighet oppdages.

5. Minimalisering av EPJ uttrekk. IT-løsningen vil tilstrebe å kun gjøre ett uttrekk av EPJ-data til Snow-boksen pr. dag, fortrinnsvis på sen kveldstid/natt, når EPJ-systemet ikke benyttes. Dette vil minimalisere belastningen på EPJ-serveren.
6. DRC-programvare. I valget mellom pasientidentifiserbar informasjon på Snow-boksen og å installere DRC-programvaren for uttrekk på EPJ-serveren, har vi valgt det siste. Dette minimaliserer sannsynligheten for å eksponere identifiserbar informasjon om pasienter og helsearbeidere og ivaretar kravene fra GDPR på best mulig måte. Løsningen introduserer imidlertid en mulighet for å påvirke EPJ-serveren. En rekke tiltak er iverksatt for å minimalisere denne risikoen.
7. Blokkering av Snow-boksen. For å eliminere mulighetene for å få tilgang til personidentifiserbar informasjon fra EPJ via Snow-boksen (som følge av hacking eller ulovlig innsyn via nettet) er slik tilgang blokkert.
8. Logging av aktiviteten på Snow-boksen. For å avdekke intern tilgang til pasientinformasjon logges all tilgang til datasett og rapporteres jevnlig til legekontoret. Eventuell urettmessig bruk av pasientinformasjon vil med stor sannsynlighet bli synlig i disse informasjonssikkerhetsrapportene. Alle systemadministratorer må benytte personlige kontoer for systemadministrasjon. Alt systemarbeid skal logges med begrunnelse for pålogging og rapporteres jevnlig til legekontoret.
9. Overføring av forskningsdatasett. For å redusere muligheten for at forskningsdatasett kommer på avveie utleveres ikke forskningsdatasett direkte til forskere. Datasettene overføres direkte til en sikker omgivelse på en sikker analyseserver der forskeren kan få tilgang.
10. Andre sikringstiltak. En rekke andre sikkerhetstiltak er iverksatt for å minimalisere risikoen for eksponering av informasjon om pasienter og helsearbeidere. Å følge «Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten» er et av disse.

Hvem har ansvar for hva hvis noe skjer?
Dette er beskrevet i GDRP artikkel 33: Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten

Artikkel 33 Nr.1 i GDPR om legekontorets ansvar :

> «Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til vedkommende tilsynsmyndighet i samsvar med artikkel 55, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Dersom bruddet ikke meldes til tilsynsmyndigheten innen 72 timer, skal årsakene til forsinkelsen oppgis.» (Behandlingsansvalig = legekontoret).

Artikkel 33 Nr. 2 i GDPR om databehandlers (UNN) ansvar :

> «Etter å ha fått kjennskap til et brudd på personopplysningssikkerheten skal databehandleren uten ugrunnet opphold underrette den behandlingsansvarlige.»

Se også artikkel 34 nr 1. om underretning av den registrerte (dvs. pasienten).