

 	Utgitt med støtte av:  HelseDirektoratet
Norm for informasjonssikkerhet <a href="http://www.normen.no">www.normen.no</a>	
<h2>Etablering av løsning for meldingskommunikasjon</h2>	<b>Støttedokument</b> <b>Faktaark nr 16</b> Versjon: 3.0 Dato: 01.12.2011

<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 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>	Virksomhetens ledelse er ansvarlig for at meldingskommunikasjon skjer iht Normen.		
<b>Gjennomføring</b>	Ved etablering av løsninger for meldingskommunikasjon.		
<b>Formål</b>	At helse- og personopplysninger overføres iht krav til konfidensialitet, integritet, tilgjengelighet og kvalitet.		
<b>Omfang</b>	Alle virksomheter som skal utveksle helse- og personopplysninger.		
<b>Hjemmel</b>	Personopplysningsforskriften § 2-11, § 2-12 og § 2-13		
<b>Referanser</b>	<ul style="list-style-type: none"> <li>• Informasjon om nasjonale meldingsstandarder på <a href="http://www.kith.no">www.kith.no</a> og PKI på <a href="http://www.difi.no">www.difi.no</a></li> <li>• Adresseregisterer på <a href="http://www.nhn.no">www.nhn.no</a></li> <li>• Faktaark 37 – Sikkerhetskrav og sikkerhetsdokumentasjon i IKT-prosjekter</li> </ul>		

Nr.	Handling/Utførelse
<b>1</b>	<b>Vurdere konsekvenser av innføring</b>  <ul style="list-style-type: none"> <li>- Avklare hvorvidt den nye kommunikasjonsløsningen skal kobles opp mot andre IKT-systemer og hvilke effekter ev. oppkoblinger kan medføre.</li> <li>- Kartlegge om andre kritiske systemer vil være avhengige av det nye systemet/evt. hvilke andre systemer den nye løsningen vil avhenge av (f.eks. katalogtjenester, sikkerhetstjenester osv.)</li> <li>- Avklare hvorvidt en eksisterende kommunikasjonskanal kan benyttes for innføringen eller hvorvidt innføringen innebærer åpning av ny kommunikasjonskanal</li> </ul>
<b>2</b>	<b>Vurdere informasjonssikkerheten hos kommunikasjonsparten</b> Helse- og personopplysninger kan kun overføres til parter som tilfredsstillt lovgivningens krav til informasjonssikkerhet. Hvis virksomheten følger kravene i Normen vil dette være tilfredsstillt – hvis ikke, må dette avklares på andre måter.
<b>3</b>	<b>Risikovurdering</b> Ved innføring av løsning for meldingskommunikasjon skal det gjennomføres en risikovurdering. Risikovurderingen skal fastsette om innføringen vil innebære behov for sikkerhetstiltak, jfr. Faktaark 7 – Risikovurdering. Risikovurderingen bør bl.a. omfatte risiko knyttet til: <ul style="list-style-type: none"> <li>- Åpning av sikkerhetsbarrierer for kommunikasjon ut og inn av egen virksomhet</li> <li>- Sikring av informasjon under overføring</li> <li>- Fare for utilsiktet utlevering av helse- og personopplysninger</li> <li>- Fare for at applikasjonskwittering ikke mottas</li> <li>- Uavviselighet (ikke-benekting)</li> <li>- Fare for at avsenders taushetsplikt blir brutt ved mottak av melding fordi internt personale som ikke har noen rolle i forhold til oppfølging av pasienten får tilgang til meldingen</li> <li>- Fare for at meldinger sendes til feil mottaker eller ikke kommer fram til rett mottaker, f.eks. som følge av for dårlig støtte til korrekt adressering</li> <li>- Risiko ved manglende meldingsovervåking</li> <li>- Risiko ved manglende tilgjengelig kompetanse for brukerstøtte og feilsøking</li> </ul>

Nr.	Handling/Utførelse
4	<p><b>Utarbeidelse av dokumentasjon og sikring av tilstrekkelig kompetanse</b></p> <p>Før løsningen settes i drift og overføres fra prosjekt til linjen må tilstrekkelig dokumentasjon være på plass. Dette innebærer bl.a.:</p> <ul style="list-style-type: none"> <li>- Avklare om brukere av IKT-systemet og driftspersonell har fått opplæring slik at informasjonssikkerheten ivaretas</li> <li>- Avklare om det finnes dokumentasjon av IKT-systemet slik at system-/ driftsansvarlig kan ivareta informasjonssikkerheten (finne svakheter, installere riktige sikkerhetsoppdateringer etc.)</li> <li>- Etablere prosedyrer for overvåkning av meldingstrafikk og behandling av avvik</li> <li>- Sørge for tilstrekkelig tilgjengelig kompetanse for feilsøking og brukerstøtte</li> </ul>
5	<p><b>Legge til rette for elektronisk adressering av meldinger</b></p> <ul style="list-style-type: none"> <li>- Etablere prosedyrer for registrering og oppdatering av adresser i NHN-Adresseregister til egne tjenester eller personer. Adressene må samsvare med den standardisering som er gjort innen virksomhetsområdet (kommune/helseforetak), sikre avsender en robust løsning som i minst mulig grad er avhengig av enkeltpersoner eller intern organisering, og bidra til at meldinger distribueres mest mulig direkte til relevant mottaker</li> <li>- Legge til rette slik at elektronisk adresse til relevante samhandlingsparter er lett tilgjengelig for personalet i virksomheten når de skal sende en melding, og at disse adressene ikke lett forveksles med andre adresser</li> </ul>
6	<p><b>Håndtere PKI-sertifikat</b></p> <ul style="list-style-type: none"> <li>- Anskaffe og installere virksomhetssertifikat for virksomhetene</li> <li>- Anskaffe og installere eventuelle personlige sertifikater</li> <li>- Registrere eksterne parter virksomheten skal samhandle med, og installere deres sertifikat</li> <li>- Etablere prosedyrer for oppdatering av eget og partens sertifikat når disse utløper</li> </ul>

Tabellen nedenfor gir en oversikt over en del gjeldende standarder og krav innen elektronisk samhandling.

Område	Informasjon
<b>Nasjonale meldingsstandarder</b>	Det nasjonale standardiseringsorganet for meldinger utvikler nasjonale standarder for meldinger i helse-, omsorgs- og sosialsektoren. Disse skal benyttes der slike finnes. For flere meldinger er det etablert en ordning for akseptansetest av meldingene hvor en leverandør vil få en godkjenning av sin implementering.
<b>Elektronisk signatur</b>	Elektronisk signatur sikrer autentisering av avsender, integritet og sporbarhet.  Format for elektronisk signatur vil kunne være beskrevet i dokumentasjonen for meldingen.  For meldinger med behov for sterk knytting til enkeltperson vil det kunne stilles krav om kvalifisert signatur iht. lov om elektronisk signatur. For andre meldinger vil virksomhetssignatur kombinert med tekstlig informasjon om ansvarlig avsender være tilstrekkelig.
<b>Kryptering</b>	Meldinger som inneholder sensitive personopplysninger skal krypteres.
<b>Rammeverk for meldingsutveksling (ebXML)</b>	Overføring av meldinger skal foregå vha. rammeverk for meldingsutveksling (ebXML) som er en internasjonal standard for

<b>Område</b>	<b>Informasjon</b>
	meldingsutveksling. Rammeverket består av en konvoluttmelding og prosedyrer for pålitelig meldingsutveksling. Konvoluttet sikrer en entydig identifikasjon av kommunikasjonspartene (avsender og mottaker) og identifiserer selve forretningstransaksjonen (sykmelding, resept, etc). Rammeverket beskriver også hvordan sikkerheten ivaretas ved overføringen av meldinger.
<b>NHN-Adresseregister / HER-id</b>	NHN-Adresseregister inneholder informasjon til å identifisere og adressere hver enkelt av virksomhetenes ulike mottakere og avsendere. Ved registrering i NHN-Adresseregister blir den enkelte virksomhet og dens egne kommunikasjonsparter (avsendere / mottakere ) knyttet til en unik identifikator som kalles HER-id. HER-id identifiserer helsepersonell, organisasjoner og avdelinger og vil bl.a. bidra til sikrere adressering av informasjon.