

		Utgitt med støtte av: 
Norm for informasjonssikkerhet i helsesektoren		<b>Støttedokument</b> <b>Faktaark nr 32</b> Versjon: 2.0 Dato: 03.12.2009
<h1>Elektronisk pasient- og brukerkommunikasjon</h1>		

<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>	Virksomhetens leder/ledelse skal påse at løsninger for pasient-/brukerkommunikasjon benyttes på en sikker måte.		
<b>Gjennomføring</b>	Ved etablering av tjenester for elektronisk pasient- og brukerkommunikasjon.		
<b>Formål</b>	Legge til rette for sikker elektronisk kommunikasjon med pasienter/brukere.		
<b>Omfang</b>	Omfatter alle systemer/løsninger som tilbyr elektronisk kommunikasjon med pasienter/brukere.		
<b>Hjemmel</b>	Personopplysningsforskriftens § 2-11. Sikring av konfidensialitet, § 2-12. Sikring av tilgjengelighet og § 2-13. Sikring av integritet		
<b>Referanser</b>	<ul style="list-style-type: none"> <li>Norm for informasjonssikkerhet i helsesektoren kap. 5.7.5 Kommunikasjon med pasienter/brukere</li> <li>Faktaark 10 – Bruk av databehandler (ekstern driftsenhet)</li> <li>Faktaark 42 – Bruk av SMS i pasientkontakt</li> <li>Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, april 2008</li> </ul>		

Nr.	Handling/Utførelse
1.	<b>Metode for kommunikasjon</b> <ul style="list-style-type: none"> <li>E-post og SMS skal ikke benyttes for overføring av helse- og personopplysninger til pasienter/bruker.</li> <li>For pasient-/brukerkommunikasjon skal det benyttes tjenester som er spesielt tilrettelagt for slik kommunikasjon. Det kan for eksempel være i en nettbasert løsning som benyttes til kommunikasjon mellom behandlende helsepersonell og pasienter/bruker</li> </ul>
2.	<b>Hovedprinsipper for løsninger med pasient- og brukerkommunikasjon</b> <ul style="list-style-type: none"> <li>Pasienten/bruker bør kunne bruke "standard" programvare for tilgang til den elektroniske løsningen (for eksempel standard nettlesere)</li> <li>Løsningen må vanskeliggjøre lokal lagring av helse- og personopplysninger hos brukeren. Løsningen skal ikke presentere informasjon slik at det er nødvendig for pasient/bruker å lagre informasjonen lokalt på egen PC for å gjøre seg kjent med informasjonen</li> <li>Data skal ikke lagres i løsningen lenger enn formålet med behandlingen av dataen tilsier</li> <li>Det må kreves samme sikkerhetsnivå ved tilgang til slike tjenester som ved ekstern tilgang til andre systemer med helse- og personopplysninger</li> </ul>
3.	<b>Risikovurdering</b> Det skal gjennomføres risikovurdering av løsningen.
4.	<b>Kryptering av kommunikasjonen</b> Alle helse- og personopplysninger skal krypteres iht gjeldende krav ved overføringen over åpne nettverk.
5.	<b>Autentisering av pasient/bruker</b> For tilgang til nettbasert løsning skal det benyttes Nivå 4 for autentisering som for eksempel engangspassord som overføres med SMS.
6.	<b>Informasjon til pasient/bruker</b> Informasjon bør omfatte: <ul style="list-style-type: none"> <li>Tjenesten bør kun benyttes fra eget utstyr (unngå for eksempel Internettkafé)</li> <li>Tiltak for å beskytte egen PC, f.eks. virusbeskyttelse, brannmur osv.</li> </ul>

Nr.	Handling/Utførelse
	<ul style="list-style-type: none"> <li>- Hvordan informasjon kan slettes fra tjenesten</li> <li>- Informasjon om hvordan tjenesten kan avsluttes/sperres</li> </ul>
7.	<b>Journalføring av opplysninger</b> <ul style="list-style-type: none"> <li>- Journalverdig informasjon fra pasient/bruker skal journalføres</li> <li>- Det bør være mulig å overføre informasjon fra tjenesten til journalsystemet (EPJ)</li> </ul>
8.	<b>Bruk av ekstern databehandler</b> Dersom det benyttes databehandler for pasient/brukerkommunikasjon skal det etableres en avtale tale mellom virksomheten og databehandler (databehandleravtale)

## Eksempel på løsning for pasient-/brukerkommunikasjon

