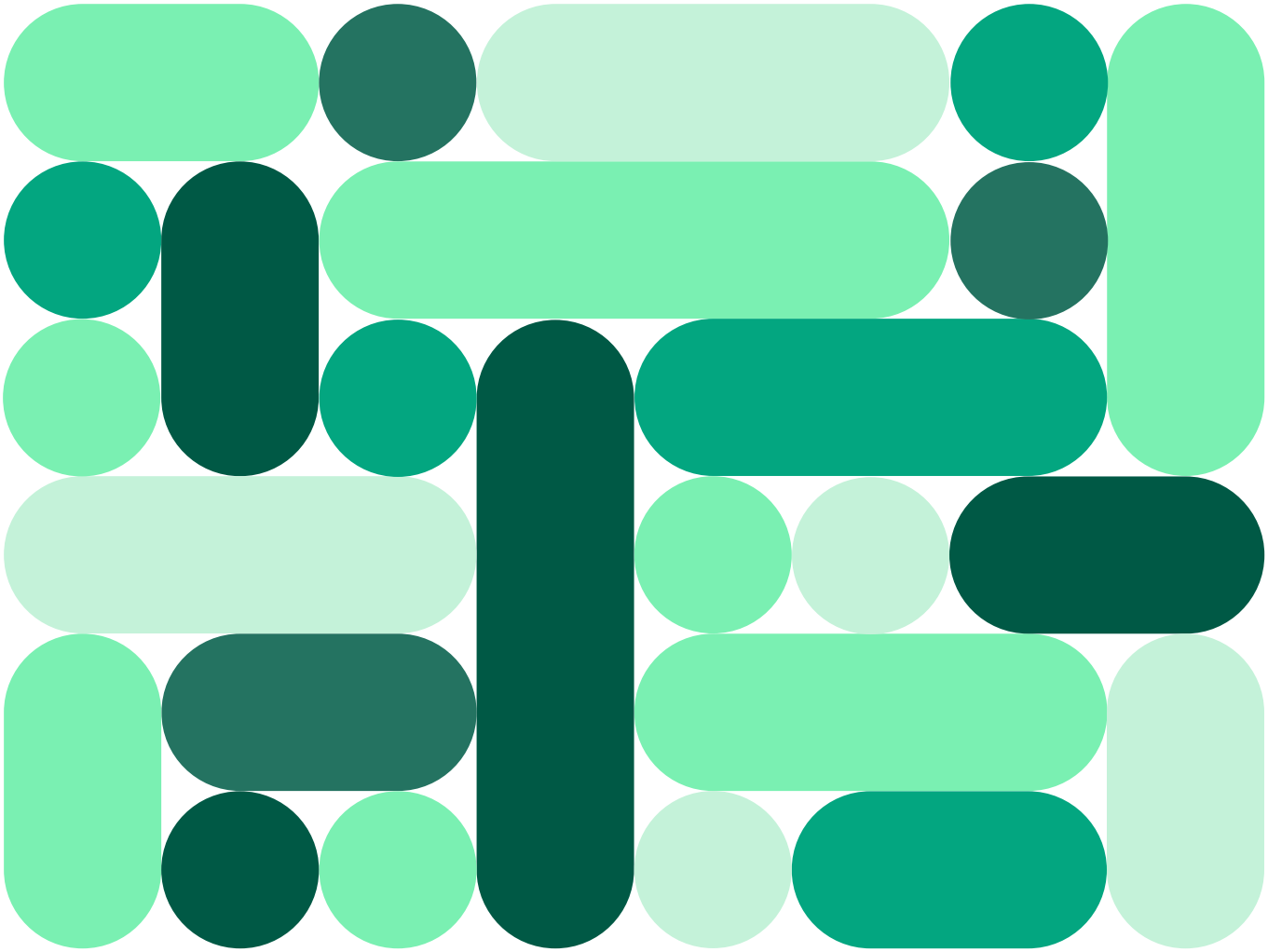
Norsk helsenett



Beskrivelse av tillitsrammeverk

8. mai 2023

Norsk helsenett

Dato	Versjon	Beskrivelse	Forfatter
09.05.2023		Første distribusjon ifm omfang av dokumentdeling leveransen planlagt tilgjengelig i september 2023	NHN

Denne rapporten er basert på følgende dokumenter:

Referanse #	Versjon	Dokumentnavn	Dokumentansvarlig

Innhold

1. Formål med dokument

Formål med dokumentet er å beskrive tillitsrammeverk som reflekterer de tillitsmekanismene som er i bruk i dag. Beskrivelsen er avgrenset mot fremtidige løsninger. Tillitsrammeverket utvikles med stegvis tilnærming basert på erfaring og behov for forbedring.

Beskrivelsen i dette notatet er delt inn i to deler:

1. Overordnet beskrivelse om hva tillitsrammeverket er; bakgrunn, behov og funksjonalitet.

2. Redegjørelse for de ulike mekanismene som inngår i tillitsrammeverket. Hvordan de fungerer slik at en skaper tillit, og hvordan de ulike stegene i en verdikjede følges opp av de ulike partene.

2. Bakgrunn – hvorfor et tillitsrammeverk?

Helsepersonell har behov for å kunne søke opp relevante og nødvendige helseopplysninger når de yter helsehjelp til pasienter, på en enkel og sikker måte. Behovet for enklere tilgang til relevante og nødvendige opplysninger gjelder uavhengig av hvor opplysningene er registrert. En slik tilgang til helseopplysninger bidrar til raskere og sikrere pasientbehandling. Digitale løsninger vil erstatte dagens manuelle prosesser og vil kunne være tidsbesparende i seg selv. Digitalisering innebærer imidlertid at en må håndtere utfordringer med store datamengder, ulike typer opplysninger og krav til tilgjengelighet.

Både pasienter og virksomhetene må være trygge på at det kun er helsepersonell med tjenstlig behov som gis tilgang til helseopplysninger. Tillitsrammeverket etablerer felles spilleregler som sikrer en felles aksept for personvern og informasjonssikkerhet i løsningen, på en måte som underbygger målet om økt pasientsikkerhet.

I helsesektoren blir det jevnlig hevdet at det er konflikt mellom hensynet til tilgjengelighet og hensynet til konfidensialitet. Det er imidlertid i pasientens interesse at relevante og nødvendige opplysninger er tilgjengelige for helsepersonell som yter helsehjelp. Det er også i pasientens interesse at opplysningene ikke tilflyter uvedkommende. Tillitsrammeverket legger til rette for at det ikke er motsetningsforhold mellom disse interessene.

2.1. Premisser for tillitsrammeverket

Tillitsrammeverket operasjonaliseres, forvaltes og håndheves sentralt av Norsk helsenett (NHN) slik at alle virksomheter som digitalt vil dele eller be om tilgang til helseopplysninger forholder seg til én organisasjon som kravstiller, legger til rette for funksjonalitet og er administrator.

Tillitsrammeverket skal i tillegg være:

1. Utformet for medlemmene i Helsenettet. Medlemskap i Helsenettet danner de ytre rammene for deling av helseopplysninger.

2. Skalerbart, slik at deling digitalt kan tas i bruk av mange virksomheter, mange systemer, og mange tjenester på en måte.

3. Økonomisk bærekraftig, slik at utviklings- og forvaltningskostnader er vurdert som hensiktsmessig.

4. Levert i henhold til akseptabel risiko, slik at forslag til tiltak vurderes mot implementeringskostnader og risiko som skal håndteres.

2.2. Overordnet beskrivelse av premisser for digital deling av opplysninger

Deling av helseopplysninger digitalt betyr at tilgjengeliggjøring av helseopplysninger utledes og behandles av maskiner i en helautomatisert prosess, uten menneskelig involvering.

Den tekniske prosessen gjennomføres på tvers av mange samarbeidende virksomheter og løsninger. For å sikre at rett mottaker får dataene må det settes opp løsninger for å verifisere identiteten til virksomheten, fagsystemet og personen som opplysninger skal tilgjengeliggjøres for. Prosess for deling av opplysninger i en verdikjede via Norsk helsenett som tiltrodd tredjepart kan beskrives i tre steg:

1. Det sendes en digital forespørsel for innhenting av opplysninger

2. En teknisk prosess som gjennomføres av maskiner vurderer om forespørselen er gyldig

3. Opplysninger gjøres tilgjengelig digitalt ved at det skjer en teknisk utlevering fra et system til et annet system.

Den maskinelle prosessen må gjennomføres i henhold til tekniske og semantiske spesifikasjoner som muliggjør digital samhandling. Det må også utarbeides rutiner for samhandlingen.

Det er ikke lenger tilstrekkelig for en helsevirksomhet å forholde seg til bare egne løsninger for tilgangskontroll, dokumentasjon og etterkontroll av tilgang. For å ivareta lovpålagte forpliktelser må helsevirksomheter og andre aktører som er involvert i den tekniske prosessen ha en felles tilnærming.

NHN er den tiltrodde tredjepart som sørger for at det er ulike mekanismer på plass for å skape tillit. Det er viktig å merke seg at tillit i denne sammenheng ikke er en følelse, men konkrete funksjoner som i sum bidrar til at en kjenner den digitale identiteten og at en vet at opplysninger utleveres til riktig adressat som har rett på å motta opplysningene.

Det lovpålagte ansvaret for de ulike behandlingsaktivitetene når det behandles person- og helseopplysninger utledes av personvernretten og suppleres med helserettslovgivningen. Det

formelle ansvaret for å behandle personopplysninger ligger alltid fast og kan ikke overdras eller delegeres på noen måte.

Hvem som gjør hva og ansvaret for en oppgaveutførelse i en digital samhandlingsløsning kan derimot avtales. Fordeling av oppgaver mellom partene som benytter en samhandlingsløsning beskrives delvis i bruksvilkår og i beskrivelse av tillitsrammeverket (dette dokumentet).

2.3. Begrepsliste

Nedenfor er en liste over begrep som er i bruk i dokumentet og en definisjon av begrepet i konteksten av tillitsrammeverk.

Begrep	**Definisjon**
1. Konsumerende virksomhet	Virksomheten som skal hente person- og helseopplysninger
2. Kilde	Virksomheten som opplysningene utleveres fra
3. Databehandler	En virksomhet som utfører oppgave på vegne av dataansvarlig. Databehandler kan være utleverende virksomhet for alle praktiske formål, men ikke dataansvarlig kilde
4. Verifisere	Å undersøke og fastslå/attestere riktigheten av noe
5. Kontrollere	Å undersøke eller sjekke
6. API	Et Application Programming Interface (API) er et teknisk programmeringsgrensesnitt som lar to eller flere programvarer kommunisere med hverandre. Et API kan brukes for å hente, lagre, oppdatere eller slette opplysninger. Et journalsystem kan bruke et API for å hente helseopplysninger digitalt på vegne av helsepersonellet.
7. Autentisering	Å bekrefte identiteten til en person, virksomhet eller programvare ved bruk av informasjonsteknologi.
8. Autorisering	Omfatter tilgangsstyring og tilgangskontroll av sluttbruker, programvare og virksomhet slik at riktige tilganger blir tildelt.
9. Identifikator	En verdi som unikt identifiserer noe eller noen.
10. Identitet	Opplysninger som forteller hvem eller hva noe eller noen er. For eksempel navn, rolle, stilling osv.
11. Identifisere	Å påvise eller gjenkjenne noe eller noen.

12. Identifikasjonsmiddel	Noe som brukes til å identifisere eller legitimere f.eks. en person, en virksomhet eller programvare. Et identifikasjonsmiddel kan være lagret digitalt eller befinne seg på en fysisk bærer, som f.eks. et smartkort.
13. eID	Elektroniske systemer som brukes for å legitimere brukere (fysiske personer) i datasystemer.
14. Samhandlingsløsning	En teknisk løsning som skal underbygge samhandling mellom helsepersonell i sektoren ved bruk av API. En samhandlingsløsning kan bestå av flere tekniske tjenester som tilbys av virksomhetene som legger til rette for samhandlingen.
15. Tillitstjeneste	Tillitstjeneste er en elektronisk tjeneste som normalt tilbys mot betaling og består av elektronisk signering, segl, tidsstempling, elektronisk tjenester for registrert sending og sertifikater for nettstedsautentisering. Se: Elektroniske tillitstjenester - Nkom

2.4. Et avtalebasert tillitsrammeverk for digital samhandling i helsesektoren

Medlemskap i Helsenettet samler virksomheter som både bruker og tilbyr tjenester, og tjenester som samler inn og tilgjengeliggjør helseopplysninger. Avtaler knytter identifiserte virksomheter i helsetjenesten og godkjente leverandører sammen i et nettverk. Forskrift om standarder og nasjonale e-helseløsninger pålegger virksomheter som yter helse- og omsorgstjenester etter spesialisthelsetjenesteloven, helse- og omsorgstjenesteloven, apotekloven og tannhelsetjenesteloven å ta i bruk Helsenettet. Det er bare medlemmer av Helsenettet som kan ta i bruk tjenester som bruker tillitsrammeverket for å dele helseopplysninger.

Medlemmene må ha en signert og gyldig kundeavtale og akseptere medlemsvilkår som stiller krav til hvordan virksomhetene håndterer sikkerheten i sin organisasjon og i sine løsninger. Spesielt relevant her er tilgangsstyring. Medlemsvilkårene innebærer at en forplikter seg til å følge Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.

Bruksvilkårene for de ulike tjenestene regulerer partenes roller og ansvar, oppgaver og forpliktelser. Før virksomheten kan ta i bruk en eller flere av tjenestene, skal bemyndiget representant for virksomheten akseptere vilkår for de tjenestene som tas i bruk.

Virksomhetens aksept av vilkårene for de enkelte tjenestene vil benyttes som en tilgangsstyring slik at det kun er medlemmene som får tilgang til å ta i bruk tjenesten som benytter tillitsrammeverket. Virksomheter som ikke har akseptert vilkår for bruk av tjenesten eller

HelseID får ikke tilgang til tjenesten. Tilgangen til disse tjenestene vil stenges dersom det avdekkes at virksomheten ikke tilfredsstiller kravene i vilkårene.

Forpliktelsene som kunden må akseptere ved å signere på bruksvilkår beskriver også de konkrete tillitsskapende mekanismene som benyttes av den enkelte tjenesten. Dette binder ulike mekanismer fra tillitsrammeverket sammen med bruksvilkårene for den enkelte tjeneste.

Ikke alle tjenester benytter samtlige tillitsskapende mekanismer som NHN tilbyr som en del av tillitsrammeverket. Hvilke mekanismer fra tillitsrammeverket som er relevant for den enkelte tjeneste beror på konkrete behov for hver enkelt verdikjede der en ser på aktørbildet, hvordan opplysninger skal utveksles og hvilke opplysninger som inngår.

2.5. Hvilke mekanismer har partene behov for?

Samtlige aktører som skal kunne dele opplysninger på tvers i en samhandlingsløsning har behov knyttet til punktene under. Behovene må identifiseres konkret, spesifiseres og løses for den enkelte samhandlingsløsning som skal benytte tillitsrammeverket.

1. Trygghet til virksomhetens identitet slik at identiteten er etterprøvbar, kontrollerbar og uavviselig.

2. Trygghet til helsepersonellets identitet slik at identiteten er etterprøvbar, kontrollerbar og uavviselig.

3. Trygghet til fagsystemets identitet slik at en vet at en digital henvendelse kommer fra et fagsystem som er benyttet i en identifisert helsevirksomhet og benyttes til helsehjelpsformål av helsepersonell.

4. Styring og kontroll av tilgang slik at utlevering av opplysninger digitalt kun skjer til helsepersonell med tjenstlig behov.

5. Beskrivelse av grunnlaget for tilgjengeliggjøring (tilgang) slik at helsevirksomheter kan ivareta etterkontroll, sporbarhet og personvern.

6. Sporbarhet slik at helsevirksomheter kan få en oversikt over alt som har skjedd i en hendelseskjede.

7. Etterkontroll slik at helsevirksomheter kan ivareta personvernrettigheter og følge opp eget personell.

8. Informasjonssikkerhet slik at risiko ved behandling av personopplysninger håndteres i hele den digitale delingsprosessen, herunder bidra til å sikre at maskiner, enheter og infrastruktur beskyttes fra trusler som kommer fra internett.

9. Beredskap der en har en forvaltning av tjenestene slik at både helsevirksomheter, databehandlere og NHN er beskyttet fra uønskede hendelser.

Helsevirksomhetene skal ha reel innflytelse om videreutvikling av tillitsrammeverk ved å prioritere og gi innspill til NHN i en etablert forvaltningsprosess. NHN ønsker derfor at sektoren

prioriterer sine behov og at NHN vurderer behovene når de utvikler tjenestene til det beste for sektoren.

2.6. Tjenstlig behov for opplysninger

Tjenstlig behov er et begrep som i denne sammenheng knyttes opp mot at opplysninger er vurdert til å være nødvendige og relevante for å yte forsvarlig helsehjelp.

Det er den enkelte helsevirksomhet som beslutter hvilke verktøy og tilganger helsepersonellet skal benytte i sin oppgaveløsning. Vurderingen beror på flere forhold, herunder rolle, ansvar og kompetanse mv. Dette styrer hvilke opplysninger helsepersonellet kan innhente, gitt at man i det enkelte tilfellet vurderer at vilkårene er oppfylte.

Det er *helsepersonellets* egen vurdering som ligger til grunn for om opplysninger er relevante og nødvendige for å yte helsehjelp i kontekst av en gitt helsehjelpssituasjon. Det er viktig å merke seg at helsepersonellets beslutning om eget tjenstlig behov, altså om informasjon som ble vurdert til å være relevant og nødvendig aldri kan overprøves av en digital samhandlingsløsning.

Samtlige av disse vurderingene må inngå for å oppfylle kravet til at helsepersonellet skal ha et "tjenstlig behov", men ikke alle vurderingene som kreves er hensiktsmessige eller egnet til å inngå i den tekniske samhandlingsløsningen for å beskrive et "tjenstlig behov" på en presis måte. Trygg digitalisering effektiviserer arbeidsprosessene slik at menneskelig intervensjon ikke lenger er nødvendig.

Partene har behov for at de digitale delingsprosessene *underbygger* tjenstlig behov til den som ber om tilgang. Dette betyr at kilden må ha ha tilstrekkelig tiltro til at tilgjengeliggjøring skjer i henhold til regelverkets krav og at en digital forespørsel er riktig, og gjort ut fra et tjenstlig behov. Hvordan dette skal gjennomføres i praksis løses ved at en har mekanismer for å enten verifisere informasjon (tilgangskontroll) eller hente frem påstander (loggført informasjon) som i sum gir etterprøvbarhet for handlinger som er foretatt i en digital samhandlingsløsning.

2.7. Hvordan underbygge at tjenstlig behov foreligger i en digital samhandlingsløsning

Når et helsepersonell har besluttet at opplysninger søkes opp og innhentes digitalt har både kilden til opplysningene og konsumenten behov for å kunne legge til grunn at dette var riktig forespørsel, dette fremgår av lovpålagte forpliktelser som påhviler helsevirksomheten.

For å underbygge tjenstlig behov er det relevant at tre konkrete identiteter verifiseres gjennom den tekniske prosessen. De følgende tre stegene vil gi kilden (utleverende virksomhet) tilstrekkelig tiltro til at det foreligger en gyldig forespørsel:

1. Kommer henvendelsen fra en helsevirksomhet der det ytes helsehjelp? I tillitsrammeverket inngår systemteknisk støtte for virksomhetsidentifisering som skaper

tiltro til at konsumerende virksomhet er en helsevirksomhet.

2. Kommer henvendelsen fra et fagsystem som benyttes i helsehjelpsøyemed i en helsevirksomhet? I tillitsrammeverket inngår systemteknisk støtte for identifisering av fagsystemet som skaper tiltro til fagsystemet som sender forespørsel om opplysninger.

3. Er det et helsepersonell og er helsepersonellet den det gir seg ut for å være? I tillitsrammeverket inngår systemteknisk støtte for autentisering som skaper tiltro til helsepersonellets identitet.

I alle de tre stegene må det følge informasjon som gjør at den enkelte forespørsel om digital innhenting av helseopplysninger både kan benyttes for teknisk tilgangskontroll og for å kunne undersøke tilgang og utlevering av opplysninger. Dette er nødvendig for å få til *trygg digitalisering* på tvers av omsorgssektoren.

3. Hvordan oppnå nødvendig tiltro for en trygg digitalisering?

Tillitsrammeverk tilbyr mekanismer som skaper trygghet til deling opplysninger digitalt. Mekanismene tilbys i 2 faser; forberedende fasen som gjennomføres før en samhandlingsløsning blir tilgjengelig for bruk og i kjøretid når en digital forespørsel for tilgang blir behandlet maskinelt.

Mekanismene i tillitsrammeverk leverer følgende:

1. Identifisering av helsevirksomheten, dvs. identifisere juridisk person
2. Identifisering og autorisering av journalsystem/EPJ
3. Identifisering og autentisering av helsepersonellet
4. Teknisk sikkerhet i digitale kommunikasjonen.

3.1. Identifisering av helsevirksomheten, dvs. identifisere juridisk person

Det er behov for å skape tiltro til at virksomhetene som skal konsumere eller dele helseopplysninger er en juridisk person som har ansatte som yter helsehjelp slik at virksomhetene kan være trygge på at de samhandlende partene har rettslig grunnlag for å behandle opplysningene.

3.1.1. Mekanismer i forberedende fase

NHN gjør det mulig for virksomheter å bli medlem av Helsenettet og å signere vilkår for bruk av tjenesten:

1. NHN tilbyr vilkår for medlemskap i helsenettet.

2. NHN definerer vilkår for bruk av samhandlingsløsninger som deler helseopplysninger.

3. NHN håndterer og forvalter inngåtte avtaler for medlemskap og bruk av tjenester som deler helseopplysninger.

4. NHN registrerer og ajourholder medlemmer av helsenettet som har godtatt vilkår for deling av helseopplysninger mellom medlemmer i helsenettet.

NHN gjør det mulig for virksomheter å identifisere seg ved digitale forespørsler om tilgang til helseopplysninger.

1. NHN tilbyr identifisering av virksomhet ved bruk av to typer identifikasjonsmidler
    a. Systemspesifikke identifikasjonsmiddel som er opprettet av NHN og som bare kan benyttes i forespørsler mot HelseID
    b. Virksomhetssertifikater utstedt av en organisasjon som tilbyr tillitstjenester i henhold til eIDAS-forordningen.

2. NHN tilbyr en løsning via Altinn, hvor den konsumerende helsevirksomheten kan delegere en rett til å opptre på sine vegne til sin databehandler.

3.1.2. Mekanismer i kjøretid

Ved digitale forespørsler identifiserer NHN den konsumerende virksomheten, og videreformidler identiteten til kilden.

1. NHN identifiserer virksomheten som ber om tilgang ved bruk av identifikasjonsmiddelet
    a. Dersom virksomheten som er knyttet til det identifikasjonsmiddelet er en databehandler må databehandler angi hvilken helsevirksomhet den opptrer på vegne av i tilgangsforespørselen. NHN utfører en kontroll av at helsevirksomheten har gitt sin databehandler denne retten i Altinn.

2. NHN videreformidler virksomhetens identitet til kilde, både konsumerende virksomhetens identitet og eventuelt databehandler

3.2. Identifisering og autorisering av journalsystem/EPJ

Identiteten til journalsystemet /EPJ som benyttes av helsepersonell til å innhente helseopplysninger skal være etterprøvbar, kontrollerbar og uavviselig.

3.2.1. Mekanismer i forberedende fase

1. Virksomheten må registrere sine journalsystem/EPJ (programvare) som benyttes av sitt helsepersonell hos NHN slik at NHN kan identifisere og etablere tillit til programvaren.

2. Virksomhetens journalsystemer/EPJ må tildeles en rett til å konsumere API og andre tjenester i NHN sine systemer for tilgangsstyring av APIer og tjenester.

3.2.2. Mekanismer i kjøretid

1. NHN autentiserer programvaren.

2. NHN kontrollerer at programvaren har rett til å bruke det aktuelle APIet.

3.3. Identifisering og autentisering av helsepersonellet

Identiteten til helsepersonellet skal være etterprøvbar, kontrollerbar og uavviselig.

3.3.1. Mekanismer i forberedende fase

1. NHN sørger for at identifikasjonsmidler og autentiseringsløsninger som skal brukes til autentisering av fysisk person leveres med en høy grad av sikkerhet.
    a. NHN stiller tekniske og sikkerhetsmessige krav i form av vilkår for tilknytning til HelseID.
    b. Vilkårene må aksepteres av identitetstilbydere som skal tilby sin autentiseringsløsning i HelseID
    c. Konsumerende virksomhet har ansvaret for at egne ansatte har identifikasjonsmidler som benyttes i HelseID og at de benytter en autentiseringsløsning som tilfredsstiller kravene i vilkårene
    d. NHN kontrollerer at kravene er ivaretatt før autentiseringsløsningen tilknyttes HelseID
    e. NHN tilgjengeliggjør autentiseringsløsninger som tilfredsstiller gjeldende krav i HelseID
    f. NHN holder oversikt over identifikasjonsmidler og identitetstilbydere som kan brukes til autentisering av helsepersonell for tilgang til helseopplysninger

2. NHN stiller krav til at journalsystem/EPJ som skal benytte HelseID integreres i henhold til gjeldende tekniske og sikkerhetsmessige spesifikasjoner i form av vilkår for bruk av tjenesten. Vilkårene må aksepteres av den konsumerende virksomheten, som har ansvar for å sørge for at vilkårene blir møtt i sine systemer.
    a. NHN kontrollerer at journalsystem/EPJ som skal integreres med HelseID etterlever kravene

3.3.2. Mekanismer i kjøretid

1. NHN sørger for at fysisk person blir autentisert i henhold til gjeldende krav ved forespørsel om tilgang til tjenester for å få tilgang til helseopplysninger.

2. Om fysisk person er et helsepersonell utledes implisitt:
    a. At juridisk person er en virksomhet som har ansatte som yter helsehjelp (avsnitt 2.1), og dermed er pliktig til å tilby et behandlingsrettet helseregister til sitt helsepersonell
    b. At helsepersonellet bruker et journalsystem som benyttes ved for å journalføre helsehjelpen som blir gitt (avsnitt 2.2)

c. At fysisk person bruker et journalsystem som tilbys av juridisk person som yter helsehjelp (avsnitt 2.4)

3.4. Teknisk sikkerhet i digitale kommunikasjonen

Partene som skal dele helseopplysninger må være trygge på at den tekniske kommunikasjonen er sikret på en tilfredsstillende måte. Systemene som samhandler må være motstandsdyktige mot sikkerhetsangrep. I tillegg må opplysningenes dataintegritet og pasientens konfidensialitet ivaretas.

3.4.1. Mekanismer i forberedende fase

NHN stiller krav som tilfredsstiller behov for teknisk sikkerhet for kommunikasjonsformål og kontrollerer at krav er ivaretatt.

3. NHN stiller tekniske og sikkerhetsmessige krav i form av tekniske spesifikasjoner for bruk av HelseID som tas i bruk av:
    a. konsument virksomhet sitt journalsystem i integrasjon med HelseID
    b. kildens journalsystem /EPJ
    c. NHN

4. NHN kontrollerer at et utvalg av disse kravene er ivaretatt ved å kontrollere at den tekniske integrasjonen mellom den konsumerende virksomheten sitt journalsystem og HelseID før tjeneste er tilgjengelig i produksjon.

3.4.2. Mekanismer i kjøretid

NHN kontrollerer at tekniske og sikkerhetsmessige krav er ivaretatt og avbryter kommunikasjon ved avvik. NHN kontrollerer:

1. At kommunikasjon transporteres over krypterte linjer.

2. At autentiserings- og autorisasjonsprotokoller brukes på i henhold til gjeldende sikkerhetsprofil.

I tillegg NHN Helse-CERT overvåker og håndterer også generelle sikkerhetshendelser.