NASJONALT KARTLEGGINGSSYSTEM FOR SELVMORD
i psykisk helsevern og tverrfaglig spesialisert rusbehandling

UiO : Universitetet i Oslo

NSSF
Nasjonalt senter for selvmords-forskning og -forebygging

Nasjonalt kartleggingssystem for selvmord
i psykisk helsevern og tverrfaglig spesialisert rusbehandling
Sognsvannveien 21, bygg 12, 0372 Oslo
E-post: Nssf-kartlegging@klinmed.uio.no
Telefon: 905 92 297

Dato: 14.01.2019

Prosjektbeskrivelse: Nasjonalt kartleggingssystem for selvmord i psykisk helsevern og tverrfaglig spesialisert rusbehandling

Denne prosjektbeskrivelsen ble først utarbeidet av NSSF i 2015 og sendt til Helsedirektoratet 01.08.2016 som vedlegg til søknad om dispensasjon fra taushetsplikten etter helsepersonelloven § 29 b. Revidert 06.01.17. med ny samlet beskrivelse av håndteringen av personsensitive opplysninger. Ny revisjon 09.08.17 med oppdatert informasjon av vedtak og vilkårene i konsesjon av 10.04.17 og dispensasjon av 12.12.16. Ny revisjon 14.01.19 etter endring av vedtak om dispensasjon datert 19.12.18.

Innledning

Helsedirektoratet fikk i tildelingsbrevet for 2015 i oppdrag fra Helse- og omsorgsdepartementet å forberede og koordinere innføringen av et nasjonalt kartleggingssystem for selvmord i psykisk helsevern, heretter kalt Kartleggingssystemet, etter modell fra National Confidential Inquiry into Suicide and Safety in Mental Health (NCISH) (1) i Storbritannia. Helse- og omsorgsdepartementet hadde på oppfordring av Nasjonalt senter for selvmordsforskning og -forebygging (NSSF) ved Universitetet i Oslo vurdert hvorvidt prosjektet burde innføres som et nasjonalt helseregister i form av egen forskrift. Departementet vurderte utfordringene med dette på kort sikt som betydelige, og besluttet derfor at ordningen i første omgang skulle etableres som et prøveprosjekt med konsesjon fra datatilsynet og dispensasjon fra taushetsplikten etter helsepersonelloven § 29 b. Systemet skulle etableres i løpet av 2015, og det ble gitt et tilsvarende oppdrag til de regionale helseforetakene om å starte innføringen av systemet i psykisk helsevern (PHV) samme året. I etterkant ble det avklart at systemet også skulle innføres innenfor tverrfaglig spesialisert behandling (TSB). Avtalespesialister innenfor disse tjenestene inngår også i systemet.

Bakgrunn

Det har over mange år vært en bekymring både i forvaltning, helseforetak og forskningsmiljøer over at det mangler en nasjonal oversikt over omfanget av og omstendighetene rundt selvmord i psykisk helsevern og tverrfaglig spesialisert rusbehandling. Dette på tross av at pasienter som mottar hjelp for psykiske lidelser i spesialisthelsetjenesten er en velkjent og viktig høyrisikogruppe for både selvmord og annen selvmordsatferd i tiden de mottar behandling, og i den første tiden etter avslutning av behandling – eller ved overføring til andre deler av behandlingskjeden. Den manglende oversikten over omfang og karakteristika ved disse selvmordene gjør det svært vanskelig å:

1) identifisere behov for forebyggende tiltak,

2) utvikle slike tiltak og

3) evaluere tiltakene.

Det har over lang tid vært ønskelig å gjøre noe med denne situasjonen. Nasjonalt senter for selvmordsforskning og -forebygging (NSSF), som er det nasjonale kompetansesenteret på området, har gjentatte ganger foreslått å utvikle et kartleggingssystem for selvmord i PHV og TSB etter modell av det engelske systemet National Confidential Inquiry into Suicide and Safety in Mental Health (NCISH). NSSF gjennomførte, på oppdrag fra Helsedirektoratet, et pilotprosjekt (2) og leverte en rapport om dette i 2011 som anbefalte en nasjonal innføring av systemet. Senere har også Sykehuset Sørlandet HF i samarbeid med NSSF prøvd ut metoden i større skala med positive erfaringer. Man fant blant annet at så mange som 46 % av alle personer som døde i selvmord i Agderfylkene i tidsperioden 2004-13 hadde hatt kontakt med PHV eller TSB siste år før dødsfallet (3). Funnet viser betydningen av å etablere en tilsvarende nasjonal kartlegging. Underveis i utviklingen av prosjektet ble det bestemt av HDIR at man så langt som mulig skulle inkludere eksisterende registerdata fra Norsk pasientregister (NPR) for å unngå dobbeltrapportering fra Helseforetakene.

Formål

Formålet med Kartleggingssystemet er todelt:

1) Identifisere alle selvmord under behandling og i de første 12 måneder etter behandling i PHV og TSB (inkludert avtalespesialister på områdene).

2) Innhente systematiske opplysninger om pasientene, behandling og omstendigheter ved dødsfallet med sikte på å identifisere svikt på systemnivå, områder for iverksetting av forebyggende tiltak, samt utvikling og evaluering av slike tiltak på gruppenivå.

Hensikten med Kartleggingssystemet er ikke å undersøke enkelttilfeller av selvmord. Derimot vil man ved å samle inn opplysninger fra enkelttilfeller på en systematisk måte kunne aggregere disse slik at de kan analyseres på gruppe- og systemnivå.

Overordnet beskrivelse av metode

Data skal hentes fra flere kilder; Dødsårsaksregisteret (DÅR), Norsk pasientregister (NPR) og fra behandlingspersonell i helsevirksomhetene.

For å identifisere og samle inn systematiserte data på pasienter døde i selvmord inntil 12 måneder etter kontakt med spesialisthelsetjenesten innenfor PHV og TSB, er det nødvendig å benytte en totrinnsprosess for datainnsamling:

> 1) Helsevirksomhetene skal registrere selvmord og nødvendige opplysninger om de avdøde pasientene direkte i Kartleggingssystemet så raskt det lar seg gjøre etter selvmord som helsevirksomheten er eller blir kjent med. Registreringen kan samordnes med øvrig nødvendig saksbehandling i foretakene (varsel til helsetilsynet, eventuelt politi, intern avvikshåndtering). Vi anslår at opp mot 80 % av selvmordene kan registreres på denne måten.
>
> 2) For å sikre inklusjon av alle selvmord i tjenestene, også de som helsevirksomhetene ikke er kjent med eller som av andre grunner ikke blir registrert i henhold til trinn 1 over, vil det være nødvendig med en årlig kobling av DÅR og NPR. På denne måten sikres det at alle selvmordene blir inkludert i Kartleggingssystemet. For denne gruppa, anslagsvis 20 % av totalt antall, vil helsevirksomheten måtte rapportere nokså lang tid etter selvmordet. Fordelt per enhet / spesialist vil dette allikevel utgjøre et svært lite antall selvmord, og arbeidsbyrden tilknyttet dette vil derfor bli beskjeden.

Datakilder

1. **Kartleggingsskjemaet** er elektronisk og fylles ut av en kliniker med kjennskap til pasienten.
   Skjemaet inneholder informasjon om pasienten (demografi og psykososiale forhold), informasjon om behandling og historikk som ikke kan hentes fra NPR, samt klinikernes egne vurderinger av årsaken til selvmordet, mulige forbedringstiltak, eventuell læring i organisasjonen og lignende.

2. **Registerdata** fra Dødsårsaksregisteret (DÅR) og Norsk pasientregister (NPR).
   Fra DÅR hentes informasjon om dødsårsak, dato og obduksjon.
   Fra NPR hentes informasjon om pasienten, kontakt med tjenestene (dato/tid/sted), medisinske data, henvisninger og tvang – som er sentral informasjon for å kunne beskrive behandlingen pasienten mottok i

spesialisthelsetjenestene. Det innhentes også somatikkdata samt situasjonsdata fra TSB. Sistnevnte inneholder blant annet informasjon om personens rusbruk, psykiatrisk komorbiditet og sosiale situasjon.

NPR har ikke opplysninger om tidligere og aktuell selvmordsatferd, en del aspekter ved behandlingen (herunder legemiddelbehandling under innleggelse) samt enkelte andre variabler vesentlige for å sikre Kartleggingssystemets formål. Slike opplysninger må derfor hentes inn fra helsevirksomhetene. Det kartleggingsskjemaet som er benyttet i Storbritannia over mange år, og i de norske pilotstudiene, er derfor revidert, forkortet og spisset mot disse variablene. Dette reduserer rapporteringsbyrden for helseforetakene og den enkelte behandler betydelig. Basert på anslag over omfanget av selvmord i populasjonen (ca. 250 dødsfall årlig) og antall enheter i spesialisthelsetjenesten (> 230, avtalespesialister ikke medregnet) vil dette gjennomsnittlig dreie seg om ett skjema årlig per enhet – naturligvis med variasjoner mellom små og store enheter. Innføringen av Kartleggingssystemet medfører således ikke et betydelig merarbeid for foretakene.

Gjennom en årlig kobling av Dødsårsaksregisteret og NPR vil man kunne «identifisere» pasienter som har dødd i selvmord, men som av ulike grunner ikke har blitt registrert i kartleggingsskjemaet. De aktuelle helsevirksomhetene vil slik få beskjed om å sende inn skjema på de pasientene som ikke ble registrert i første trinn av datainnsamlingsprosessen.

Beskrivelse av datainnsamlingen

Datainnsamlingen er todelt:

1. Innhenting av registerdata (data fra DÅR og NPR):

    a) Dødsårsaksregisteret oversender liste med identiteter for alle personer som er registrert med selvmord og usikker ytre dødsårsak, til avdeling helseregistre, Helsedirektoratet.
    b) Ved bruk av data i Norsk pasientregister (NPR) avgrenses utvalget fra DÅR til alle med selvmord som dødsårsak (og dødsfall med usikker ytre årsak) som har vært i kontakt med psykisk helsevern og/eller tverrfaglig spesialisert rusbehandling siste år før sin død. For dette utvalget mottar Kartleggingssystemet opplysninger fra DÅR og behandlingshistorikk i henhold til variabelliste (også utover siste år før død) fra hele den offentlig finansierte spesialisthelsetjenesten fra NPR.
    c) Når helsevirksomhetene innrapporterer opplysninger om selvmord, jf. punkt 2 a (under) utleverer NPR behandlingshistorikk fra den offentlig finansierte spesialisthelsetjenesten for den aktuelle pasienten til Kartleggingssystemet.

2. Innhenting av informasjon direkte fra helsevirksomhetene skjer i en totrinns prosess:

a) Helsevirksomhetene bes om å rapportere inn selvmord og nødvendige opplysninger om disse direkte til Kartleggingssystemet så raskt det lar seg gjøre etter et selvmord eller ved dødsfall hvor selvmord ikke kan utelukkes. Innrapporteringen gjøres i en sikker løsning via et kryptert nettskjema og portalen Tjenester for Sensitive Data (TSD) ved Universitetet i Oslo.
b) For å sikre at det innhentes informasjon fra helsevirksomhetene også i tilfeller der virksomhetene ikke er kjent med selvmordet, eller av andre grunner ikke har rapportert i henhold til trinn a), er det nødvendig med en rutinemessig kobling av opplysninger mottatt fra helsevirksomhetene, Dødsårsaksregisteret (DÅR) og Norsk Pasientregister (NPR).

For pasientene som først blir identifisert ved koblingen av DÅR og NPR, vil Kartleggingssystemet be helsevirksomhetene om å rapportere nødvendige opplysninger, på samme måte som beskrevet i punkt 2 a, dvs. via det tilrettelagte nettskjemaet og portalen Tjenester for Sensitive Data (TSD) ved Universitetet i Oslo.

I praksis vil de ulike trinnene beskrevet som del 1 og del 2 av datainnsamlingen gjentas regelmessig i prosjektperioden, med denne rekkefølgen:

1. Helsevirksomhetene fyller ut skjema for personer antatt død i selvmord (foreløpig), jf. beskrivelsen i punkt 2 a
2. Behandlingshistorikk fra NPR hentes ut for disse pasientene basert på oversendte identiteter, jf. beskrivelsen i punkt 1 c
3. DÅR og NPR trekker ut data for personer faktisk død i selvmord når endelig liste med døde i selvmord (fasiten) fra DÅR foreligger. Opplysningene ses i sammenheng med opplysninger som allerede er mottatt fra helsevirksomhetene. jf. beskrivelsen i punkt 1 a og b
4. HF fyller ut skjema for personer faktisk død i selvmord som det ikke allerede er fylt ut skjema for, jf. beskrivelsen i punkt 2 b.
5. Prosjektet sletter eventuelle opplysninger de har mottatt fra helsevirksomhetene som gjelder personer som ikke har selvmord som dødsårsak. Slike tilfeller vil først bli identifisert/avdekket når opplysningene fasiten fra DÅR foreligger.

Prosedyre for håndtering av direkte og indirekte identifiserbare data

Hensikten med Kartleggingssystemet er ikke å undersøke enkelttilfeller av selvmord. Derimot vil man ved å samle inn data fra enkelttilfeller på en systematisk måte kunne

aggregere disse slik at de kan analyseres på gruppe- og systemnivå. For å kunne sammenstille data fra henholdsvis helsevirksomhetene, DÅR og NPR må man allikevel ha et personentydig system for å sikre korrekt kobling av opplysningene.

Siden Kartleggingssystemet er avhengig av at det i enkelte deler av datainnsamlingsprosessen benyttes direkte identifiserbare opplysninger (fødselsnummer) for å kunne koble med registerdata, er det utviklet et system for håndtering av de direkte identifiserbare personopplysningene som sikrer at dette kun er tilgjengelig for Helsedirektoratet, avdeling helseregistre, under kobling med registerdata. Prosjektet organiseres på en slik måte at all databehandling i Kartleggingssystemet skjer ved bruk av indirekte identifiserbare opplysninger med en unik prosjektID som løpenummer.

Prosjektmedarbeidere i Kartleggingssystemet får ikke tilgang til fødselsnummeret til de registrerte. Helsevirksomhetene fyller ut kartleggingsskjemaet i en elektronisk løsning der fødselsnummer skilles automatisk ut under innsending til Tjenester for sensitive data (TSD) og legges i en egen mappe. Det ble foretatt en Risiko- og sårbarhetsanalyse (ROS) av løsningen 03.05.2018 (4). Det skal inngås databehandleravtale med Helsedirektoratet, Avdeling helseregistre, som har ansvar for nøkkelforvalterrollen i prosjektet. Dette innebærer ansvar for koblingsnøkkel (fødselsnummer og prosjektID). Helsedirektoratet, avdeling helseregistre, vil benytte TSD som underleverandør for deler av den praktiske håndteringen av de direkte identifiserbare data. Avdeling helseregistre vil være den eneste med tilgang til det krypterte fødselsnummeret og prosjektID som oppbevares i egen mappe i TSD, og som skal brukes for å koble dataene fra virksomhetene med data fra DÅR og NPR.

Om TSD

All håndtering av data i Kartleggingssystemet foregår innenfor rammene av Tjenester for Sensitive Data (TSD) (5) som driftes av USIT ved Universitetet i Oslo. TSD er et system utviklet for lagring og behandling av personsensitive data med en meget høy grad av sikkerhet. Systemet er et fysisk og logisk lukket nett med sterk konfigurasjonskontroll. Alle filer inn og ut av systemet loggføres. TSD oppfyller de strengeste kriterier for oppbevaring av sensitive data. Pålogging til systemet skjer gjennom to-faktor godkjenning.

Kartleggingssystemet benytter TSDs mulighet til granulær tilgang, se under. Oppdelingen sikrer at:

1. Kartleggingssystemet ikke på noe tidspunkt får tilgang til fødselsnummeret til pasientene.
2. Ingen gruppe på noe tidspunkt har tilgang til komplette data (dvs. fødselsnummer, kartleggingsskjema, og registerdataene).

TSD er bygd opp slik at hvert prosjekt har et dedikert område og prosjektadministratorer. Prosjektet deles så inn i grupper som kun har tilgang til spesifiserte mapper med data. I det aktuelle prosjektet vil gruppene være databehandleransvarlig (personale ansatt i Kartleggingssystemet) og nøkkelforvalter (Helsedirektoratet, Avdeling helseregistre). Hver gruppe har en moderator, som oppnevnes av TSD på bestilling fra prosjektadministrator. For å legge til nye medlemmer i gruppene må de først meldes inn av prosjektadministrator og deretter godkjennes av moderatoren i den aktuelle gruppen.

Prosedyren er illustrert i Figur 2 «Beskrivelse av dataflyt i Nasjonalt kartleggingssystem for selvmord», som er vedlagt.

Om Nettskjema

Data fra helseforetakene sendes kryptert inn i en egen mappe i TSD. Til dette benyttes et dedikert nettskjema fra Nettskjematjenesten (6) ved UiO som er integrert med TSD. Når nettskjemaet er innsendt vil det ikke være mulig for respondenten eller noen andre eksternt å gjenutsende eller oppdrive dataene.

All datahåndtering og analyser av data tilhørende Kartleggingssystemet vil foregå innad i TSDs lukkede og sikrede nettverk. All aktivitet her utføres av autorisert personale med taushetsplikt, og all aktivitet loggføres. All håndtering av data på dette nivået vil foregå med prosjektspesifikke løpenumre.

Innsyn

Informasjon om enkeltpersoner vil aldri utleveres fra Kartleggingssystemet.

Etterlatte kan søke innsyn i pasientjournalen jf. Helsepersonelloven § 24 ved å henvende seg til helseforetaket som behandlet pasienten, eller i Dødsårsaksregisteret jf. Dødsårsaksregisterforskriften § 5-1 ved å henvende seg til Dødsårsaksregisteret.

Formidling

Det vil bli produsert årlige rapporter hvor Kartleggingssystemets resultater presenteres. Disse vil dels legges åpent tilgjengelig på nett, dels formidles direkte til myndigheter, RHF og andre sentrale interessenter. NSSF vil også formidle funn direkte til et større publikum, som for eksempel brukerorganisasjoner og befolkningen generelt gjennom blant annet media. Resultatene vil også formidles på etablerte arenaer (fagtidsskrifter, kongresser, pågående undervisningstiltak ved universitet og høgskoler, undervisningstiltak i helseforetakene og spesialistkurset i klinisk suicidologi.

All formidling vil foregå med basis i aggregerte data, enkeltpersoner (f.eks. pasienter døde i selvmord, deres behandlere eller enheter ved lokale helseforetak) vil ikke på noen måte kunne identifiseres i publikasjoner fra Kartleggingssystemet.

Vedlegg

1. Figur 1. Kartleggingssystemet: Totrinnsmodell for datainnsamling
2. Figur 2. Beskrivelse av dataflyt i Nasjonalt kartleggingssystem for selvmord
3. Tabell 1. Oversikt over dataflyt i Nasjonalt kartleggingssystem for selvmord
4. ROS for avidentifisering av pnr, Universitetet i Oslo, 14.5.2018

Referanser:

(1) National Confidential Inquiry into Suicide and Safety in Mental Health: https://sites.manchester.ac.uk/ncish/

(2) Nasjonalt Senter for Selvmordsforskning- og forebygging (2011). *Granskning av selvmord i det psykiske helsevernet.* Hentet fra: http://www.med.uio.no/klinmed/forskning/sentre/nssf/aktuelt/aktuelle-saker/2012/Pilotrapport%20granskning.pdf

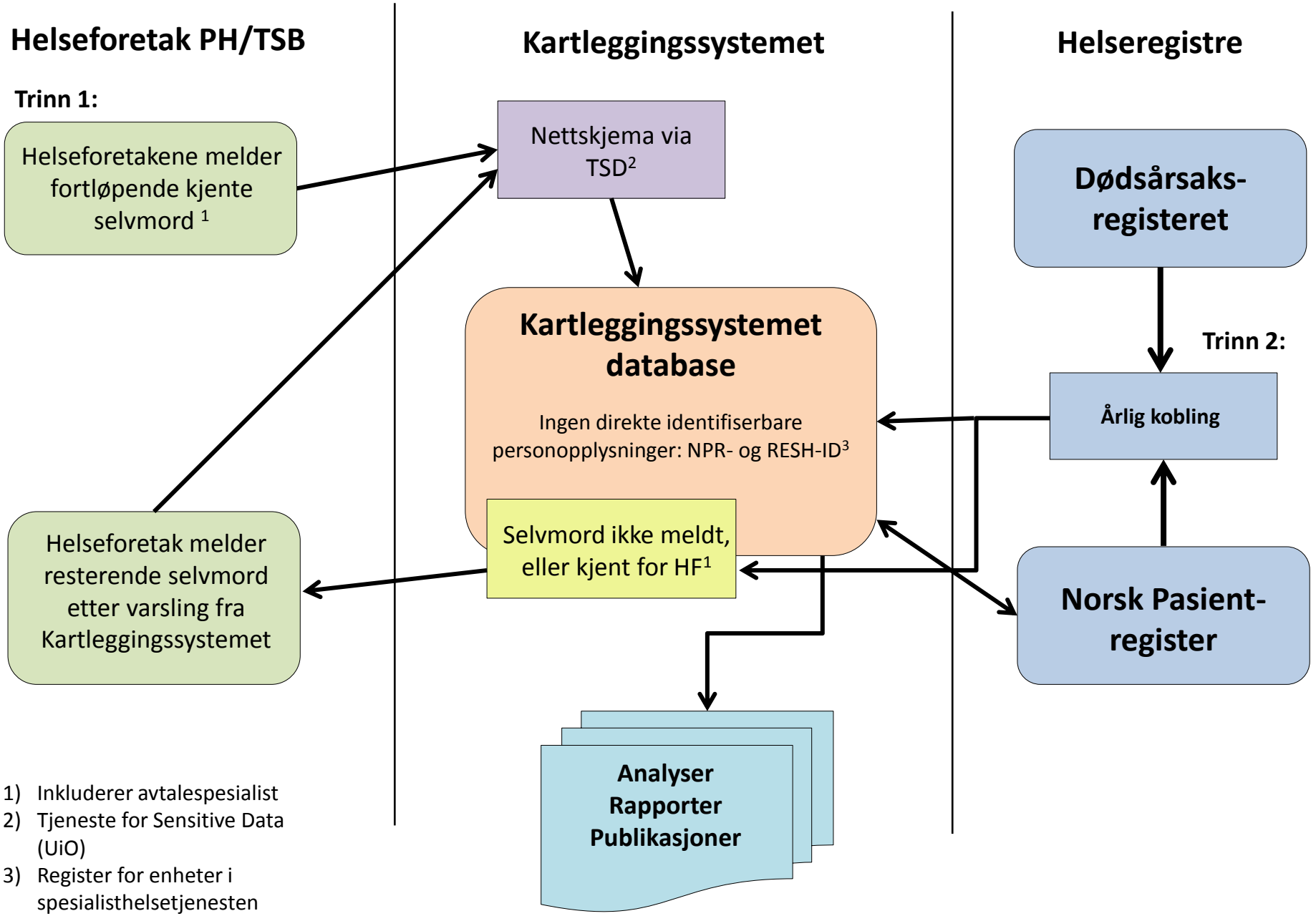
(3) Haaland, V. Ø., Bjørkhold, M., Freuchen, A., Ness, E., & Walby, F. A. (2017): Selvmord, psykisk helsevern og tverrfaglig spesialisert rusbehandling i Agder 2004-13. Tidsskriftet den Norske Legeforening, 137(18). doi:10.4045/tidsskr.16.0503

(4) ROS-analyse for avidentifisering av fødselsnummer (vedlagt): https://www.uio.no/tjenester/it/applikasjoner/nettskjema/drift-og-utvikling/oppdrag/uio/nssf/ros/ros.html

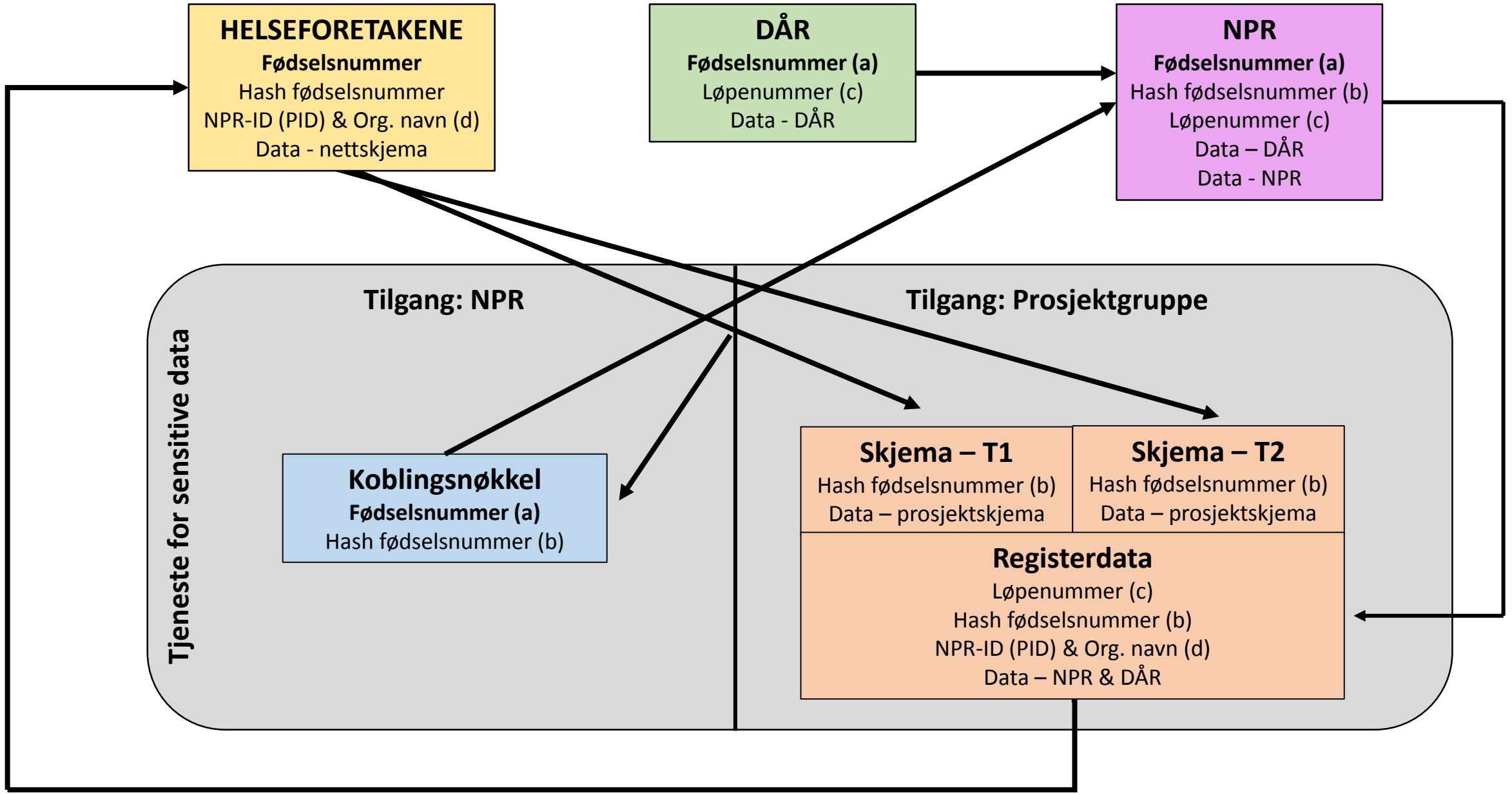
(5) Tjenester for sensitive data, UiO: http://www.uio.no/tjenester/it/forskning/sensitiv/

(6) Nettskjema, USIT, UiO: https://nettskjema.no/

Kartleggingssystemet: Totrinnsmodell for datainnsamling 150817



1) Inkluderer avtalespesialist
2) Tjeneste for Sensitive Data (UiO)
3) Register for enheter i spesialisthelsetjenesten



Figur. **Beskrivelse av dataflyt i Nasjonalt Kartleggingssystem for selvmord**

Tabell - Oversikt over dataflyt i Nasjonalt Kartleggingssystem for Selvmord
Dato: 13.12.18

Tid i måneder	Steg	Arbeidsoppgave	Kommentar	Utfører	Mottaker	Trinn	Dataflyt
0	1	Behandlingspersonell på behandlingssted får informasjon om at en person er død i selvmord	Inkluderer dødsfall hvor det er usikkerhet rundt dødsårsaken, men selvmord ikke kan utelukkes	Helseforetak		1A	
0	2	Behandlingspersonell fyller ut kartleggingsskjema		Helseforetak		1A	
0	3	Kartleggingsskjema med data og prosjektID sendes prosjektet	ProsjektID generes automatisk av en en-veis algoritme ved innsending - basert på fødselsnummeret.	Helseforetak	Prosjektet	1A	Helseinformasjon + prosjektID
0	4	Fødselsnummer skilles automatisk ut under innsending til egen mappe i TSD sammen med prosjektID	ProsjektID og fødselsnummer utgjør koblingsnøkkelen.	Helseforetak		1A	Fødselsnummer + prosjektID
12	5	Saksbehandler i avdeling helseregistre logger inn i TSD, krypterer filen, og legger den krypterte filen i mappe som er tilgjengelig for prosjektet.	Saksbehandler som gjennomfører prosedyren må oppbevare passordet for å dekryptere filen.	Nøkkelforvalter	Prosjektet	1B	Fødselsnummer + prosjektID
12	6	Prosjektet eksporterer den krypterte filen ut av TSD og sender den som vedlegg til avd. Helseregistre iht. gjeldende prosedyre	Kun avdeling helseregistre har passordet for å dekryptere filen. Avdeling helseregistre mottar fil etter eksisterende prosedyre	Prosjektet	Nøkkelforvalter	1B	Kryptert fil med fødselsnummer og prosjektID
12	7	Registerdata fra NPR for personer identifisert i koblingsnøkkelen som er eksportert fra TSD sendes til prosjektet		NPR			Løpenummer
12 - 24	8	DÅR sender liste med døde i selvmord som inneholder fødselsnummer og løpenummer	DÅR sitter med fasit tidligst på dette tidspunktet (inntil 18 mnd etter at hf har registrert info om mistenkt selvmord)	DÅR	Nøkkelforvalter	1B	Fødselsnummer + løpenummer
25	9	Liste fra DÅR kobles med aktivitetsdata i NPR ved hjelp av fødselsnummer	Etter eksisterende prosedyre i avdeling helseregistre	NPR		1B	Løpenummer
25	10	Registerdata fra NPR og DÅR sendes prosjektet med hash fødselsnummer og løpenummer	Etter eksisterende prosedyre i avdeling helseregistre	NPR	Prosjektet	1B	Registerdata, løpenummer, prosjektID, PID & org. nr.
25	11	Registerdata fra NPR og DÅR og kartleggingsskjema kobles		Prosjektet		1B	ProsjektID (trinn 1)
	12	Personer som er rapportert som ikke døde i selvmord fjernes fra databasen		Prosjektet		1B	Løpenummer
25	13	Prosjektet identifiserer personer som **ikke** er rapportert i trinn 1	Ved å se hvilke løpenumre fra DÅR som mangler prosjektID. For disse personene vil det opplyses om PID og organisasjonsnummer i oversendt datafil fra avdeling helseregistre/NPR	Prosjektet		2A	ProsjektID + helseinformasjon (trinn 1)
25 - 36	14	Prosjektet varsler helseforetakene om registrering	Prosjektet purrer helseforetakene inntil to ganger	Prosjektet	Helseforetak	2A	PID og Org.nr.

25 - 36	15	Behandlingspersonell fyller ut kartleggingsskjema som i trinn 1	Bruker NPR-ID (PID) og organisasjonsnummer som de får av prosjektet. Ivaretar at løpenummer fra DÅR er primær-nøkkel	Helseforetak		2A	
25 - 36	16	Kartleggingsskjema sendes inn til prosjektet som i trinn 1		Helseforetak	Prosjektet	2A	Helseinformasjon (trinn 2) + prosjektID
	17	Saksbehandler i avdeling helseregistre logger inn i TSD, krypterer filen, og legger den kryperte filen i mappe som er tilgjengelig for prosjektet.	Saksbehandler som gjennomfører prosedyren må oppbevare passordet for å dekryptere filen.	Nøkkelforvalter	Prosjektet	2B	fødselsnummer + prosjektID
	18	Prosjektet eksporterer den krypterte filen ut av TSD og sender den som vedlegg til avd. Helseregistre iht. gjeldende prosedyre	Kun avdeling helseregistre har passordet for å dekryptere filen. Avdeling helseregistre mottar fil etter eksisterende prosedyre	Prosjektet	Nøkkelforvalter	2B	kryptert fil med fødselsnummer og prosjektID
	19	Avdeling helseregistre mapper opp tilsendte Løpenummer med prosjektID	Liste med løpenummer og prosjektID sendes prosjektet	NPR		2B	løpenummer + prosjektID (trinn 2)
36	20	Kartleggingsskjema fra trinn 2 kobles med registerdata	Registerdata for disse er allerede mottatt	Prosjektet		2B	Helseinformasjon (trinn 2) + Registerdata
36	21	Årgang komplett		Prosjektet		-	Helseinformasjon, registerdata, løpenummer, prosjektID

UiO : Universitetet i Oslo

ROS for avidentifisering av pnr

Deltagere: Halvor Bjørn (USIT), Benjamin Sørlie Ormset (USIT), Martin Øverlien Myhre (NSSF/MEDFAK), Anine Kildahl (NSSF/MEDFAK), Fredrik Walby (NSSF/MEDFAK). Espen Grøndal (IT-sikkerhetssjef ved UiO) var med på begynnelsen av ROSen.

Dagfinn Bergsager fra USIT ledet ROSen.

Denne ROS-analysen ble gjennomført 3.mai 2018

Bakgrunn

UiO er pålagt å gjennomføre Risiko og sårbarhetsanalyser (ROS) av alle applikasjoner. Alle ROS-analyser for prosjekter som samler inn data til Tjenester for Sensitive data (TSD) lages på bakgrunn av ROS-analyser for Nettskjema og TSD. Prosjekteier er ansvarlig for gjennomføring og oppfølging av ROS-analysen.

Denne ROS baserer seg på:

- Sikkerhetsdokumentasjon og ROS av Nettskjema
- Systembeskrivelse og ROS av TSD

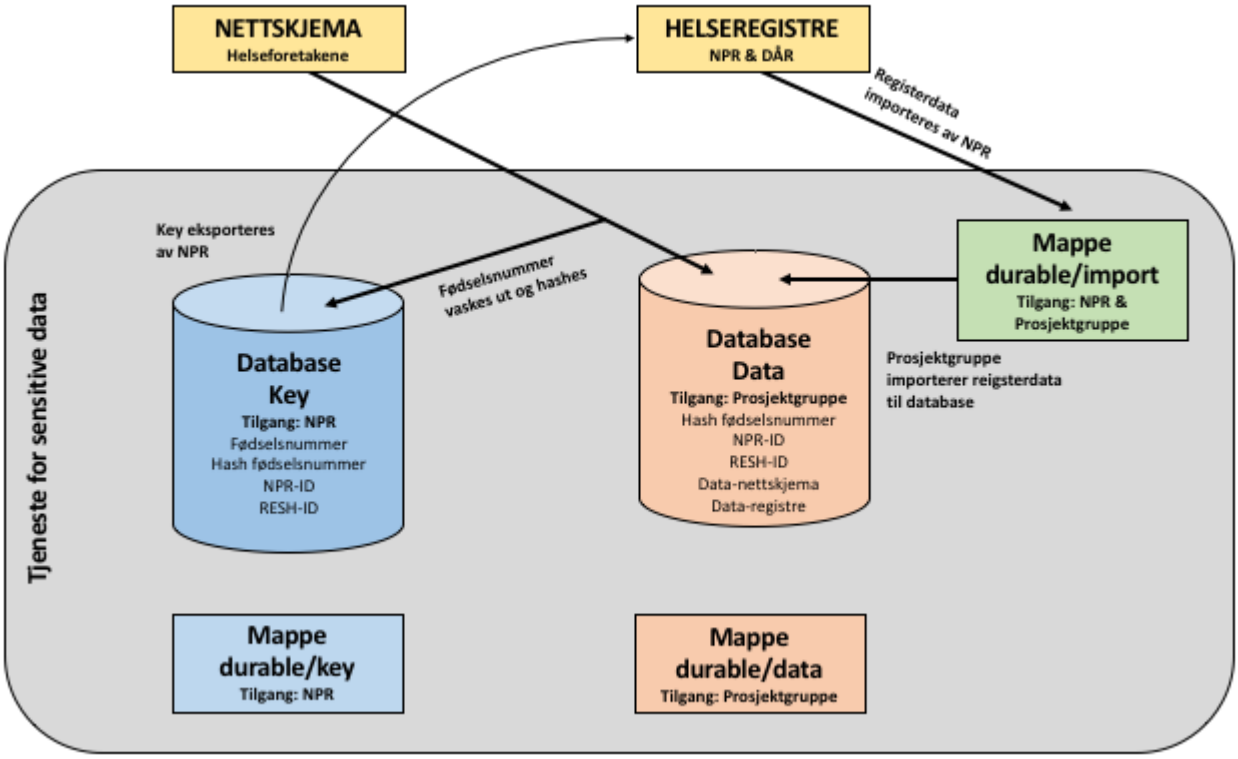
Om prosjektet

Desember 2017 ble det skrevet en avtale mellom USIT og Nasjonalt senter for selvmordsforskning og –forebygging (NSSF) om å utvikle en ekstra funksjonalitet i Nettskjema for å avidentifisere fødselsnummer. Prosjektet skal forske på selvmord i Norge og har konsesjon fra Datatilsynet.

Prosjektet skal samle inn data om alle selvmord under og etter behandling i spesialisthelsetjenesten. Svarene skal samles inn fra behandlere via Nettskjema.

Pasienter registreres med via inklusjonskjema og behandler skriver inn følgende ID for alle registrerte: Fødselsnummer og NPR-ID. Prosjektet trenger tilgang til NPR-ID for å kunne følge opp svar fra behandlere. Det er kun Norsk Pasient Register (NPR) som trenger fødselsnummer i tillegg til NPR-ID. De trenger begge deler for å kunne gi ut data om pasienter. NPR skal selv få tilgang til å hente ut liste over NPR-ID og fødselsnummer fra TSD uten å få tilgang til resten av datasettet.

Alle nettskjema har et spørsmål som ber om fødselsnummer, men disse lagres ikke i klartekst sammen med svarene. Fødselsnummer lagres som en hash (SHA256) sammen med svaret. Fødselsnummer og hash av fødselsnummer lagres separat og kun NPR har tilgang til denne koblingsnøkkelen. NPR har ikke tilgang til resten av datasettet og ingen har tilgang til både datasettet og koblingsnøkkel. NPR skal kunne hente ut fødselsnummer for å kunne ta ut pasientdata for disse fra sine systemer ca 3 ganger i året. Disse pasientdataene skal NPR selv laste opp i TSD via de mekanismer som TSD har for innlevering av data. Fødselsnummer skal erstattes med eksisterende hash av fødselsnummer før data lastes opp. Dette er i utgangspunktet TAB-separerte filer.



Oppsummering av ROS

- **Risiko**: Ondsinnet person fra NPR eksporterer koblingstabell
  - **Tiltak:**
    - NPR har ikke tilgang til dataene til prosjektet
    - Vi logger alle dataeksporter
    - NPR har allerede tilgang til data om alle pasienter via sine systemer
    - Prosjektet bestemmer hvem som har tilgang

- **Risiko**: NPR eksporterer koblingsnøkkel ukryptert og blir lesbare for forskere med eksportrett i prosjektet. Det er ikke fare for at koblingsnøkkel havner hos tredjepart på veien fra TSD til NPR.
  - **Tiltak:**
    - Strenge rutiner for hvordan koblingsnøkkel skal krypteres og slettes fra eksportmappa på server etterpå
    - Det er maks 2 personer i prosjektet som har eksportrett og derfor mulighet til å lese data i eksportmappa.

- **Risiko**: Prosjekteier ber om at ondsinnet person får tilgang til data i TSD
  - **Tiltak:**
    - Ingen har tilgang både til koblingsnøkkel og data. USIT/TSD sørger for at det aldri forekommer.
    - Alle henvendelser og endring av rettigheter logges.

- **Risiko:** En person får tilgang til både nøkkel og data
  - **Tiltak:**
    - NPR må ha rutiner for at fødselsnummer blir erstattet med hash av fødselsnummer før de laster pasientdata opp i TSD
    - Prosjekteier må se til at NPR følger disse rutinene og gi dem god opplæring
    - USIT/TSD legger opp til at løsningen kan gjenbrukes av andre prosjekter med tilsvarende rutiner og gjør det ulovlig for en bruker å ha tilgang til begge typer data.

- **Risiko:** Forsker lager alle potensielle IDer, ettersom det er et begrenset antall tilgjengelige kombinasjoner av fødselsnummer. Dette krever tilgang til Nettskjema og prosjektområdet i TSD.
  - **Tiltak:**
    - Et meget begrenset antall forskere har tilgang til dataene og nettskjema
    - Det krever inngående tekniske kompetanse i prosjektets løsning for å kunne generere slike rekker av hash-fødselsnummer.
    - Forsker kan allerede ringe foretaket og å bekrefte helseopplysninger ved behov

Ta kontakt med Dagfinn Bergsager dersom foretaket ønsker mer teknisk dokumentasjon om løsningen.

Av Dagfinn Bergsager
Publisert 3. mai 2018 08:37 - Sist endret 14. mai 2018 12:42