

 <p>Norm for informasjonssikkerhet www.normen.no</p>	Utgitt med støtte av: 
<h2>Kommunikasjon over åpne nett</h2>	<b>Støttedokument</b> <b>Faktaark nr 24</b> Versjon: 2.1 Dato: 15.12.2010

<b>Målgruppe</b>  Dette faktaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder / sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
<b>Ansvar</b>	IKT-ansvarlig skal sørge for at kommunikasjon over åpne nett blir sikret.		
<b>Gjennomføring</b>	Ved bruk av åpne nett til kommunikasjon av helse- og personopplysninger.		
<b>Formål</b>	Å ivareta tilfredsstillende sikkerhet ved elektronisk kommunikasjon av helse- og personopplysninger over åpne nett.		
<b>Omfang</b>	Alle virksomheter som kommuniserer over åpne nett.		
<b>Hjemmel</b>	Personopplysningsforskriften §§ 2-11, 2-12 og 2-13		
<b>Referanser</b>	<ul style="list-style-type: none"> <li>• Veileder i informasjonssikkerhet ved tilknytning mellom kommuner, fylkeskommuner og helsenettet</li> <li>• Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet</li> <li>• Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, april 2008</li> </ul>		

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.

Norsk Helsenett er et åpent nett og må sikres på samme måte som andre åpne nett.

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

Nr	Handling/Utførelse
1.	<b>Autentisering av kommunikasjonspartner</b> 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 PKI og virksomhetssertifikater.
2.	<b>Autentisering av personer/brukere</b> Ved autentisering av personer som kommuniserer helseopplysninger over et åpent nett skal det benyttes sikkerhetsnivå 4 for autentisering.
3.	<b>Kryptering av informasjon</b> Opplysninger sendt over et åpent nett sendes i utgangspunktet over i klartekst slik at de kan leses dersom nettet avlyttes. Helse- og personopplysninger sendt over et åpent nett må derfor krypteres slik at innholdet i opplysningene er uleselig for andre enn mottaker. Krypteringsstyrke skal være iht. gjeldende krav.
4.	<b>Kryptering av kommunikasjonskanal</b> Alternativt til å kryptere selve informasjonen kan en kryptere kommunikasjonskanalen som informasjonen sendes over. Både SSL (Secure Sockets Layer) og TLS (Transport Layer Security) kan brukes for å etablere en kryptert kommunikasjonskanal. SSL er primært for å kryptere oversendt informasjon over nettet og benyttes mye for eksempel på nettsted hvor Internettbrukere skal oversende helse- og personopplysninger. TLS er primært for å sette opp en sikker kommunikasjonskanal mellom klient/serverapplikasjoner som kommuniserer helse- og personopplysninger over et åpent nett.

Nr	Handling/Utførelse
	Andre metoder for å sikre kommunikasjonskanaler er for eksempel VPN (Virtuelt Privat Nettverk) eller IPSec (Internet Protocol Security).
5.	<p><b>Sikkerhet i tilkoblingsløsningen til Norsk Helsenett</b></p> <p>Norsk Helsenett utplasserer en teknisk sikkerhetsløsning som virksomheten må forholde seg til og inkorporere i sitt eget nettverk. Sikkerhetstiltakene fra Norsk Helsenett utgjør en del av sikkerheten i tilkoblingsløsningen. Eksempler på sikkerhetstiltak er at Norsk Helsenett:</p> <ul style="list-style-type: none"> <li>– utplasserer en sikkerhetsbarriere (ruter/brannmur) som er ferdigkonfigurert inn mot virksomhetens sikre sone. Hovedhensikten med ruterer er å sikre helsenettet og aktører i helsenettet.</li> <li>– gjennomfører sentrale tiltak for å hindre at ondsinnet programvare sprer seg til/fra kunder i helsenettet</li> <li>– gir garanti for bl.a. opptid og tjenestekvalitet i nettet etter avtale med kunden</li> <li>– gjennomfører overvåkning av nettet fra og med utplassert sikkerhetsbarriere i virksomheten</li> </ul> <p>Følgende ivaretas ikke av Norsk Helsenett og virksomheten må selv:</p> <ul style="list-style-type: none"> <li>– sørge for å kryptere helse- og personopplysninger før de sendes over helsenettet</li> <li>– sørge for sikker autentisering av brukere ved tilgang til helse- og personopplysninger</li> <li>– etablere løsninger mot ondsinnet programvare i virksomhetenes interne nettverk</li> </ul>
6.	<p><b>Fjernaksess</b></p> <ul style="list-style-type: none"> <li>– Virksomheten bør etablere en enhetlig løsning for fjernaksess</li> <li>– Det anbefales at leverandør inngår avtale med Norsk Helsenett for tilgang til virksomheten</li> <li>– Det skal i størst mulig grad benyttes tekniske tiltak som utstyr og programvare. Det er ikke tilstrekkelig med bare skriftlige prosedyrer som viser ansvar og arbeidsoppgaver</li> <li>– All tilgang til virksomhetens systemer gjennom fjernaksess, skal kun skje etter en særskilt tillatelse, og med individuell pålogging også for leverandørens personell</li> <li>– Alle aktiviteter skal registreres som hendelse. Leverandør skal dokumentere hva som er utført i virksomheten. Hendelsesregistre kan være både elektroniske og manuelle</li> </ul>
7.	<p><b>E-post</b></p> <p>Alminnelige e-postløsninger 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.</p>
8.	<p><b>Telemedisin</b></p> <p>Ved bruk av telemedisinske løsninger må disse være utformet slik at informasjonssikkerheten er tilstrekkelig ivaretatt. Dette vil kunne innebære blant annet transportsikkerhet, autentisering av klienter som brukes i telemedisin og mekanismer for tilgangskontroll av brukere.</p>
9.	<p><b>Hendelsesregistrering</b></p> <p>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.</p>

Nr	Handling/Utførelse
10.	<p><b>Rammeverk for sikkert meldingskommunikasjon (ebXML)</b></p> <p>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.</p> <p>For mer informasjon henvises det til Faktaark 16 - Etablering av løsning for meldingskommunikasjon.</p>
11.	<p><b>Adresseregisteret</b></p> <p>Sikker adressering er viktig ved kommunikasjon over åpne nett slik at en er sikker på at informasjon blir sendt til riktig mottaker. Adresseregisteret kan være et viktig bidrag til sikkert identifisering ved kommunikasjon over for eksempel Norsk Helsenett.</p> <p>For mer informasjon henvises det til Faktaark 16 – Etablering av løsning for meldingskommunikasjon.</p>