

 Norm for informasjonssikkerhet www.normen.no	Utgitt med støtte av: 
<h2>Elektronisk pasient- og brukerkommunikasjon</h2>	Støttedokument Faktaark nr 32 Versjon: 2.1 Dato: 15.12.2010

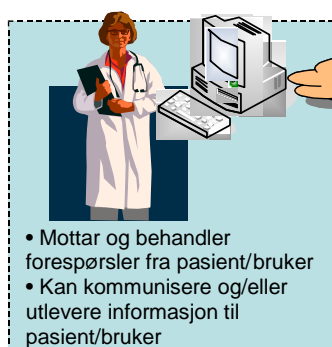
Målgruppe Dette faktaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder / sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
Ansvar	Virksomhetens leder/ledelse skal påse at løsninger for pasient-/brukerkommunikasjon benyttes på en sikker måte.		
Gjennomføring	Ved etablering av tjenester for elektronisk pasient- og brukerkommunikasjon.		
Formål	Legge til rette for sikker elektronisk kommunikasjon med pasienter/brukere.		
Omfang	Omfatter alle systemer/løsninger som tilbyr elektronisk kommunikasjon med pasienter/brukere.		
Hjemmel	Personopplysningsforskriften §§ 2-11, 2-12 og 2-13		
Referanser	<ul style="list-style-type: none"> • Norm for informasjonssikkerhet kapittel 5.7.5 • Faktaark 10 – Bruk av databehandler (ekstern driftsenhet) • Faktaark 42 – Bruk av SMS i pasientkontakt • Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, april 2008 		

Nr.	Handling/Utførelse
1.	Metode for kommunikasjon <ul style="list-style-type: none"> - E-post og SMS skal ikke benyttes for overføring av helseopplysninger til pasienter/bruker. - 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
2.	Hovedprinsipper for løsninger med pasient- og brukerkommunikasjon <ul style="list-style-type: none"> - Pasienten/bruker bør kunne bruke "standard" programvare for tilgang til den elektroniske løsningen (for eksempel standard nettlesere) - 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 - Data skal ikke lagres i løsningen lenger enn formålet med behandlingen av dataen tilsier - Det må kreves samme sikkerhetsnivå ved tilgang til slike tjenester som ved ekstern tilgang til andre systemer med helse- og personopplysninger
3.	Risikovurdering Det skal gjennomføres risikovurdering av løsningen.
4.	Kryptering av kommunikasjonen Alle helse- og personopplysninger skal krypteres iht gjeldende krav ved overføringen over åpne nettverk.
5.	Autentisering av pasient/bruker For tilgang til nettbasert løsning skal det benyttes autentisering på sikkerhetsnivå 4.
6.	Informasjon til pasient/bruker Informasjon bør omfatte: <ul style="list-style-type: none"> - Tjenesten bør kun benyttes fra eget utstyr (unngå for eksempel Internettkafé) - Tiltak for å beskytte egen PC, f.eks. virusbeskyttelse, brannmur osv.

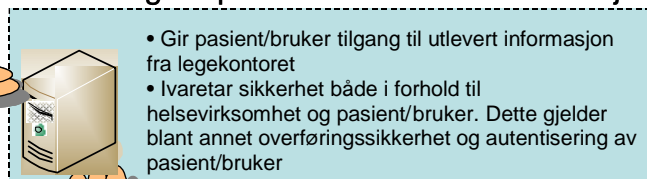
Nr.	Handling/Utførelse
	<ul style="list-style-type: none"> - Hvordan informasjon kan slettes fra tjenesten - Informasjon om hvordan tjenesten kan avsluttes/sperres
7.	Journalføring av opplysninger <ul style="list-style-type: none"> - Journalverdig informasjon fra pasient/bruker skal journalføres - Det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

Eksempel på løsning for pasient-/brukerkommunikasjon

Helsevirksomhet



Løsning for pasient-/brukerkommunikasjon



Internett

Pasient/bruker

