NORMEN

# Kommunikasjon over åpne nett (faktaark 24)

Versjon 5.0
04.02.2021

Utarbeidet med støtte fra direktoratet for e-helse
Vedtatt av styringsgruppen for Normen

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

| | |
|---|---|
| Tema for faktaarket | Dette faktaarket omhandler kommunikasjon over åpne net. Formålet med faktaarket å ivareta tilfredsstillende sikkerhet ved elektronisk kommunikasjon av helseog personopplysninger over åpne nett<br><br>De fleste kommunikasjonsnett er i utgangspunktet åpne nett, for eksempel internett eller usikrede trådløse nettverk. Informasjon som sendes i slike nett kan leses av de som får tilgang. Ved bruk av kryptering, sikker autentisering mv. vil informasjonen blir sikret mot uautorisert tilgang.<br><br>Ved etablering av løsninger for kommunikasjon over åpne nett skal det gjennomføres en risikovurdering. |
| Dette faktaarket er spesielt relevant for | Målgruppen for faktaarket er:<br>• Leverandør<br>• IKT-ansvarlig<br>Sikkerhetsleder / sikkerhetskoordinator<br>• Virksomhetens<br>• leder/ledelse<br>• Databehandler |
| Krav i Normen | Faktaarket gjelder for følgende kapitler i Normen<br>• Normen kapittel 5.2.2 Autentisering<br>• Normen kapittel 5.3.5 Kryptering<br>• Normen kapittel 5.5.3.1 Krav til elektronisk samhandling<br>• Normen kapittel 5.5.3.3 Datadeling i sanntid<br>• Normen kapittel 5.5.4 E-post og SMS<br>• Normen kapittel 5.9 Nødrutiner |
| Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk | Følgende lov- og forskriftsbestemmelser er spesielt relevante for faktaarket:<br>• Sikring av kommunikasjon med TLS, Nasjonal sikkerhetsmyndighet( NSM)<br>• NSM Cryptographic recommendations v 1.0, NSM<br>• NSMs grunnprinsipper for IKT-sikkerhet v 2.0<br>• Referansekatalogen for IT-standarder, Digitaliseringsdirektoratet |

# Kommunikasjon over åpne nett

I Normen er det krav om tekniske tiltak slik at all kommunikasjon av helse- og personopplysninger utenfor virksomhetens kontroll krypteres. Dette gjelder åpne nett Åpne nett er kommunikasjonskanaler virksomheten selv ikke har vurdert som godkjent for å overføre helseopplysninger uten ekstra tiltak. Kommunikasjonskanaler som benytter åpne nett brukes mellom virksomheter og innad i en virksomhet. Eksempler på åpne nett som ikke er tilstrekkelig sikret for kommunikasjon av helseopplysninger er internett og mobilnett (3G/4G).

Helsenettet er et åpent nett og må sikres på samme måte som andre åpne nett.
Ved bruk av kryptering, sikker autentisering mv. vil informasjonen bli sikret mot uautorisert tilgang.

Følgende er eksempler på tilstrekkelig sikring av åpne nett dersom anbefalte sikkerhetsnivåer er benyttet:

- TLS (Transport Layer Security) benyttes for eksempel til kryptert webtrafikk (HTTPS)
- Kryptert VPN (Virtual Private Network) benyttes ofte til sikker fjerntilgang

Ved etablering av løsninger for kommunikasjon over åpne nett skal det gjennomføres en risikovurdering.
Tabellen som følger gir nærmere beskrivelser av hvordan konkrete krav kan løses.

**1. Autentisering og korrekt adressering av kommunikasjonspartner**

Ved kommunikasjon mellom to parter over et åpent nett er det viktig at partene på en sikker måte kan autentisere seg for hverandre. Sikker autentisering er viktig for å verifisere at kommunikasjonsparten faktisk er den som den utgir seg for å være. Dette kan for eksempel gjøres ved å bruke PKI1[1] og virksomhetssertifikater[2] Adressering skal være sikret. Det vil si at man skal være sikker på at benyttet adresse er korrekt.

Mottaker må være tilstrekkelig presist identifisert. Et eksempel på utilstrekkelig identifisering vil være forsendelse av taushetsbelagte helseopplysninger til et legekontors organisasjonsnummer i Altinn, hvis dette innebærer at regnskapsfører vil få tilgang til opplysningene.vil få tilgang til opplysningene.

[1] Public Key Infrastructure – Se faktaark 49
[2] Norske myndigheter har startet et arbeid med å se på utfordringer med bruk av virksomhetsidentiteter ved samhandling og har som mål å publisere en beste praksis for autentisering av virksomheter i 2021.

## 2. Autentisering av personer/brukere

Autentisering skal foregå på en sikker måte når det blir gitt tilgang til helse- og personopplysninger mellom virksomheter. Ved autentisering av personer som kommuniserer helseopplysninger over et åpent nett skal den autoriserte brukeren autentiseres med sikker autentiseringsløsning. Dette innebærer at den autoriserte skal bekrefte sin identitet på en sikker måte. Sikker måte må besluttes på grunnlag av en risikovurdering.

Sikring av konfidensialitet og integritet:

Ved overføring av helse- og personopplysninger over åpne nett skal opplysningene sikres mot at uvedkommende får kjennskap til opplysningene. I tillegg skal overføringen være sikret mot utilsiktet eller uautorisert endring eller sletting.

All overføring av helse- og personopplysninger over åpne nett må derfor alltid krypteres slik at innholdet i overføringen alltid er uleselig for andre enn mottakende virksomhet.

Kommunikasjonskanaler som benytter åpne nett for kommunikasjon av helse- og personopplysninger skal som et minimum alltid krypteres. Det finnes flere alternative metoder for slik kryptering, jf. NSMs grunnprinsipper for IKT-sikkerhet v. 2.0 punkt 2.7.4. Krypter alle trådløse forbindelser, og krypter kablede nettverk som er utenfor fysisk kontroll (2.4.2). For mer informasjon, se også veiledning fra NSM for sikring av kommunikasjon med TLS.

Kryptering er bare effektivt så lenge nøkler beskyttes. Private nøkler og passord må beskyttes mot uvedkommende. Sørg for at sertifikater er signert av en betrodd part eller etabler en egen strategi for håndtering av kryptografi i virksomheten, jf. NSMs grunnprinsipper for IKT-sikkerhet v 2.0 punkt 2.7.1.

Dersom man etter risikovurdering kommer frem til at det må benyttes innholdskryptering, må det sørges for at kommunikasjonsmetoden støtter dette på en standardisert måte.

## 4. Sikring av tilgjengelighet

Ved kommunikasjon over åpne nettverk er det viktig at virksomheten tar høyde for at kommunikasjonen kan bli brutt. Dette for å sikre evnen til vedvarende tilgjengelighet til helse- og personopplysninger. Det skal også gjennomføres tiltak for å gjenopprette tilgjengeligheten og tilgangen til helse- og personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse.

Bruk av sanntidskommunikasjon over åpne nett er sårbar for utilgjengelighet. For tjenester med behov for høy oppetid er det viktig å sørge for at løsninger som tilbyr tilgang til helse- og personopplysninger over åpne nett har tilstrekkelig robusthet. Dette kan oppnås ved å ha gode testrutiner som tester robusthet og ha redundante komponenter med overvåking.

I tillegg må virksomheter som benytter slike løsninger over åpne nett ha rutiner på hvordan brukere skal forholde seg til utilgjengelighet. Dersom utilgjengelighet ikke kan aksepteres, må det etableres egnede nødprosedyrer som beskrevet i Faktaark 11.

For mer informasjon vises til NSMs grunnprinsipper for IKT-sikkerhet v 2.0 punkt 2.2.7.

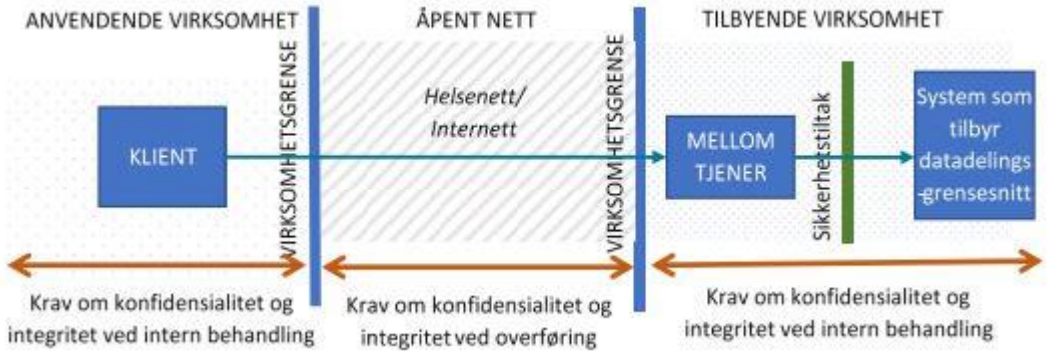
## 5. Sikring ved datadeling over åpne nett

Datadeling er deling av strukturerte data mellom virksomheter i sanntid.

Et datadelingsgrensesnitt er et grensesnitt/API[3] [3] som tilgjengeliggjør en virksomhet sine data, for eksempel helseopplysninger, for andre virksomheter, over åpne nett ved bruk av webteknologi.

Krav til konfidensialitet og integritet må sikres ved bruk av et datadelingsgrensesnitt over åpne nett.

Figuren under viser en skjematisk, forenklet skisse av bruk av datadelingsgrensesnitt.




Tilbyende virksomhet er dataansvarlig for informasjonen som tilgjengeliggjør helseog personopplysninger til innbyggere eller brukere med tjenstlig behov gjennom et datadelingsgrensesnitt.

Anvendende virksomhet har en klient som brukes for å aksessere et datadelingsgrensesnitt med sensitiv informasjon hos en annen virksomhet. Anvendende virksomhet kan være en annen dataansvarlig, en databehandler som har en databehandleravtale med tilbyende virksomhet eller en innbygger som får tilgang til egne helseopplysninger.

En eller flere mellomtjenere kan stå mellom klienter og selve datadelingsgrensesnittet. En mellomtjener kan tilby utvidet funksjonalitet slik som transformering av innhold, bytte av teknisk protokoll osv. En av mellomtjenerne bør ha funksjonalitet for å godkjenne trafikk fra klienter man stoler på. Alle godkjenninger og avvisninger skal logges. En mellomtjener skal unngå mellomlagring og logging av sensitiv informasjon. Der data må mellomlagres skal det ikke lagres lengre enn nødvendig. For eksempelet ved trafikkinspeksjon vil det si at data skal slettes i det inspeksjonen er gjennomført. Kun autorisert driftspersonell skal ha tilgang til mellomtjenere.

En virksomhetsgrense rammer inn virksomhetens ansvar og kontrollområde. Innenfor sin virksomhetsgrense kan virksomheten inngå avtale med leverandører som da blir databehandlere, for eksempel ved drift av mellomtjener. Krav til konfidensialitet og integritet ved overføring av helseopplysninger over åpne nett gjelder fra virksomhetsgrense til virksomhetsgrense.

Krav til sikring av kommunikasjonskanal er beskrevet i punkt 3. Hver virksomhet må innenfor sin virksomhetsgrense følge krav til konfidensialitet og integritet ved sin egen behandling av helseopplysninger. Sikkerhets- og samhandlingsarkitektur ved intern samhandling (faktaark 20b) omhandler dette temaet.

[3] Application Programming Interface

Prinsippene gjelder også for andre anvendelser av API-er, for eksempel i en nettløsning der det benyttes nettlesere som klienter, eller bruk av datadeling innad i en virksomhet som benytter åpne nett mellom klient og tjener.

**6. Fjernaksess**

Det henvises til Veileder for fjernaksess mellom virksomhet og leverandør

**7. E-post**

E-postløsninger som sender meldinger i klartekst skal aldri benyttes for utveksling av helse- og personopplysninger. Dette gjelder bl.a. internt i en virksomhet og til kommunikasjon med pasienter. For kommunikasjon til pasienter skal det benyttes løsninger som sørger for sikker kommunikasjon, for eksempel via et webgrensesnitt, og som sørger for at helse- og personopplysninger ikke overføres ukryptert eller hvor det forutsettes at dokumentet må lastes ned på pasienten/brukerens utstyr.

For ytterligere detaljer henvises det til veileder i digital pasientkommunikasjon.

For mer informasjon om beskyttelse av e-post og nettleser henvises til NSMs grunnprinsipper for IKT-sikkerhet v. 2.0 punkt 2.8.

**7. Hendelsesregistrering**

Dersom man har tjenester som er tilgjengelige i et åpent nett er det viktig å registrere hvem som har hatt tilgang til tjenesten. Eksempelvis i en tjeneste for pasient-lege kommunikasjon må alle tilganger til tjenesten registreres, slik at det i ettertid er mulig å finne ut om det er gjort urettmessige tilganger.

For mer informasjon om hendelsesregistrering henvises til NSMs grunnprinsipper for IKT-sikkerhet v. 2.0 punkt 3.2.4.

**8. Rammeverk for sikker meldingskommunikasjon (ebXML)**

Overføring av meldinger i et åpent nettverk må sikres dersom man ønsker å forhindre uautorisert innsyn i oversendt informasjon. ebXML-rammeverket er en internasjonal standard for meldingsutveksling, som kan ivareta krav til sikker kommunikasjon. Rammeverket beskriver blant annet hvordan sikkerhetstiltak som for eksempel kryptering og signering av meldinger kan ivaretas.