Direktoratet for e-helse

Sentralt styringsdokument

Steg 2 for digital samhandling

Vedlegg I

Strategi for informasjonssikkerhet og personvern for målbildet helhetlig samhandling

Publikasjonens tittel:
Sentralt styringsdokument
Steg 2 for digital samhandling

Vedlegg I: Strategi for informasjonssikkerhet og personvern

Rapportnummer
IE-1087

Utgitt:
Januar 2022

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Besøksadresse:
Verkstedveien 1, 0277 Oslo Tlf.:
21 49 50 70

Innhold

Bilag

1 Innledning

1.1 Innhold i dokumentet

Målbildet for helhetlig samhandling i helse- og omsorgstjenesten skisserer en ny digitalisert måte å samhandle på i helse- og omsorgstjenesten. Det er derfor viktig å ha fokus på informasjonssikkerhet og personvern fra tidlig av i arbeidet med nye samhandlingsløsninger.

Direktoratet for e-helse har utarbeidet en overordnet strategi for informasjonssikkerhet og personvern for målbildet for helhetlig samhandling og som gjelder alle stegene i det videre arbeidet. Konkrete vurderinger gjøres i de ulike stegene i arbeidet med samhandlingsløsningene og basert på denne strategien.

Innholdet i dokumentet er delt inn i følgende kapitler:

Kapittel 1 – Innledning

I dette kapittelet beskrives innhold i dokumentet og overordet om konseptet for helhetlig samhandling.

Kapittel 2 – Risiko og sårbarhetsanalyse og overordnet personvernvurdering
I dette kapittelet oppsummeres vurderinger fra Bilag J1 Overordnet personvernvurdering og Bilag J2 Overordnet risiko- og sårbarhetsvurdering.

Kapittel 3 – Strategi for informasjonssikkerhet og personvern

I dette kapittelet beskrives kritikaliteten sett fra de ulike perspektivene til innbygger, virksomhet(ene) og samfunnet i stort. Videre beskrives de overordnede prinsippene for informasjonssikkerhet og personvern – som utgjør selve strategien, og veien videre for arbeidet.

1.2 Forutsetninger og avgrensninger

Det gjøres følgende forutsetninger:

- Vurderingen knyttes til det skisserte målbildet for helhetlig samhandling (omtalt under). Det omfatter nye samhandlingsløsninger, blant annet ulike typer nye nasjonale informasjonstjenester og komponenter som skal understøtte samhandlingen. Det innebærer at det omfatter både steg 1, steg 2 og fremtidige steg i arbeidet med målbildet for helhetlig samhandling.
- Helse- og omsorgsdepartementet gjennomfører regelverksarbeid for å sikre nødvendig rettsgrunnlag for behandlingen av helseopplysningene i nye samhandlingsløsninger. Helse- og omsorgsdepartementet har allerede igangsatt et lovarbeid som er den rettslige oppfølgingen av Én innbygger – én journal.
- Norsk helsenett SF tar ansvar for å ivareta personvernet og informasjonssikkerheten i konkrete samhandlingsløsninger i steg 1, steg 2 og fremtidig steg i arbeidet med målbildet for helhetlig samhandling. Det omfatter å gjennomføre risiko- og sårbarhetsanalyser og en fullverdig personvernkonsekvensvurdering etter EUs personvernforordning (DPIA) for de enkelte løsningene.

Det gjøres følgende avgrensinger:

- Vurderingen omhandler ikke Felles kommunal journal.

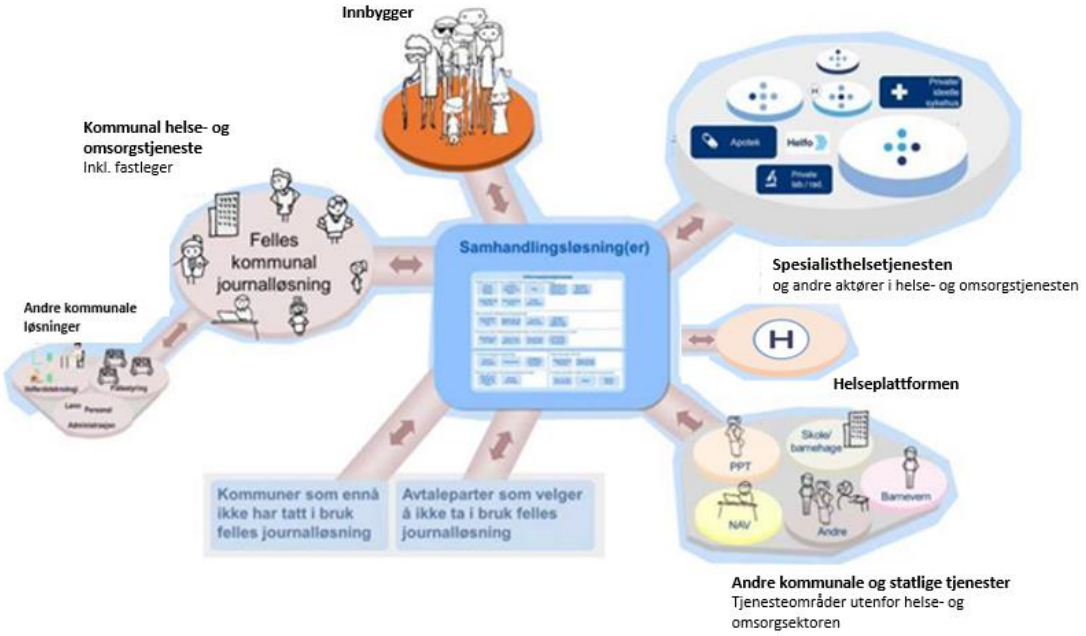
- Vurderingen omhandler ikke eksisterende nasjonale samhandlingsløsninger fordi det legges til grunn at personvernspørsmål allerede er utredet. Dette gjelder e-resept, kjernejournal, Helsenorge og Helsenettet.

Vurderingen er ikke en fullverdig DPIA. Det vil være behov for at Norsk helsenett gjennomfører DPIA så snart informasjonsgrunnlaget er tilstrekkelig.

1.2 Konseptbeskrivelse

Direktoratet for e-helse har i samarbeid med sektor beskrevet et målbilde for helhetlig samhandling som gir en visjon for fremtiden, og som beskriver samhandlingen i helse- og omsorgstjenesten frem mot 2030. Program digital samhandling bruker målbildet som styringsverktøy for å vise retningen. Målbildet består av nye informasjonstjenester som programmet tar sikte på å realisere innen 2030 for å understøtte ytelse av helse- og omsorgshjelp. Dette inkluderer å sikre kontinuitet i direkte helsehjelp, for eksempel når innbygger beveger seg mellom ulike virksomheter eller skrives ut fra sykehus, og å sikre samhandling med responssenter for velferdsteknologiske utstyr og digital hjemmeoppfølging.

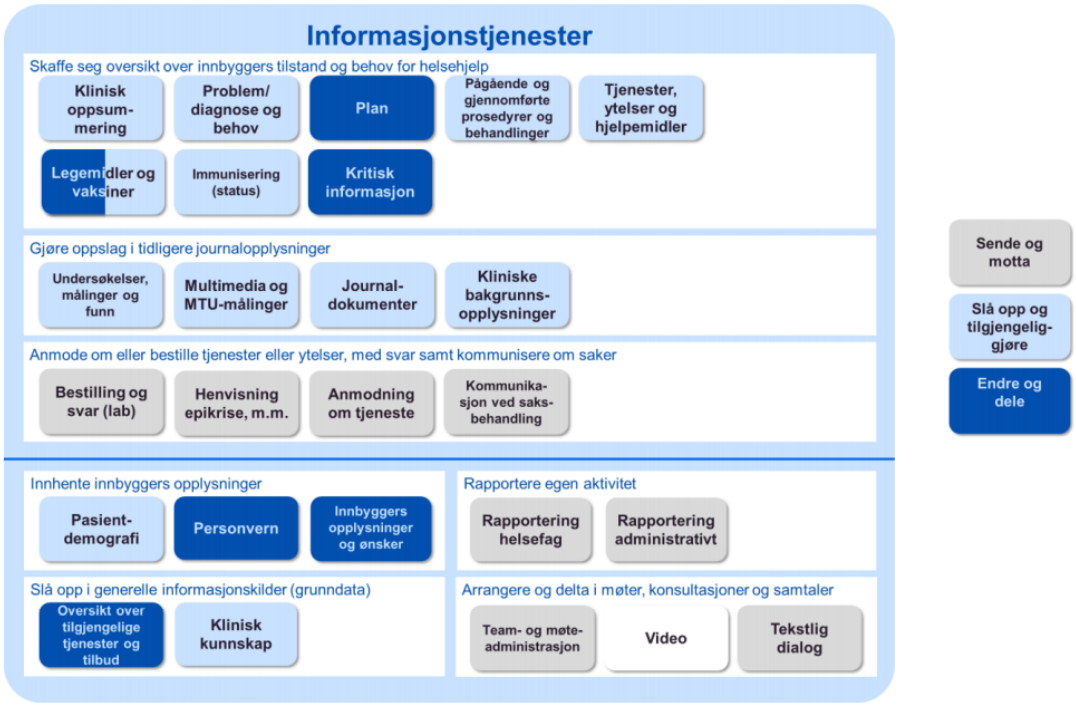
Målbildet for helhetlig samhandling er å tilby informasjonstjenester på en samhandlings-infrastruktur som representerer et sett av informasjonsbehov som ikke er tilstrekkelig dekket i dagens nasjonale e-helseløsninger for samhandling. Hver informasjonstjeneste gir mulighet for å utveksle eller dele helseinformasjon mellom ulike aktører. Figur 3 viser hvilke aktører som samhandler gjennom felles samhandlingsløsninger når målbildet er realisert. Målbildet for helhetlig samhandling ble utarbeidet i forprosjektet for helhetlig samhandling og felles kommunal journalløsning, prosessen og resultatet kan lese mer om i bilag G2 Helhetlig samhandling til sentralt styringsdokument til Akson – helhetlig samhandling og felles kommunal journalløsning.



Figur 1 Aktører som samhandler gjennom felles løsninger når målbildet er realisert

En informasjonstjeneste definerer et utvalg av informasjon som kan deles. Informasjonen kan deles ved hjelp av de ulike organisatoriske samhandlingsformene "sende og motta", "slå opp og tilgjengeliggjøre" og "endre og dele". Disse beskrives nærmere senere i kapittelet. Informasjonstjeneste og samhandlingsform er vist i figur 2. Informasjonsinnhold for hver

informasjonstjeneste må defineres med utgangspunkt i internasjonale standarder, terminologi og kodeverk, med tilhørende tekniske grensesnitt (API).



Figur 2 Informasjonstjenester for helhetlig samhandling

Aktivitetene som vises i målbildet gjenspeiler aktivitetene helsepersonell gjennomfører når de tar mot, gjennomfører behandling, planlegger videre behandling og oppsummerer behandlingen. Informasjonstjenestene understøtter aktivitetenes behov for informasjon:

- **Skaffe seg oversikt over innbyggers tilstand og behov for helsehjelp:** Informasjonstjenestene i denne kategorien benytter helsearbeiderne til å få oversikt over hvem innbyggeren er og kritisk informasjon om innbyggerens helse. Eks. på dette er å få oversikt over evt. legemiddelallergier.
- **Gjøre oppslag i tidligere journalopplysninger:** Informasjonstjenesten gir helsepersonell muligheten til å grave seg dypere ned i innbyggerens sykdoms- og undersøkelseshistorikk fra tidligere besøk i helsetjenesten. Eks. hvis fastende langtidsblodsukker blir målt kan helsepersonell gå inn å journalen og få resultater fra tidligere tester som dagens resultater kan sammenlignes med.
- **Anmode om eller bestille tjenester eller ytelser, med svar samt kommunisere om saker:** Informasjonstjenestene tilrettelegger for samhandling innad i helsetjenesten og med aktører utenfor. Det kan være bestilling av nye prøver eller svar på prøver som er gjennomført, eller anmodning om tjenester fra evt. andre aktører som for eksempel samhandling med nav når innbygger skal sykemeldes. sykemelding til NAV.
- **Innhente innbyggers opplysninger:** Informasjonstjenestene tilbyr informasjon om innbyggeren som for eksempel foreldreansvar og behov for tolk som helsepersonell kan bruke i samhandling med andre aktører for å dekke innbyggernes behov best mulig. Eks. Identifisere hvorvidt innbyggere som blir akuttinnlagt har foreldreansvar og det er behov for å iverksette tiltak for å ivareta barn.

- **Slå opp i generelle informasjonskilder (grunndata):** Grunndatatjenesten tilbyr informasjon om hvilke tjenester som er tilgjengelig i kommunen innbyggeren bor i samt at den tilbyr klinisk fagkunnskap.
- **Rapportere om aktivitet:** Informasjonstjenestene som benyttes for å rapportere om aktivitet til Helfo for refusjon og rapportering av medisinske data til registre slik at den blir tilgjengelig for blant annet forskning.
- **Arrangere og delta i møter, konsultasjoner og samtaler:** Informasjonstjenestene gir helsepersonell muligheten til å samhandle digitalt for å utveksle informasjon med annet helsepersonell og innbyggere.

Målbildet for helhetlig samhandling er beskrevet nærmere i vedlegg M Målbildet for helhetlig samhandling.

2 Risiko- og sårbarhetsvurdering og personvernvurdering

2.1 Innledning

I dette kapittelet oppsummeres vurderinger fra den overordnede risiko- og sårbarhetsvurderingen og den overordnede personvernvurderingen.

2.2 Overordnet risiko- og sårbarhetsvurdering

Det er gjennomført en vurdering av informasjonsverdiene for målbildet om helhetlig samhandling og de ulike trusselaktørene som kan være relevante og deres mulighetsrom. Dette er oppsummert i en rekke scenarier i risiko- og sårbarhetsanalysen. Risikoreduserende tiltak for disse scenarioene beskrives på overordet nivå, da detaljer for den tekniske løsningen fremdeles ikke er avklart. Risiko- og sårbarhetsvurderingen er et verktøy for modning og bevissthet på informasjonssikkerhet for ulike tiltak.

Det vil gjøres oppdateringer av risiko- og sårbarhetsvurderingen på ulike områder gjennom arbeidet med målbildet for helhetlig samhandling, ettersom nye forhold blir avklart og behovene endres. Det vil også utarbeides ulike ROS for spesifikke problemstillinger. Slike kan være ROS for skytjenester, valgt leverandør, samt spesifikke løsningskomponenter. Direktoratet for e-helse står for den overordnede vurderingen, mens Norsk helsenett SF vil gjennomføre tekniske og mer detaljerte vurderinger for de enkelte løsninger.

For ytterligere informasjon om den overordnede risiko- og sårbarhetsvurderingen, henvises det til bilag J2 - Risiko- og sårbarhetsvurdering.

2.3 Overordnet vurdering av ivaretagelse av personvernprinsipper og rettigheter

Det er gjennomført en overordnet vurdering av sentrale personvernspørsmål for det skisserte målbildet for helhetlig samhandling. Vurderingen bygger på tidligere personvernvurderinger fra forprosjektet for helhetlig samhandling og felles kommunal journal, Akson.

Den overordnede personvernvurderingen omfatter bl.a. en gjennomgang av grunnleggende rettigheter, personvernprinsippene og rettighetene og indentifisering av risiko knyttet til personvernet. Dette for å synliggjøre hva programmet må være bevisst på i det videre arbeidet med løsningene og hvilke tiltak som vil måtte settes inn. Vurderingen viser at enkelte av personvernprinsippene og rettighetene vil kunne bli utfordret. Det er imidlertid mulig å redusere risikoen betydelig ved gjennomføring av ulike tiltak.

Norsk helsenett SF vil gjennomføre en vurdering av personvernkonsekvenser (DPIA) for de enkelte løsningene og sikre at prinsipper og rettigheter ivaretas i de konkrete løsningene.

For en mer utfyllende beskrivelse av prinsippene og rettighetene, henvises det til bilag J1 - Overordnet personvernvurdering.

3 Strategi for informasjonssikkerhet og personvern

3.1 Innledning

Tilstrekkelig sikkerhet er en forutsetning for at virksomheter skal kunne levere tjenester i tråd med forventninger og forpliktelser, og for at innbyggerne og andre aktører skal kunne benytte tjenestene etter hensikten.

Strategien forutsetter at roller og oppgaver i realiseringen av samhandlingsløsningen er avklart. Videre at alle relevante lov- og forskriftskrav innen informasjonssikkerhet og personvern, samt Norm for informasjonssikkerhet og personvern (Normen)[1] i helse- og omsorgssektoren – legges til grunn og følges.

Sikkerhetsstrategien for helhetlig samhandling tar utgangspunkt i dimensjonene innbygger, virksomhet og samfunn. I samfunnsperspektivet ligger også samarbeid med andre aktører, samfunnet som sådan, og skadevirkningen som påføres tredjeparter eller samfunnet. Videre at man skal ha en helhetlig tilnærming til sikkerhet og beredskap i tjenesteleveransen og i verdikjeden.

Evnen til helhetlig samhandling i denne sammenhengen er å anse som en viktig samfunnsfunksjon, og er et nødvendig bidrag for å ivareta befolkningens og samfunnets grunnleggende behov knyttet til liv og helse. Den teknologiske utviklingen og integrerte informasjonssystemer bidrar til økt samhandling og en mer effektiv helsetjeneste. Samtidig er det viktig å ivareta ulike hensyn og interesser når det kommer til sikkerhetskrav og beskyttelsesbehov knyttet til innbyggernes helseopplysninger og for å sikre personvernet. Det vil derfor være en balansegang mellom hvor mye man skal beskytte informasjonssystemer uten at det mister nevnte funksjonsevne, samtidig som sikkerhetsinteresser knyttet til opplysninger og personvern ivaretas på en god måte. I et samfunnsperspektiv kan det oppstå situasjoner der det vil være vanskelig å tilfredsstille alle hensyn og interesser. I slike tilfeller må den ansvarlige myndighet vurdere hvilke funksjoner som skal prioriteres. Overordnet målsetting for programmet er å tilrettelegge for bedre samhandling i helsesektoren og tidseffektive løsninger, uten at uhensiktsmessige sikkerhetsmekanismer går på bekostning av dette.

Målet er at den digitale samhandlingen skal være robust og at det skal bidra til virksomhetene som benytter seg av løsningen også blir det. Dette innebærer at virksomhetene skal ha høy pålitelighet og ha lav forekomst av brudd på informasjonssikkerhet og personvern gjennom flere år, på tross av at de er preget av å utføre komplekse oppgaver under et høyt tidspress. For å kunne oppnå dette behøves det tilpasset opplæring og fokus på sikkerhet og personvern, samt gode beslutninger på komplekse problemstillinger som fører til høy kvalitet og pålitelighet på helsetjenester til befolkningen. Det fordrer at helsepersonell som bruker løsningen får tilstrekkelig opplæring i hvordan man raskt og enkelt skal løse hendelser som kan true informasjonssikkerheten til innbyggernes helseopplysninger. Det skal legges opp til at man lærer av tidligere feil og forventer at virksomhetene har et beredskapsperspektiv. Beredskapsperspektiv for virksomhetene betyr at de forbereder seg på «det verste», eksempelvis bortfall av funksjoner for helhetlig

[1] Normen er en bransjenorm for informasjonssikkerhet og personvern i helsesektoren. Den bygger på strukturen i ISO 2700x, samt NSMs grunnprinsipper for sikkerhet. Siste versjon av Normen er mappet til ISO 27001 og Annex A. Normen utarbeides av organisasjoner og virksomheter i sektoren og er derfor godt forankret.

samhandling i lengre tid, og ruster seg for å håndtere dette på alle nivåer i virksomheten. Hvis Norsk helsenett SF og virksomhetene som benytter samhandlingsløsningen gjør dette i praksis, så vil det tilfredsstille de fem prinsippene i det som omtales som robuste virksomheter (High Reliability Organizations).

Det videre arbeidet med sikkerhet for helhetlig samhandling bør se hen til det pågående arbeidet med strategi for digital sikkerhet for helse- og omsorgssektoren.

3.2 Kritikalitet og perspektiver

I risiko- og sårbarhetsanalysen fremkommer det at konfidensialiteten, integriteten og tilgjengeligheten av helseopplysninger har betydning for innbyggernes liv og helse, personvern, virksomhetenes omdømme og samfunnet for øvrig. I lys av dette skal informasjonssikkerhet og personvern være høyt prioritet i arbeidet med å realisere målbildet for helhetlig samhandling. Det er både viktig for å sikre og beskytte omdømmet til virksomhetene i helsesektoren og helsemyndighetene, og gjøre dem kompetente og bevisste på betydningen av helseopplysningenes tilgjengelighet, integritet og konfidensialitet. Høy kritikalitet sett ut ifra de ulike brukerperspektivene (innbygger, virksomhet og samfunnet) legger føringer for sikkerhetsprinsippene.

3.2.1 Innbyggerperspektivet

Dette perspektivet omhandler innbyggers mulighet for å benytte tjenesten i henhold til dennes forventning, avtalemessige forankring, eller lovmessige rett eller plikt.

Innbyggers primære hensikt med å oppsøke helse- og omsorgstjenesten vil være å få god helsehjelp med høy kvalitet. For å kunne yte dette må det helsepersonell de til enhver tid møter ha et helhetlig bilde av tilstanden til pasienten, inkludert informasjon om legemidler, diagnoser, og annet. Fra dette perspektivet fremkommer det at tilgjengeligheten og integriteten til informasjonen vil ha innvirkning på innbyggers liv og helse, og det er derfor særdeles kritisk for den enkelte, spesielt personer i utsatte situasjoner med komplekse sykdomsbilder.

Føring av journal er pålagt ved lov og er derfor noe pasienten i liten grad kan motsette seg. Pasienten må da kunne gi helseopplysningene i tillit til at disse blir vernet mot innsyn fra uvedkommende, i alle deler av verdikjeden. For å ivareta pasientens mulighet for selvbestemmelse og kontroll er pasienten imidlertid gitt en rekke rettigheter, for eksempel rett til innsyn, sperre mv.

Det vil være essensielt å tilby gode verktøy for innbygger for å kunne ivareta sine rettigheteri henhold til helse- og personvernlovgivningen. Ettersom helsetjenesten er stor og kompleks, med mange ulike aktører, vil det være særdeles viktig å etablere tjenester for personvern som er forståelige nok til at innbyggere med ulike forutsetninger kan ivareta sine interesser.

3.2.2 Virksomhetsperspektivet

Helsesektoren har en stor bredde med mange ulike typer virksomheter. Tjenesteleverandør for helhetlig samhandling vil være Norsk helsenett SF i tråd med dagens situasjon.

For å kunne ivareta sin rolle som forvalter av helhetlig samhandling er det kritisk at løsningene har høy tillit. Brudd på informasjonssikkerheten vil medføre tap av tillit og vil ha store konsekvenser for omdømmet til sektoren.

Tilgjengeligheten til informasjon om pasient vil være av kritisk karakter også for de tilknyttede virksomhetene. Deres oppgave er å yte helsehjelp til innbygger og må følge lovkravet helsepersonell har om å dokumentere helsehjelp. Det må nødvendigvis være mulig for virksomhetene å kunne levere helsetjenester i en periode med bortfall av digital samhandling, men det anses å være kort tid før det får konsekvenser for kvaliteten av tjenestene, og kan potensielt gå ut over liv og helse.

Målet er at helhetlig samhandling skal bli kjennetegnet som robust, og at det skal bidra til at virksomhetene som benytter tjenestene også blir det. Det fordrer at helsepersonell som bruker samhandlingsløsningen får tilstrekkelig opplæring i hvordan man raskt og enkelt skal løse hendelser som kan true informasjonssikkerheten til innbyggernes helseopplysninger. Det skal legges opp til at virksomhetene lærer av tidligere feil og har et beredskapsperspektiv der de forbereder seg på det verste, og ruster seg for å håndtere dette på alle nivåer i virksomheten.

Et sentralt poeng i denne sammenheng er at virksomhetene evner å levere forsvarlig helsehjelp gjennom helhetlig samhandling, men også når tjenestene har bortfall i perioder. Det underliggende er imidlertid at samhandlingsløsningene vil være en kritisk funksjon i seg selv for at virksomhetene skal kunne yte forsvarlig helsehjelp.

3.2.3 Samfunnsperspektivet

Ytelse av helsehjelp, herunder helse- og omsorgstjenester og folkehelsetiltak, er definert som en av samfunnets kritiske funksjoner. Begrepet kritisk samfunnsfunksjon forbeholdes funksjoner som samfunnet ikke kan klare seg uten i syv døgn eller kortere uten at dette truer befolkningens sikkerhet og/eller trygghet.

Evnen til helhetlig samhandling er å anse som en viktig samfunnsfunksjon, og er et nødvendig bidrag for å ivareta befolkningens og samfunnets grunnleggende behov knyttet til liv og helse. Den teknologiske utviklingen og integrerte informasjonssystemer bidrar til økt samhandling og en mer effektiv helsetjeneste. Samtidig er det viktig å ivareta ulike hensyn og interesser når det kommer til sikkerhetskrav og beskyttelsesbehov knyttet til innbyggernes sensitive helseopplysninger og for å sikre personvern. Det vil derfor være en balansegang mellom hvor mye man skal beskytte informasjonssystemer uten at de mister nevnte funksjonsevne, samtidig som sikkerhetsinteresser knyttet til opplysninger og personvern ivaretas på en god måte. I et samfunnsperspektiv kan det oppstå situasjoner der det vil være vanskelig å tilfredsstille alle hensyn og interesser.

Helse- og omsorgsdepartementet gjennomfører en vurdering av hvilke løsninger som anses å understøtte de grunnleggende nasjonale funksjonene jf. lov om nasjonal sikkerhet. På dette tidspunkt er det ikke avgjort om funksjonen helhetlig samhandling vil inngå. En vurdering av aspektene rundt dette er omtalt i kapittel 3 i bilag J2 – Overordnet risiko- og sårbarhetsvurdering.

3.3 Overordnede sikkerhetsprinsipper

De overordnede prinsippene for sikkerhet utgjør de strategiske føringene som skal ligge til grunn for de digitale samhandlingsløsningene. Disse vil være førende for hele livsløpet for program digital samhandling.

De overordnede sikkerhetsprinsippene (strategien) er:

1. Pasient og bruker skal enkelt kunne utøve sine rettigheter.

2. Helsepersonell skal ha tilgang til relevante og nødvendige helseopplysninger.
3. Sikkerhet og personvern skal være innebygget og ivaretas gjennom samhandlingsløsningenes livsløp.
4. Løsninger for helhetlig samhandling skal være robuste gjennom samhandlingsløsningenes livsløp.
5. Helhetlig samhandling skal baseres på moderne og fremtidsrettede rammeverk for informasjonssikkerhet og risikohåndtering.
6. Lagdelt sikkerhetsarkitektur og sikring i dybden skal benyttes i samhandlingsløsningene.

Prinsippene er omtalt nærmere nedenfor.

1. Pasient og bruker skal enkelt kunne utøve sine rettigheter.

Pasient og bruker er gitt en rekke rettigheter i personvernregelverket, herunder personopplysningsloven, EUs personvernforordning (også kalt GDPR - General Data Protection Regulation) og særlovgivning om personvern i helseretten.

EUs personvernforordning gir den registrerte en rekke rettigheter når personopplysninger samles inn og behandles om enkeltpersoner. Den registrertes rettigheter står sentralt i forordningen, og en av hovedbegrunnelsene for reguleringen er å sikre at den enkelte får bedre kontroll med behandlingen av opplysninger om seg selv. En rekke rettigheter er spesialregulert i helselovgivninger som for eksempel rett til innsyn, retting, sletting og sperring. Rettighetene er nærmere beskrevet i bilag J1 kapittel 4.

Pasienter som har god informasjon og mulighet til å utøve sine rettigheter, vil kunne ha større grad av selvbestemmelse og kontroll over behandlingen av helseopplysninger. Dette er et sentralt mål i arbeidet med helhetlig samhandling. I målbildet for helhetlig samhandling er pasient og bruker satt i sentrum med hensyn til å kunne utøve og ivareta sine rettigheter. Det skal gjennomføres tiltak som skal gi pasienter og brukere god informasjon og mulighet til å utøve sine rettigheter på en enkel måte.

2. Helsepersonell skal ha tilgang til relevante og nødvendige helseopplysninger.

Samhandlingsløsninger må både ha høy grad av sikkerhet for å ivareta helseopplysningenes konfidensialitet, samtidig som den må være intuitiv nok til at helsepersonellet kan ta i bruk løsningen uten at tilgjengeligheten forringes. Løsningene vil brukes av mange virksomheter som i dag har egne prosesser og verktøy for å tildele brukere unike identiteter med forskjellige tilgangsrettigheter. For å ivareta hensiktsmessig forvaltning av tilganger vil det være nødvendig å benytte en sterk identitets- og tilgangsstyring. Dette betyr å benytte moderne identitetsstyringsteknologi, stille krav til at løsningene har innebygd personvern og tilgangsstyring som begrenser tilganger innenfor definisjon av tjenstlig behov, samt at man etablerer prosesser for å tilbaketrekke rettigheter fortløpende.

3. Sikkerhet og personvern skal være innebygget og ivaretas gjennom samhandlingsløsningenes livsløp.

Samhandlingsløsningene vil være operasjonelle over lang tid. Helse- og omsorgstjenesten vil endre seg gjennom at nye arbeidsformer utvikles (som for eksempel digital avstandsoppfølging og teambaserte arbeidsformer), og gjennom at ny teknologi blir tilgjengelig. Det er derfor et krav at løsningene skal være tilpasningsdyktig med tanke på nye og endrede behov og muligheter.

Strategien forutsetter at alle relevante lov- og forskriftskrav innen informasjonssikkerhet og personvern, samt Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, legges til grunn og følges.

Kravet til innebygd personvern i personvernforordningen artikkel 25 innebærer at ved anskaffelse, utvikling, videreutvikling og vedlikehold av et informasjonssystem skal det tas hensyn til personvern og sikkerhet. Informasjonssystemene skal være sikre, robuste og ivareta de registrertes rettigheter og friheter gjennom hele livsløpet. Herunder skal personvernprinsippene i artikkel 5 være en integrert del av løsningen og det må treffes tekniske og organisatoriske tiltak for å ivareta sikkerheten.[2]

Program digital samhandling må etablere en programutviklingsprosess der sikkerhet er innebygd. Det finnes ulike rammeverk for sikker utviklingssyklus, for eksempel Datatilsynets veileder for programutvikling, og Open Web Application Security Project (OWASP).

Aktiviteter i programutviklingen skal dokumenteres, herunder også sikkerhetsaktiviteter. Det skal utarbeides dokumentasjon på sikkerhetstesting, sikkerhetshetskrav, akseptkriterier, design, kildekode og kodeanalyse.

Sikkerhetstesting gjennomføres som en del av, og koordineres på linje med annen testing. Det skal testes for å sikre at krav til programvaresikkerhet og innebygd personvern er ivaretatt gjennom design og koding, og at kravene er riktig implementert i programvaren. Det skal gjennomføres sikkerhetstesting på nye informasjonssystemer før de settes i produksjon.

Videre må det etableres, og gjennom hele livsløpet vedlikeholdes sikkerhetsmessig, forvaltning av samhandlingsløsningene.

Sikkerhet og personvern for samhandlingsløsningene kan imidlertid ikke kun ivaretas gjennom tekniske tiltak, men må kombineres med menneskelige og organisatoriske grep. Roller og ansvar innenfor sikkerhet og personvern må være avklart og kjent i de ulike virksomhetene. Det må arbeides kontinuerlig med kompetansebygging slik at personell i alle ledd kan utøve god sikkerhetsadferd. Dette gjelder eksempelvis personell som er involvert i utvikling, forvaltning og bruk av tjenestene.

4. Løsninger for helhetlig samhandling skal være robuste gjennom hele livsløpet.

Sett opp mot kritikaliteten til løsningen fra det samfunnsmessige perspektivet, så fremkommer det at løsningene må ha en veldig høy robusthet, og tilfredsstille kjennetegnene til en robust virksomhet (High Reliability Organization).

[2] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/

I en slik robust virksomhet tenker man ikke bare på informasjonssikkerhet, men ser det større bildet på sikkerhet i lys av innbyggere (pasientsikkerhet og personvern), virksomheten selv (informasjonssikkerhet og beredskap) og samfunnet i stort (samfunnssikkerhet og samfunnsberedskap). Man har en felles kultur og et helhetlig tankesett rundt personvern, sikkerhet og beredskap. Denne type kultur og tankesett kan ikke implementeres over natten, men må være et målbilde som det jobbes mot kontinuerlig over tid. Kjennetegnene på en slik virksomhet er som følger:

- Virksomheten er opptatt av feil, og adresserer disse umiddelbart og helhetlig. Brukere rapporterer om mulige feil, og leverandør responderer.
- Virksomheten anerkjenner kompleksitet innen helhetlig samhandling, og kombinerer informasjon fra personell med operasjonelle data for å finne løsninger.
- Virksomheten forstår at de som arbeider i tjenesten har viktig innsikt for å se mulige feilkilder og hvor det er rom for forbedringer, og etablerer åpen kommunikasjon.
- Virksomheten kan hente seg inn fort ved uønskede hendelser, og har alternativer metoder å arbeide på dersom det er nødvendig. Virksomheten er også i stand til å finne løsninger på uforutsette problemer og samtidig holde høy kvalitet i tjenesten.
- Virksomheten har respekt for kompetanse, og har en forståelse for hvor ekspertise befinner seg. Denne benyttes aktivt for å finne gode løsninger.

5. Helhetlig samhandling skal baseres på moderne og fremtidsrettede rammeverk for informasjonssikkerhet og risikohåndtering.

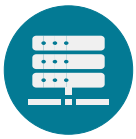
Aktørene som vil benytte samhandlingsløsninger vil representere en stor bredde i sektoren. Virksomhetene vil være av ulik størrelse og ha forskjeller i modenhet, kapasitet og kompetanse til å kunne implementere de kontroller og kapabiliteter som er nødvendige for å oppfylle egenskapene til en robust virksomhet (High Reliability Organization). Se kjennetegn på en slik virksomhet i prinsippet over. For å kunne være robuste virksomheter må sikkerhetsarbeidet baseres på moderne og fremtidsrettede rammeverk for informasjonssikkerhet og risikohåndtering.

Zero Trust er et fremtidsrettet rammeverk for informasjonssikkerhet som ble lansert i 2010. I henhold til dette rammeverket må man ta utgangspunkt i at en virksomhet ikke kan opprette sikre soner, men heller må etablere sikkerhetskontroller der man ikke stoler på noen brukere, terminaler eller applikasjoner når man skal gi tilgang til informasjon. Se nærmere om *Zero Trust* i neste prinsipp.

Et annet fremtidsrettet rammeverk er dynamisk risikostyring. På de mest kritiske funksjonene bør det gjøres dynamisk (kontinuerlig) risiko- og sårbarhetsvurdering slik at man evner og levere tjenestene selv under uønsket påvirkning, eller redusere risikoen for bortfall av tjenestene enten ved tilsiktet eller utilsiktet handling.

Virksomhetene som benytter helhetlig samhandling, må ivareta ulik modenhet på informasjonssikkerhet også gjennom kontinuerlig opplæring av personell. Ved å gjennomføre tilsyn og revisjoner kan man avdekke arbeidsrutiner eller prosesser som ikke ivaretas skikkelig og sette inn skreddersydde tiltak.

Virksomhetene som forvalter og benytter helhetlig samhandling skal følge kravene i Norm for informasjonssikkerhet og personvern (Normen), og de bør benytte tilhørende veiledningsmateriell for å øke kompetanse og modenhet innen informasjonssikkerhet og personvern.



6. Lagdelt sikkerhetsarkitektur og sikring i dybden skal benyttes i samhandlingsløsningene.

Det tradisjonelle synet på at det finnes en klar sikker sone, der man lager beskyttelsesmekanismer kun på de ytre grensene i denne sonen, blir stadig utfordret. Det er derfor hensiktsmessig å legge opp til sikring med større motstandskraft.

I *Zero Trust* ivaretas tjenstlig behov ved at tilganger gis så smalt som mulig. All forespørsel om informasjon om en pasient må være av et autentisert helsepersonell og må underlegges en egen tilgangsbeslutning. Det betyr at enhver forespørsel om informasjon sjekkes og autoriseres. I tillegg vil man i en *Zero Trust*-tankegang logge og analysere all bruk av systemet slik at eventuelle avvik og brudd kan finnes og reageres på så raskt som mulig.

Samtidig er det nødvendig med samarbeid og tilgjengeliggjøring av helseopplysninger for helsepersonell i andre virksomheter. Dette forutsetter at det er tillit til at samhandlingspartene det deles data med, behandler dataene i samsvar med lover og forskrifter. I dagens systemlandskap i helsesektoren håndteres identiteter/brukere i hver enkelt virksomhet og tilgangsstyringen varierer fra virksomhet til virksomhet. For å klare å dele informasjon på tvers av virksomheter med data- og dokumentdeling, må dette baseres på tillit mellom aktørene.

Program digital samhandling arbeider med å etablere en felles tillitsmodell for data- og dokumentdeling som har som mål å skape tillit mellom aktørene og forenkle både identitets- og tilgangsstyringen ved bruk av data- og dokumentdelingsløsninger i helsesektoren.

En utfordring med operasjonelle kontroller er at de ikke nødvendigvis hindrer feil fra å skje. Sikringstiltak kan gjøre at feil sjeldnere oppstår, eller gjøre det mulig å oppdage de innen rimelig tid i etterkant, men kan ikke garantere tilstrekkelig sikring. Det må derfor implementeres flere lag av sikkerhet og derav ha tilstrekkelig sikring i dybden hvorav diversitet skal være et av flere målparametere.

Ideen bak å ha sikring i dybden er å sørge for at det ikke fins ett *single point of failure*, altså et punkt i løsningen som kun har én sikkerhetsmekanisme. Dersom denne mekanismen forbigås vil løsningen være kompromittert dersom man ikke har flere lag av sikkerhet. For å oppnå sikring i dybden kan man kombinere ulike tiltak på fysisk, teknisk eller administrativt nivå. Sikring i dybden gjennomføres ved å implementere flere sikkerhetstiltak som sikrer mot samme angrepsvektor, dersom en sikkerhetsmekanisme feiler vil ytterligere sikringstiltak fremdeles være intakt. Fysisk sikring kan eksempelvis være at helsepersonell må ha datamaskiner på rom med lås, teknisk kan være tilgangsstyring, og administrative tiltak kan være verifiserte prosesser for utdeling av adgangskort.

Ved implementering av passive sikkerhetsmekanismer legges naturlig menneskelig adferd til grunn og hjelper brukeren til å gjennomføre oppgaven på en trygg måte. Passive sikkerhetsmekanismer skal derfor bygges inn slik at personell trygt kan gjennomføre ulike oppgaver i samhandlingsløsningen uten at løsningen blir kompromittert av personellet. Dette kan være teknisk validering av felter eller andre mekanismer som sørger for at feil gjort av helsepersonell ikke påvirker systemet. For eksempel kan det være hensiktsmessig å etablere mekanismer som sjekker at det ikke er uautorisert robotisert bruk av systemet eller API-er.

Et annet aspekt som kan understøtte dette prinsippet er *fail secure*- og *fail safe* mekanismer. At et system er *fail safe* eller *fail secure* betyr ikke at det ikke kan svikte, men snarere at systemets design forhindrer eller demper utrygge konsekvenser av systemets feil. Det vil si at hvis et slikt system feiler, forblir det like trygt som det var før feilen.

3.4 Videre arbeid med informasjonssikkerhet og personvern

Strategien for informasjonssikkerhet og personvern legger overordnede føringer for arbeidet med det skisserte målbildet for helhetlig samhandling.

Det vil være nødvendig å jobbe videre med informasjonssikkerhet og personvern i stegene som realiserer målbildet og gjennom videre forvaltning av de ulike løsningene for helhetlig samhandling. I det videre arbeidet må det gjennomføres konkrete risikovurderinger som beslutningsgrunnlag for utvikling og forvaltning av løsningene.

Alle virksomhetene som forvalter og benytter løsningene må også ha et bevisst forhold til informasjonssikkerhet og personvern, inkludert hensiktsmessig internkontroll og risikostyring. Informasjonssikkerhetshendelser skal ivaretas gjennom rapportering, vurdering, respons og læring.

Tredjepartsleverandører som skal bidra, for eksempel ved å utvikle tilleggsapplikasjoner basert på de API-ene som er tilgjengelige gjennom helhetlig samhandling, skal følge de til enhver tid gjeldende krav til informasjonssikkerhet og personvern.

Strategien forutsetter at roller og oppgaver i realiseringen av samhandlingsløsningene avklares. Videre at alle relevante lov- og forskriftskrav innen informasjonssikkerhet og personvern, samt Norm for informasjonssikkerhet og personvern (Normen) i helse- og omsorgssektoren, legges til grunn og følges av alle involverte virksomheter.

Vurderinger og konklusjoner fra risiko- og sårbarhetsvurderingen og den overordnede personvernvurderingen vil være utgangspunkt for det videre arbeidet med informasjonssikkerhet og personvern. Ved nye og endrede forhold som kan påvirke informasjonssikkerhet og personvern bør disse vurderingene eventuelt oppdateres. Ved utarbeidelse av mer detaljerte og konkrete risikovurderinger i den videre prosessen og DPIA skal det sees hen til de overordnede vurderingene.

Når det tas beslutninger og utarbeides retningslinjer for helhetlig samhandling vil denne strategien utgjøre en overordnet ramme. Prinsippene som beskrives i strategien legger føringene for det videre arbeidet med informasjonssikkerhet og personvern for helhetlig samhandling.

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Kontakt:
postmottak@ehelse.no