Felles kommunal journal interim AS

Vedlegg 5:
Informasjonssikkerhet og personvern

Styringsdokument

Felles kommunal journal: Et felles journalløft for kommuner utenfor helseregion i Midt-Norge

Versjon 0.8

18.11.2022

Innholdsfortegnelse

1. INNLEDNING

I dette vedlegget finner du:

- beskrivelse av forutsetninger og avgrensninger knyttet til informasjonssikkerhet og personvern
- vurdering av ansvars- og oppgavefordeling knyttet til informasjonssikkerhet og personvern
- vurdering av personvernkonsekvenser
- vurdering av overordnet risikobilde
- videre arbeid med informasjonssikkerhet og personvern

Til vedlegget følger bilag 5.1 og bilag 5.2. I bilag 5.1 vurderes konseptet knyttet til ulike områder for personvern som formål, grunnlag, og art, samt personvernprinsipper. I bilag 5.2 vurderes risiko og hendelser, samt sentrale tiltak for å imøtekomme risikoer som er identifisert.

En felles plattform betyr ikke at alle skal lese alt, men at de som har tjenstlige behov for informasjon får tilgang til den raskt og effektivt. Det er viktig å utrede personvernspørsmål tidlig for å sikre at plattformen vil bidra til å opprettholde innbyggers rettigheter i henhold til regelverket.

God pasientsikkerhet er helt sentralt for alt arbeid i helse- og omsorgssektoren. Pasientsikkerhet hviler på diagnostisk[1] og terapeutisk[2] sikkerhet, samt informasjonssikkerhet[3]. I fremtidens løsninger må personvern og informasjonssikkerhet være en del av løsningens grunnleggende design. Alle innbyggere skal være sikret tilgang til, og kontroll med egne helseopplysninger, og de skal gis tilgang til logger over hvem som har produsert/endret/sett på opplysningene. De skal også kunne reservere seg mot at enkelte helsepersonell får tilgang, eller at definerte informasjonselementer ikke skal deles. Innbyggerne skal ha tillit til at konfidensialitet, integritet og tilgjengelighet ivaretas etter beste evne. Informasjonssikkerhet, digital beredskap og personvern har av den grunn høy prioritet for å bidra til god og trygg helsebehandling som oppleves tillitsskapende av den enkelte, og samfunnet generelt[4].

Viktigheten av en enhetlig og helhetlig tilnærming til informasjonssikkerhet og personvern i et fremtidig økosystem tilknyttet kommuner og virksomheter, kan ikke uttrykkes sterkt nok. Særlig viktig blir dette når informasjon som behandles i og av plattformen er sensitive personopplysninger og funksjoner som kan påvirke evnen til å yte forsvarlig helsehjelp. Potensielt kan det påvirke liv og helse.

2. FORMÅL

Formålet med å gjennomføre vurderinger innenfor informasjonssikkerhet og personvern har vært å peke på viktige elementer som må håndteres i det videre arbeidet. Prosjektet vil bestå av en kompleks verdikjede med mange aktører som gir økt sårbarhet og risiko, og som må håndteres i prosjektet. For å oppnå akseptabel risiko må hele verdikjeden sikres; det betyr at alle aktører må håndtere og sikre sin del i tillegg til at verdikjeden som helhet blir ivaretatt ved å bruke styringssystem

[1] Diagnostisk sikkerhet: At vi med størst mulig grad av sikkerhet kan si hva pasienten lider av og hvilke konsekvenser det kan ha.

[2] Terapeutisk sikkerhet: At vi behandler pasienten med relevante og effektive tiltak og at behandlingen aldri representerer en større risiko enn selve tilstanden.

[3] Informasjonssikkerhet: Å sikre at informasjon er oppdatert, helhetlig og korrekt (integritet), at den ikke kommer på feil hender eller på avveie (konfidensialitet) og at den finnes der og når behovet oppstår (tilgjengelighet).

[4] Referansearkitektur for informasjonssikkerhet, digital beredskap og personvern for kommunal sektor (RSB) v.1.0 (2020).

for informasjonssikkerhet og personvern.
Det er gjennomført en vurdering av hva som behandles i og av prosjektet, samt hvilke risikoer som finnes. Vurderingene er gjort på et konseptuelt nivå, og er gjennomført «på vegne av» den første kommunen som tar i bruk økosystemet.

Pasientjournalloven §19 fastslår at

> *«innenfor rammen av taushetsplikten skal den dataansvarlige sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte. Den dataansvarlige bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige. Opplysningene skal gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten».*

Kommunene, fastleger og andre aktører utfordres på denne oppgaven i dag. Den enkelte kommune, som en virksomhet som yter helsehjelp, har plikt til å ha en pasientjournal for gjennomføring av helsepersonellets dokumentasjonsplikt (jfr. Helsepersonelloven §39). For å dekke de ulike tjenesteområdene benytter de fleste kommuner forskjellige journalløsninger. Det er ofte 5-6 ulike journalløsninger i bruk i samme kommune, og de kommuniserer stort sett dårlig eller ikke i det hele tatt. Dermed er det liten eller ingen samhandling mellom løsningene, så selv internt i samme kommune får man ikke delt, eller samhandlet rundt samme informasjon. Der man skulle delt informasjon direkte i løsningene må man i stedet kommunisere muntlig, per telefon, i møter, via e-meldinger eller på papir. Dette utfordrer informasjonssikkerhet og personvern, deriblant innbyggers mulighet til å utøve sine rettigheter.

Det overordnede målbildet for prosjektet er etablering av et plattformbasert økosystem hvor informasjonsdeling står sentralt. Via en felles plattform skal alle sikres tilgang til samme informasjonskilde, uavhengig av tid og sted, kun avhengig av hvem man er og hvilken rolle man innehar.

3. FORUTSETNINGER OG AVGRENSNINGER

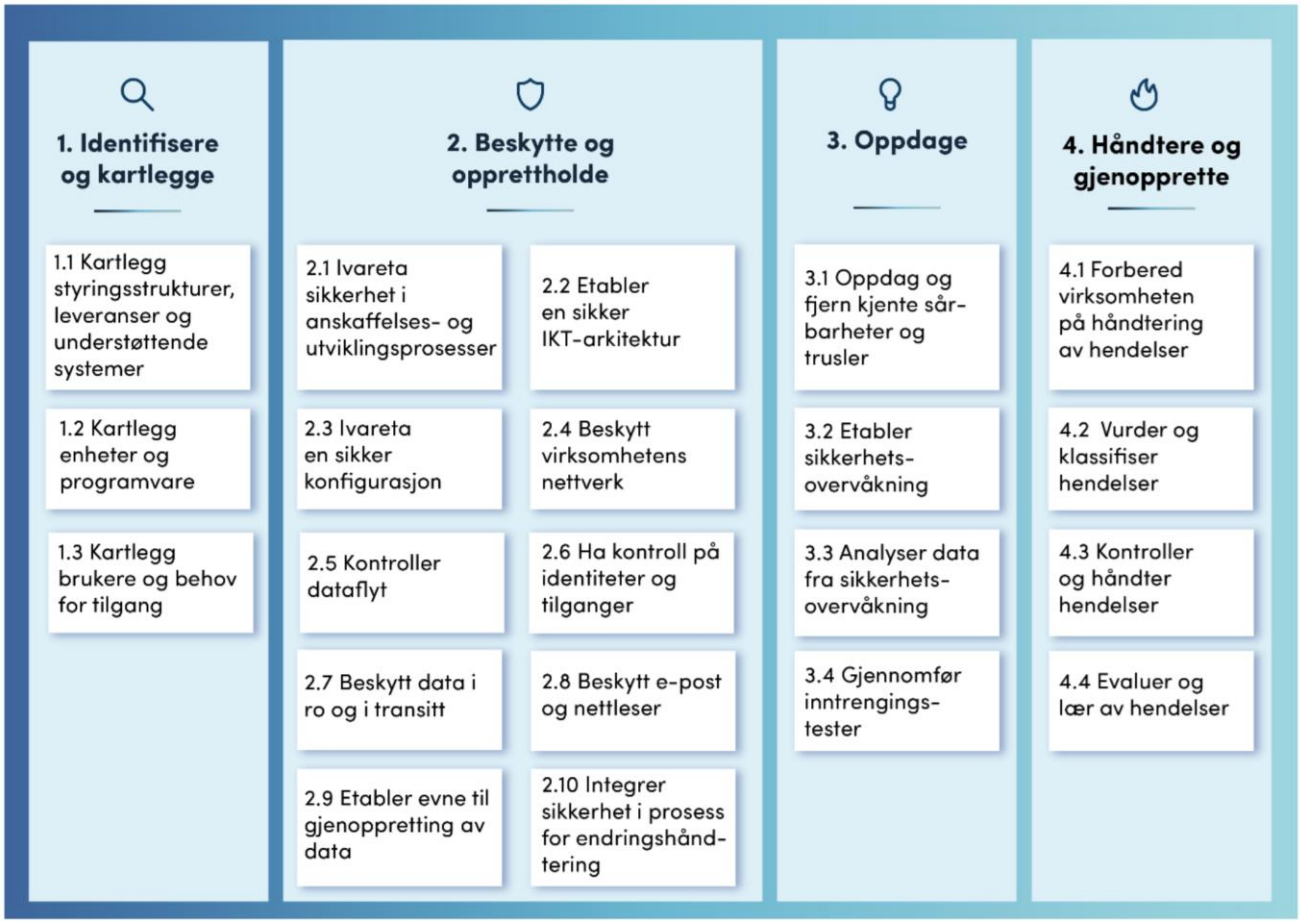
Et prosjekt som dette må forholde seg til ulike føringer og rammebetingelser. Dette omfatter både juridiske rammebetingelser gjennom lov og forskrift, organisatoriske-, økonomiske-, samt tekniske rammebetingelser. Både internasjonalt, nasjonalt, kommunalt og sektorielt (helse og omsorg). Det legges til grunn at prosjektet skal etterleve alle relevante lover, forskrifter og strategier for sektoren. For nærmere beskrivelse se vedlegg 1.

Målet er å ivareta informasjonssikkerhet ved å sikre både tilgjengelighet, integritet og konfidensialitet. I tillegg skal personvernet ivaretas ved at alle løsninger i økosystemet bruker innebygget personvern som standard i sitt design. Robusthet[5] blir i tillegg viktig å ivareta i økosystemet. Norm for informasjonssikkerhet[6] «Normen» legges til grunn, tilsvarende Nasjonal Sikkerhetsmyndighet (NSM) sine grunnprinsipper for IKT sikkerhet[7].

[5] Robusthet – fra engelsk 'Resilience' som både handler om et systems motstandsdyktighet mot påført stress og/eller skade, men først og fremst dets evne til å hente seg inn etter slike hendelser.

[6] Normen | Direktoratet for e-helse

[7] Grunnprinsipper for IKT-sikkerhet | NSM



Figur 1: NSM Grunnprinsipper er delt inn i fire kategorier, og består for tiden av 21 prinsipper med tilhørende tiltak. Hentet fra nsm.no

«Referansearkitektur for informasjonssikkerhet, personvern og beredskap i kommunal sektor (RSB) er en veiledning/kravsett på hvordan man kan oppnå tilstrekkelig sikkerhets- og beredskapsmessig evne for å levere og konsumere trygge og sikre tjenester.
RSB har en helhetlig tilnærming til å finne tjenestekritikalitet for tjenestene, som brukes for å dimensjonere rett og tilstrekkelig sikkerhets- og beredskapsevne. I tillegg gis veiledning i forhold til hvilke sikkerhets-, beredskaps- og personvernprinsipper som bør implementeres.
RSB er kost, kvalitet, og risikobasert slik at i hvilken styrke det enkelte personvern, sikkerhets- og beredskapsprinsipp skal implementeres i, vil avhenge av tjenestekritikalitet og tjenestetype.»

(Referansearkitektur for informasjonssikkerhet, personvern og beredskap i kommunal sektor versjon 1.0)

Risikovurdering og personvernvurdering er avgrenset slik at det ikke omfatter markedsplassen, dette med bakgrunn i at markedsplassen kun beskrives konseptuelt på nåværende tidspunkt. Nasjonale løsninger er heller ikke en del av omfanget i vurderingen da vi legger til grunn at informasjonssikkerhet er ivaretatt av de som har ansvaret.

Mangel på detaljkunnskap om plattform, understøttende IKT-infrastruktur samt applikasjonene som skal kjøres mot plattformen medfører at vi kun legger overordnede betraktninger og vurderinger til grunn i risiko- og personvernvurderingen på dette tidspunktet i arbeidet. I videre arbeid med de konkrete utprøvningene må det gjennomføres nye og oppdaterte vurderinger.

Det forutsettes at det må gjennomføres risiko- og personvernvurderinger av plattformen, integrasjoner og av de enkelte applikasjonene som tilgjengeliggjøres på plattformen. Det gjelder eksisterende og nye tjenester og det må skje fortløpende, også i forhold til utprøvninger.

4. INFORMASJONSSIKKERHET OG PERSONVERN I FORHOLD TIL REALISERING AV MÅLBILDE

Helsepersonells tilgang til informasjon i plattformen vil styres via applikasjonene i økosystemet. Tilgangsstyringen består av autentisering[8] der det vil være kommunene som har ansvar for å definere hvem som skal ha tilgang. Autorisering[9] omhandler det å styre hva helsepersonell skal kunne lagre, se, kontrollere og/eller endre av pasientinformasjon på informasjonsplattformen. Vi legger til grunn at helsepersonell skal logge på applikasjonene ved å bruke HelseID.

At opplysningene om pasienten er relevante sikter til at de er nødvendige, oppdaterte og korrekte, samtidig som helsepersonell ikke oversvømmes av overflødig informasjon. Det er applikasjonsleverandørene som skal ivareta relevansen for det enkelte helsepersonell gjennom sine applikasjoner.

For at tilgangen til helseinformasjon på informasjonsplattformen skal fungere, sett i forhold til deling av informasjon med andre virksomheter, må prosjektet definere retningslinjer (policy) for informasjonssikkerhet og personvern, herunder også tilganger i økosystemet. I tillegg må prosjektet ha oversikt over ansvarsfordelingen knyttet til sikkerhet mellom ulike aktører og løsninger i økosystemet.

Som en viktig sikkerhetsfunksjon, og for å redusere antall angrepsflater[10], bør identitet og tilgangsstyring ivaretas, eksempelvis gjennom en delkomponent som sentralisert IAM (Identity and Access Management). Avklaring av hvem som for eksempel er ansvarlig for identitetsstyring, tilgangsstyring og autorisasjon er en viktig del av videre arbeid. Det vises også til et eksempel på rolle og ansvar senere i vedlegget.

I det videre arbeidet med å realisere målbildet er en felles informasjonsplattform master for informasjonen. Tilsvarende vil felles plattform være master for informasjon som utveksles fra kommunale tjenester og mot spesialisthelsetjenesten. I en stegvis realisering vil det være helt sentralt å fortløpende avklare hvilken informasjon som har sin autorative kilde i plattformen, og hvilken informasjon som fortsatt har autorativ kilde i sluttbrukerapplikasjonene (journalsystemer, applikasjoner etc.).

Risiko- og sårbarhetsanalyser (ROS) må gjennomføres både av prosjektet og leverandørene av applikasjoner og plattform. Disse må være tilgjengelige for prosjektet til enhver tid, og ferdigutfylte maler må tilgjengeliggjøres for kommunene slik at de kan gjøre sine ROS analyser og vurderinger av personvernkonsekvenser (DPIA). I tillegg må ferdigutfylt mal for protokoll over behandlingsaktiviteter tilgjengeliggjøres.

Drift, sikkerhetsovervåking, analyse og håndtering av sikkerhetshendelser i økosystemet bør være mest mulig sentralisert og må sees i et helhetlig perspektiv.

4.1. Sikring av informasjon i økosystemet

Målbildet er et plattformbasert økosystem og bør etablere en styringsmodell[11] som legger premisser for deltagerne. Det vil si leverandørmarkedet, kommuner eller andre aktører som skal være en del av

[8] Autentisering er å sikre at en person er den man utgir seg for. Det vil si å slå fast identitet

[9] Autorisering vil si å verifisere hvilke roller du kan ha og har, det vil si at du har de utdannings-, autorisasjons- og stillingsmessige rollene som kreves for at du kan gis tilgang til en bestemt informasjon

[10] Med angrepsflate mener vi et område eller system som er tilgjengelig for angrep og dermed er utsatt.

[11] En styringsmodell (engelsk: governance model) omhandler rolle- og ansvarsfordeling mellom aktørene

økosystemet. Dette er også beskrevet i vedlegg 4. Dersom deltagerne dokumenterer at de tilfredsstiller premissene for deltagelse (at de er compliant[12]), slippes de inn i økosystemet. I motsatt fall må de utbedre eventuelle avvik før de får tilgang. Organisasjonen som er ansvarlig for økosystem (plattform og markedsplass) må etablere et styringssystem for å forstå sin virksomhetsrisiko som ansvarlig for hele verdikjeden [13]på et overordnet nivå og styre virksomheten etter dette.

Leverandørkjede-angrep som kommer via underleverandører eller samarbeidspartnere kan være krevende å oppdage, og for å ivareta det vil prosjektet anbefale Zero Trust-arkitektur[14] for å sikre verdikjeden.

Et annet tiltak for å sikre hele verdikjeden kan være å stille krav til alle deltagerne i forhold til å definere akseptabel risiko. Dette kan oppnås ved at representanter fra de ulike aktørene jobber sammen i forhold til risikovurdering og personkonsekvensvurdering.

4.2. Skybaserte løsninger

Prosjektet anbefaler skybaserte løsninger i økosystemet i tråd med nasjonal strategi for bruk av skytjenester[15]. Dette vil kreve at prosjektet også tar ansvar for den helhetlige sikkerheten i økosystemet, samt gjør nødvendige kartlegginger og undersøkelser av sikkerhet hos aktuelle skytjenesteleverandører. Dette som beskrevet i NSMs grunnprinsipper for IKT-sikkerhet og i Normen. For at overføring av personopplysninger ut av EØS, enten til tredjeland eller internasjonal organisasjon, skal være lovlig må det finnes et overføringsgrunnlag. Retningslinjer[16] gitt av Personvernrådet (EDPB) forklarer at dersom en ansatt i et datterselskap i samme konsern utenfor EØS har fjerntilgang til norske virksomheters personopplysninger, vil fjerntilgangen regnes som en overføring. Tilleggskravet i forhold til Schrems II- dommen om at man alltid må undersøke om beskyttelsesnivået i praksis vil kunne bli undergravd av forhold i tredjelandet, for eksempel overvåkningslover som går lenger enn det som er nødvendig og proporsjonalt. Dette vil blant annet være aktuelt for amerikanske virksomheter. Dette er grunnleggende krav som må ivaretas og jobbes med i forhold til valg av skytjenester og databehandlere i løsningene som velges.

Vi legger som utgangspunkt til grunn at lagring, også skybasert, skjer i løsninger som er på norsk jord og under norsk jurisdiksjon.

5. INFORMASJONSSIKKERHET OG PERSONVERN I GJENNOMFØRINGSFASEN

Videre arbeid må være i tråd med føringene for informasjonssikkerhet og personvern. Dette gjelder samtlige perioder gjennom hele gjennomføringsfasen.

Det må legges vekt på nivå for akseptabel risiko og håndtering av denne. Å sørge for velfungerende styring og kontroll av informasjonssikkerhet og personvern i den enkelte utprøvingen er en viktig oppgave. Ansvaret for dette tillegges vertskommunen, samt at det klargjøres før oppstart av faktisk utprøvingsprosjekt. Prosjektorganisasjonen kan bistå utprøvingene og vertskommunene i forberedelsene og gjennomføringen.

---

[12] Compliance kan bety å overholde regler (for eksempel spesifikasjon, policy, standard eller lov). «I samsvar med».

[13] Med verdikjede menes her de ulike aktivitetene som til sammen utgjør et tjenestetilbud og deres tilhørende informasjon.

[14] Zero Trust-arkitektur er en måte å designe IT arkitektur basert på «Stol aldri på, alltid verifiser» (never trust, always verify)

[15] Nasjonal strategi for bruk av skytenester | Regjeringen

[16] Overføring av personopplysninger ut av EØS | Datatilsynet

NSMs grunnprinsipper for IKT- sikkerhet brukes for å sette i gang nødvendige tiltak, og vi anbefaler å bruke støtteverktøy[17] fra NSM i arbeidet. I forberedelses- og utprøvingsfasen vil det være spesielt viktig å identifisere og kartlegge risiko sett i forhold til den aktuelle brukerreisen som ligger til grunn for den spesifikke utprøvingen. De ulike aktørene (virksomhetene og aktørene som deltar) i utprøvninger må eksempelvis kartlegge hvilke enheter som er i bruk i virksomheten, både klienter[18], servere og nettverksutstyr. Dette inkluderer kartlegging av programvare som benyttes i virksomheten, i det aktuelle tjenesteområdet.

Der utprøvinger etablerer eller endrer IKT-arkitekturen, vil tiltak innen kategori to i NSMs grunnprinsipper, *beskytte og opprettholde* (ref. figur 1), være viktig for å ivareta en sikker arkitektur. Tiltak innenfor NSM sine hovedkategorier oppdage, håndtere og gjenopprette vil være nødvendige og relevante for alle faser i en utprøvning (med unntak av forberedelse og innsikt fasen).

Risikovurdering (ROS), personvernkonsekvensutredning (DPIA) og protokoll over behandlingsaktiviteter må utføres av og for hver enkelt aktør i utprøvingsprosjektet. Ferdigutfylte maler kan tilgjengeliggjøres for aktørene. I tillegg må ferdigutfylt mal for protokoll over behandlingsaktiviteter tilgjengeliggjøres.

Vurderinger må oppdateres underveis i utprøvingene og ikke minst i videreføringsfasen der flere aktører tar i bruk løsningen.

For alle utprøvinger skal det sikres at de registrerte sine rettigheter ivaretas. Opplæring, kompetanse og holdningsskapende aktiviteter i forhold til brukerne i utprøvingene er også viktige tiltak.

I alt arbeidet med informasjonssikkerhet og personvern må nivå for akseptabel risiko avklares. I tillegg må risiko som ligger utenfor dette nivået håndteres. For prosjektet vil dette bety å etablere velfungerende styring og kontroll av felles logisk informasjonskilde og det tilhørende økosystemet. I tillegg er det viktig å vektlegge at primærhelsetjenesten skal kunne levere trygge og sikre tjenester.

Følgende områder må det jobbes videre med:

- Roller og ansvar for informasjonssikkerhet
- Dataansvarliges ansvar
- Databehandlers ansvar
- Styringssystem
- Risikostyring
- Forholdsmessighet ved valg av tiltak
- Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet
- Oversikt over teknologi og behandling av helse- og personopplysninger
- Vurdering av tjenestekritikalitet (RSB)
- Risikovurderinger bla. før utprøvinger, etableringer og ved organisatoriske/tekniske endringer
- Vurdering av personvernkonsekvenser før utprøvinger og behandling av personopplysninger starter
- Ivaretakelse av rettighetene til de registrerte
- Opplæring, kompetanse og holdningsskapende arbeid til brukerne av økosystemet
- Tilgangsstyring, roller og rutiner
- Fysisk sikkerhet og håndtering av utstyr
- NSMs grunnprinsipper for IKT-sikkerhet
- Sikker IT drift

[17] Støtteprodukter | NSM

[18] Bærbare og stasjonære pc, mobil og nettbrett

- Kommunikasjonssikkerhet
- Leverandørforhold og avtaler
- Håndtering av informasjonssikkerhetsbrudd
- Nødrutiner

6. STYRINGSSYSTEMER FOR INFORMASJONSSIKKERHET OG PERSONVERN

For å sikre metodisk styring og bruk av risikoreduserende sikkerhetsprosjekt bør det tas i bruk styringssystemer for informasjonssikkerhet og personvern (ISMS).

ISMS-er som etableres for å styre, utøve, kontrollere og forbedre informasjonssikkerhet og personvern i prosjektet, herunder i hele økosystemet og av de enkelte aktører og verdikjeder, må etableres med grunnlag i beste praksis for informasjonssikkerhet, IKT-sikkerhet og risikostyring. Prosjektet må sikre at informasjonssikkerhet og personvern ivaretas på en enhetlig og helhetlig måte og at anerkjente standarder og tiltaksrammeverk, gitt ved eksempler i vedlegg 1, i kapittelet *Informasjonssikkerhet, IKT-sikkerhet og personvern*, legges til grunn for ISMS-er og sikkerhetstiltak. Mer informasjon om å etablere ISMS-er finnes eksempelvis hos Datatilsynet[19], med hensyn til personvern, og hos Digitaliseringsdirektoratet[20] med hensyn til standarden ISO 27001.

Organisasjonen(e) som får ansvaret for forvaltningen av økosystemet (plattform og/eller markedsplass) må etablere et ISMS for å identifisere, vurdere, forstå og håndtere både virksomhets- og helhetlig risiko, knyttet til verdiene som behandles i økosystemet, samt for verdikjeder og aktører som påvirker økosystemet. Dette som grunnlag for å styre, utøve, kontrollere og forbedre både ISMS og tilpassede sikkerhetstiltak for å bidra til forsvarlig sikring av verdiene. I økosystem-sammenheng må det etableres en styrings- eller governance-struktur som regulerer rettigheter og plikter til de som vil integrere med plattformen. Dette kan gjøres med medlemsavtaler, bruksvilkår for tjenesten eller annet. Forvaltningsorganisasjonen vil ha et ansvar for å etablere styringsstrukturen, men den må utvikles i samarbeid med aktørene i økosystemet slik at man oppnår eierskap og felles forståelse for kravene til samhandlende aktører.

For å identifisere, vurdere, håndtere og redusere risiko til et akseptabelt nivå og på en enhetlig måte, må det iverksettes helhetlige tiltak, i henhold til beste praksis. Et eksempel på beste praksis for IKT-sikkerhet er at sikkerhetsfunksjoner bør sentraliseres[21] i prosjektet. Dette vil redusere ulikhet i infrastruktur, samt sikkerhetstiltak som er ment å oppfylle de samme funksjonene. Dette vil derfor kunne føre til en betydelig reduksjon i helhetlig kompleksitet. Sentralisering vil medføre redusert behov for sikkerhetstiltak med tilhørende kostnader for den enkelte kommune eller virksomhet, herunder redusert behov for å styre, utøve, kontrollere og forbedre sikkerhetsfunksjoner som ivaretas sentralt. De sikkerhetsfunksjoner som i dagens løsninger kunne ha påvirket prosjektet, og som i dag ivaretas av kommuner og enkeltvirksomheters ISMS[22], vil ved sentralisering kunne reduseres for den enkelte kommune og virksomhet til å primært omhandle organisatoriske og menneskelige tiltak. Samtidig vil sentraliserte sikkerhetsfunksjoner kunne ivaretas enhetlig, profesjonelt og bidra til å

[19] Iverksette styringssystem for informasjonssikkerhet | Datatilsynet

[20] Kva seier NS-ISO/IEC 27001? | Digdir

[21] Økosystemet inneholder mange aktører og løsninger. Det må foreligge en virksomhet som er ansvarlig for informasjonssikkerhet i økosystemet.

[22] Sikres med både teknologiske, fysiske, organisatoriske og menneskelige tiltak

skape tillit ved lik bruk og praksis. Det vil også kunne bli betydelig bedre forutsetninger for enhetlig og helhetlig forbedring og automatisering av teknologiske sikkerhetstiltak.

I prosjektets videre arbeid er det viktig å planlegge hvordan de enkelte aktører som vil påvirke informasjonssikkerhet og personvern i økosystemet og i prosjektets verdikjeder, skal bidra til å sikre at informasjonssikkerhet og personvern ivaretas på en enhetlig og helhetlig måte i prosjektet.

6.1. Roller og ansvar knyttet til informasjonssikkerhet og personvern i stegvis utvikling

I et økosystem er det mange aktører. En viktig oppgave i det videre arbeidet vil være å avklare ansvars- og oppgavefordeling knyttet til informasjonssikkerhet og personvern. Dette blir også pekt på som et risikoområde i vurderingen.

Roller og ansvar i den enkelte virksomhet inngår i den enkeltes virksomhet sitt styringssystem for informasjonssikkerhet og personvern, som omtalt i kapitlet over. Vi har her utarbeidet et eksempel på en rolle- og ansvarsmatrise (hovedansvarlig, utførende, konsulterende og informerende = HUKI matrise) som kan brukes mellom de ulike aktørene som et ledd i den stegvise utviklingen på vei mot målbildet. Hensikten er å skape en tydelighet rundt hvem som er hovedansvarlig for hver oppgave eller prosess, hvem som er utførende, hvem skal konsulteres og hvem som bør informeres[23]. I matrisen under er det kun lagt til grunn *eksempler* på oppgaver som kan være aktuelle knyttet til arbeid med informasjonssikkerhet og personvern, samt eksempler på hovedansvarlig, utførende, informert og konsultert.

Aktørene som er definert i dette eksempelet er listet opp øverst i HUKI matrisen. Se forklaringer til enkelte aktører under matrisen.

Oppgave	**Prosjektet (etterfølger)**	**Plattform-leverandør/ forvalter**	**Applikasjons-leverandør**	**Ansvarlig i virksomhet***	**Teknisk personell i virksomheten (IT)**	**Leder eller autorisasjonsansvarlig i tjeneste (kommune)****
Sikre at det foreligger og anvendes et styringssystem for informasjonssikkerhet i økosystemet	H/U	I	I	K/I		
Sørge for at det foreligger en ansvarsfordeling knyttet til sikkerhet i løsningene som er en del av økosystemet	H	U	U	K/I	U	
Sikre at plattformen ivaretar tilstrekkelig informasjonssikkerhet, samt gjennomføre, realisere og følge tiltak for dette	H	U	U	K/I	U	

[23] Rolle- og ansvarsmatrise | KS

Sørge for at kravene til innebygget personvern etterfølges i plattformen	H	U	U	K/I/U	U	U
Sørge for tilstrekkelig informasjonssikkerhet og nødvendige tiltak for å ivareta denne i applikasjoner	K	K	H	I	K/I	
Sørge for at kravene til innebygget personvern etterfølges i applikasjoner	K	K	H	K/I	K/I/U	K/I/U
Sørge for at identitetsstyring etableres og fungerer i plattformen	H	U	I	K/I	I	
Sørge for at identitetsstyring etableres og fungerer i applikasjoner	K/I	K/I	H		I	
Autorisere og de-autorisere tilgang til ressurser og informasjon i gitte ressurser				H		U
Sørge for innebygget personvern identitetsstyring	K/I	K/I	I	U		
Definere rammeverk og rutiner for tilganger (eks roller)	H/U	K/I	U/K/I	K/I	K/I	(K/I)

Tabell 1: HUKI-matrise knyttet til informasjonssikkerhet og personvern i stegvis utvikling

**Ansvarlig i virksomhet er den som har behandlingsansvar*
***Med leder eller autorisasjonsansvarlig i tjeneste (kommune) menes tjenesteleder eller avdelingsleder som har oversikt over ansatte og som i dag er ansvarlig for å bestille og vedlikeholde tilganger*

7. VURDERING AV BETYDNING FOR RISIKO- OG PERSONVERNKONSEKVENSER

7.1. Metode for gjennomføring

I arbeidet med risiko- og personvernvurdering er det anvendt maler fra to ulike kommuner. Malene er i stor grad brukt som et utgangspunkt for gjennomgang og vurderinger. De er derimot ikke komplett utfylt nå, og inngår som en del av videre arbeid. Malene som er benyttet er generelle maler som ikke er spesifikt tilpasset helse, eller prosjektet. Utarbeidelse av et tilpasset malverk vil måtte gjøres i senere faser av arbeidet.

Sentrale områder i mal for personvernkonsekvensvurdering (DPIA) er i bilag 5.1 overført som et skriftlig dokument med beskrivelser på de ulike områdene. ROS-mal er utfylt, men på et mindre omfattende nivå enn det ville vært ved et konkret og avgrenset område eller løsning.

Arbeidet med overordnet personvernvurdering og risikovurdering er gjennomført av kommunale ressurser i prosjektet. Dette har vært viktig for å sikre erfaring og forankring til en kommunal

virkelighet og utfordringsbilde. Vurderingene er gjort med utgangspunkt i en tenkt kommune som kan brukes som grunnlag i forbindelse med utprøving.

7.2. Overordnet personvernvurdering

I prosjektets arbeid er det gjennomført en personvernvurdering av den konseptuelle løsningen på et overordnet nivå. Se bilag 5.1 for vurderingen som er gjort.

Plattformen er foreløpig beskrevet på et overordnet nivå, og det er derfor gjort en vurdering basert på realisering av et målbilde. For hver nye tjeneste/løsning som tilgjengeliggjøres gjennom stegvis utvikling av plattformen, må det gjennomføres en personvernkonsekvensvurdering (DPIA) som detaljert kan vurdere den nye konkrete tjenesten/løsningen eller utviklingssteget.

Over tid vil plattformen inneholde store mengder helseopplysninger som både er regnet som «særlige kategorier av opplysninger» og som samtidig representerer systematiske og omfattende vurderinger av den enkelte innbyggers tilstand. I tillegg kan informasjonen bli gjenstand for automatisert behandling som danner grunnlag for avgjørelser som i betydelig grad vil påvirke den registrerte (som omtalt i personvernforordningen artikkel 35(3)). I sum gjør dette at det er helt nødvendig å gjennomføre en vurdering av personvernkonsekvensene.

Det er viktig å sikre bred involvering i arbeidet med DPIA. Her bør eksempelvis personvernombud, pasientombud, pasient- og brukerorganisasjoner, helsepersonell og teknisk personell aktivt med.

Et viktig element i den konseptuelle løsningen er deling av informasjon mellom helsepersonell som har tjenstlig behov, noe som vil være et aktuelt tema å diskutere som et ledd i en vurdering av konsekvenser for personvern (DPIA). I helsepersonelloven §45 heter det «Med mindre pasienten motsetter seg det, skal helsepersonell som skal yte eller yter helsehjelp til pasient etter denne lov, gis nødvendige og relevante helseopplysninger i den grad dette er nødvendig for å kunne gi helsehjelp til pasienten på forsvarlig måte. Det skal fremgå av journalen at annet helsepersonell er gitt helseopplysninger.»

For mange pasienter er det i dag en utfordring å måtte fortelle sin sykehistorie om igjen til helsepersonell både i samme virksomhet og i andre virksomheter. For pasientsikkerheten kan dette være en utfordring hvis pasienten ikke evner å fortelle eller glemmer av vesentlig informasjon. Mange pasienter tror i dag at helsepersonell allerede har tilgang til relevant helseinformasjon. Ved gjennomføring av DPIA sammen med representanter for de registrerte må det gjøres en forholdsmessig vurdering i forhold til deling av informasjon ved hjelp av plattformen.

Etter hvert som vi får mer konkret kunnskap om, og avgrensning av endelig løsning, informasjon, informasjonsflyt, berørte aktører er det flere vurderinger og tiltak som må videreutvikles. Etter at det er gjennomført en konsekvensvurdering av virkningen for personvern må det vurderes om risikoen for de registrertes rettigheter og friheter:

- er redusert til et akseptabelt nivå, slik at når tiltak er etablert kan behandlingen av personopplysninger gjennomføres
- ikke er redusert til et akseptabelt nivå, slik at behandlingen av personopplysninger dermed ikke kan gjennomføres
- ikke er redusert til et akseptabelt nivå, slik at forhåndsdrøfting med Datatilsynet må gjennomføres før ledelsen tar en beslutning om behandling av personopplysninger

7.3. Overordnet risikovurdering

Det er gjennomført en overordnet risikovurdering av den konseptuelle løsningen for økosystemet med plattform, mens markedsplassen er utelatt fra vurderingen. Vurderingen som er gjort, samt forslag til tiltak finnes i bilag 5.2. Risiko- og sårbarhetsanalysen er gjort ut fra en kommunes ståsted, med tanke på stegvis utvikling, og med fokus på den første kommunen som tar plattform i bruk. Det må gjøres

nye risikovurderinger ved planlegging av utprøvinger i alle steg, som må oppdateres i løpet av utprøvingene.

I arbeidet med risikovurdering har vi innledningsvis identifisert og vurdert risiko og hendelser som kan føre til negative konsekvenser, samt analysert hva disse kan medføre. Det er identifisert og vurdert risikoer innenfor hovedområdene *konfidensialitet, integritet, tilgjengelighet, personvern/GDPR og drift/forvaltning*

Det er avdekket uønskede hendelser av kritisk/høy risiko, moderat risiko og lav risiko. Eksempler på tiltak er utarbeidet på risikoer kategorisert som moderat, høy og kritisk.

Det er i risiko- og sårbarhetsanalysen avdekket både tilsiktede og utilsiktede trusler. Tilsiktede trusler kan være bevisste handlinger for å skade informasjonen på plattformen. Relevante aktører for slike handlinger kan for eksempel være ansatte, organiserte kriminelle eller fremmede statsmakter. Relevante aktører for utilsiktede trusler, der aktører gjør feil eller ubevisste handlinger som skader informasjonen på plattformen, kan være administratorer, helsepersonell, drifts- og support personell, brukere av plattformen, eller hendelser som strømbrudd, brann, vannlekkasje eller maskinvare.

I forbindelse med planlegging av første utprøving må prosjektet gjennomføre tiltak for å sørge for akseptabel risiko. Det må lages en plan med tydelige frister, og oppgi hvem som er ansvarlig for gjennomføringen. Planen skal forankres hos prosjektets ledelse. Dersom planlagte tekniske tiltak for å oppnå akseptabel risiko ikke kan innføres umiddelbart, bør risikoreduserende administrative tiltak i form av f.eks. rutine vurderes. Risikomatrisen må oppdateres etter at det risikoreduserende tiltaket er gjennomført.