Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

# Kommunikasjon over åpne nett

**Støttedokument**
**Faktaark nr 24**
Versjon: 4.0
Dato: 27.09.2018

| | | | |
|---|---|---|---|
| **Formål** | Å ivareta tilfredsstillende sikkerhet ved elektronisk kommunikasjon av helse- og personopplysninger over åpne nett. | | |
| **Ansvar** | IKT-ansvarlig skal sørge for at kommunikasjon over åpne nett blir sikret. | | |
| **Gjennomføring** | Ved bruk av åpne nett til kommunikasjon av helse- og personopplysninger. | | |
| **Omfang** | Alle virksomheter som kommuniserer over åpne nett. | | |
| **Målgruppe**<br><br>Dette faktaarket er spesielt relevant for: | ☒ Leverandør<br>☒ IKT-ansvarlig<br>☐ Forsker<br>☐ Prosjektleder | ☒ Sikkerhetsleder / sikkerhetskoordinator<br>☒ Virksomhetens leder/ledelse<br>☐ Forskningsansvarlig | ☐ Medarbeider/ansatt<br>☒ Databehandler<br>☐ Personvernombud |
| **Hjemmel** | Personvernforordningen artikkel 32 | | |
| **Referanser** | • Veileder for fjernaksess mellom leverandør og virksomhet<br>• Sikring av kommunikasjon med TLS, Nasjonal sikkerhetsmyndighet | | |

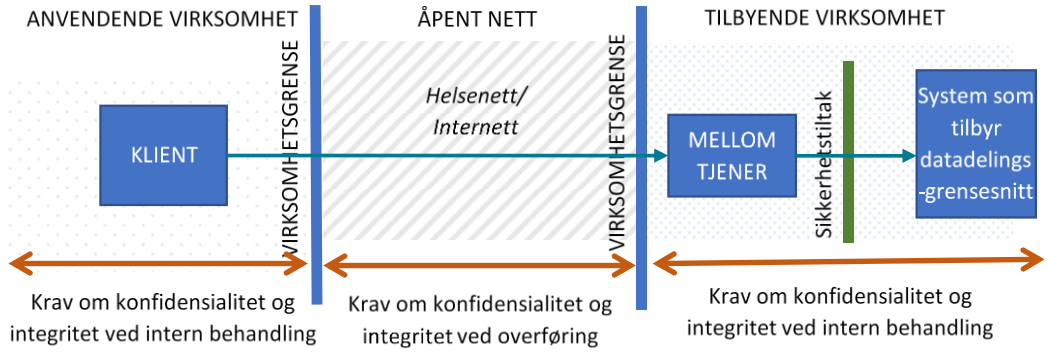
Innholdet i dokumentet er gjennomgått og oppdatert ut fra Normen 5.3, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning

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 offentlige nett, mobilnett(3G/4G) og internett. Videre er eksempler på tilstrekkelig sikring av åpne nett VPN, TLS og IPsec der anbefalte sikkerhetsnivåer er benyttet.
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.

Ved etablering av løsninger for kommunikasjon over åpne nett skal det gjennomføres en risikovurdering.

| Nr | Handling/Utførelse |
|---|---|
| **1.** | **Autentisering og korrekt adressering av kommunikasjonspartner**<br>Ved kommunikasjon mellom to parter over et åpnet 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 PKI og virksomhetssertifikater. Adressering skal være sikret. Det vil si at man skal være sikker på at benyttet adresse er korrekt.<br><br>Mottaker må være tilstrekkelig presist identifisert. Et eksempel på utilstrekkelig identifiseirng vil være forsendelse av taushetsbelagte helseopplysninger til et legekontors organisasjonsnummer i Altinn, hvis dette innebærer at regnskapsfører vil få tilgang til opplysningene. |
| **2.** | **Autentisering av personer/brukere**<br>Normen setter krav til at det skal benyttes sikker autentiseringsløsning når det blir gitt tilgang til helseopplysninger for personell fra andre virksomheter. Ved autentisering av personer som kommuniserer helseopplysninger over et åpent nett anbefales det sikker autentisering. Dataansvarlig kan gjennom risikovurdering evt. konkludere med at lavere nivåer kan benyttes dersom andre tiltak totalt sett gir en god nok sikkerhet. |
| **3.** | **Krav til konfidensialitet og integritet:** |

| Nr | Handling/Utførelse |
|---|---|
| | 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.<br><br>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.<br><br>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. Dette faktaarket viser til Nasjonal Sikkerhetsmyndighet sin anbefaling for slik kryptering.<br><br>Dersom man etter risikovurdering kommer frem til at man må benytte innholdskryptering, må man sørge for at kommunikasjonsmetoden støtter dette på en standardisert måte. |
| **4.** | **Sikring av tilgjengelighet**<br><br>I henhold til EU sin personvernforordning artikkel 32, skal det gjennomføres egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. 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.<br><br>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.<br><br>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 reserveløsninger og/eller manuelle rutiner. |
| **5.** | **Sikring ved datadeling over åpne nett**<br>Datadeling er deling av strukturerte data mellom virksomheter i sanntid.<br><br>Et datadelingsgrensesnitt er et grensesnitt/API som tilgjengeliggjør en virksomhet sine data, for eksempel helseopplysninger, for andre virksomheter, over åpne nett ved bruk av webteknologi.<br><br>Krav til konfidensialitet og integritet må sikres ved bruk av et datadelingsgrensesnitt over åpne nett.<br><br>Figuren under viser en skjematisk, forenklet skisse av bruk av datadelingsgrensesnitt. |

| Nr | Handling/Utførelse |
|---|---|
| |  <br><br>Tilbyende virksomhet er dataansvarlig for informasjonen som tilgjengeliggjør helse- og personopplysninger til innbyggere eller brukere med tjenstlig behov gjennom et datadelingsgrensesnitt.<br><br>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.<br><br>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.<br><br>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.<br><br>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. Faktaark 20b – Sikkerhetsarkitektur ved intern samhandling omhandler dette temaet.<br><br>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**<br>Det henvises til faktaark 36 og veileder for fjernaksess for detaljer om fjernaksess |

| Nr | Handling/Utførelse |
|---|---|
| **7.** | **E-post**<br>E-postløsninger som sender meldinger i klartekst skal aldri benyttes for utveksling av helse- og personopplysninger. Dette gjelder både internt i en virksomhet, til kommunikasjon med pasienter osv. 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 blir liggende på brukerens lokale PC.<br><br>For ytterligere detaljer henvises det til veileder i bruk av portalløsninger, SMS og e-post. |
| **8.** | **Hendelsesregistrering**<br>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 om det er gjort urettmessige tilganger. |
| **9.** | **Rammeverk for sikkert meldingskommunikasjon (ebXML)**<br>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.<br><br>For mer informasjon henvises det til Faktaark 16 - Etablering av løsning for meldingskommunikasjon. |