

 <p>Norm for informasjonssikkerhet www.normen.no</p>	Utgitt med støtte av: 
<h2>Alternative tekniske løsninger for primærhelsetjenesten</h2>	Støttedokument Faktaark nr 28 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 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 ledelse er ansvarlig for å etablere en sikker teknisk løsning.		
Gjennomføring	Valg av teknisk løsning skal baseres på definerte behov og formålet med databehandlingen.		
Formål	Bidra til at primærhelsetjenesten etablerer sikre og kontrollerbare tekniske løsninger.		
Omfang	Alle virksomheter i primærhelsetjenesten skal etablere en teknisk løsning som ivaretar kravene til sikring av helse- og personopplysninger.		
Hjemmel	Personopplysningsforskriften §§ 2-11, 2-12, 2-13, 2-14 og 2-15		
Referanser	<ul style="list-style-type: none"> • Norm for informasjonssikkerhet kapittel 5.5 • Veileder i informasjonssikkerhet ved tilknytning mellom kommuner, fylkeskommuner og helsenettet 		

Nr.	Aktivitet/Beskrivelse
1	Vurdering av og beslutning om teknisk løsning for ekstern kommunikasjon: a) Ingen ekstern kommunikasjon b) Kommunikasjon med trygge parter (laboratorier, NAV, HELFO, apotek, spesialisthelsetjenesten, leverandør, mv) c) Kommunikasjon med pasient (publikumstjenester)
2	Alternative tekniske løsninger (listen under er kun eksempler) a) Lokalt nettverk med tilkobling til Norsk Helsenett (helsenettet) for å sende rekvisisjoner og henvisninger og motta laboratoriesvar. Adskilt PC for tilgang til Internett b) Som a), men tilkoblet Internett via helsenettet og hjemmekontor (utekontor) via helsenettet c) Servere plassert hos leverandør og all kommunikasjon går via helsenettet. Internett nås via helsenettet d) Bruk av kommunens tekniske løsning med kommunen som databehandler. Internett og helsenettet nås via kommunens nettverk Se under for nærmere beskrivelse av eksemplene inklusive fordeler og ulemper.

Eksempler

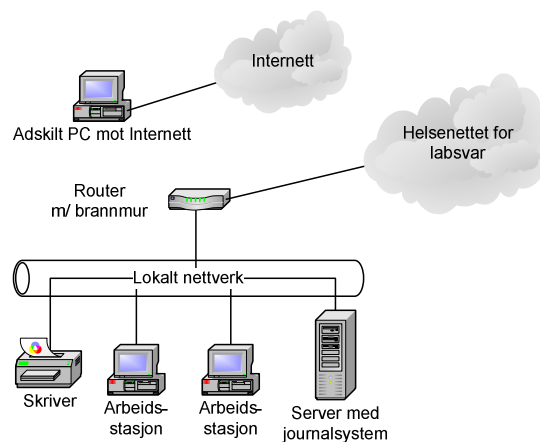
Det er viktig å presisere at dette er eksempler og at de kun viser mulige tekniske løsninger. Alternativene er flere og må tilpasses behov og krav.

a) Lokalt nettverk med tilkobling til helsenettet for å sende rekvisisjoner og henvisninger og motta laboratoriesvar og epikriser. Adskilt PC for tilgang til Internett

Journal- og pasientadministrative systemer driftes lokalt på eget nettverk (server) og det er kun behov for ekstern kommunikasjon for å motta laboratoriesvar og epikriser via helsenettet. Løsningen har lav risiko og krever få tekniske sikkerhetstiltak. Ofte er det tilstrekkelig med sikkerhetsløsning levert av maskin- og programvareleverandør inklusive sikkerhetskopiering og løsning for tilkobling til helsenettet. Tilgang til Internett er løst med en adskilt PC.

Fordeler: Ingen trusler utenfra. Er det tillatt med minnepinner, etc. er det nødvendig med antivirus. Se Faktaark - 26 Sikring av trådløs teknologi.

Ulemper: Adskilte tekniske løsninger som krever vedlikehold.

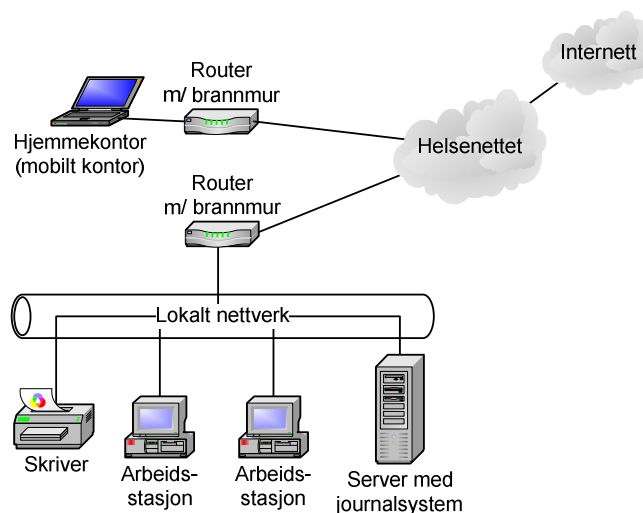


b) Som a), men tilkoblet Internett via helsenettet og hjemmekontor (mobilt kontor) via helsenettet

Som over, men nettverket er i tillegg koblet til helsenettet med Internett og hjemmekontor (mobilt kontor). Løsningen har høyere risiko og krever sikring slik at det ikke opprettes gjennomgående forbindelser fra Internett ved at det er to uavhengige sikkerhetsbarrierer mellom nettverk og Internett, at all kommunikasjon initieres innenfra og ut og at trafikken overvåkes. Det må etableres teknisk løsning for tilgang til Internett som hindrer uautorisert utlevering av helse- og personopplysninger (for eksempel ved bruk av tynne klienter og terminalserver).

Fordeler: Mulig å kommunisere med eksterne virksomheter.

Ulemper: Krever kompetent bistand for oppsett og drift av løsningen.

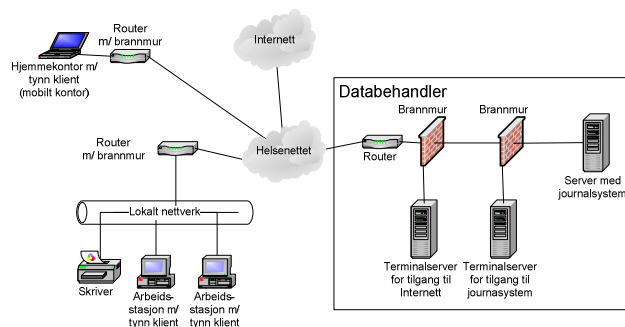


c) Servere plassert hos leverandør og all kommunikasjon går via helsenettet. Internett nås via helsenettet

Legekantoret benytter databehandler for drift av servere. All kommunikasjon går via helsenettet inklusive hjemmekontor (mobilt kontor) og Internett. Helsenettet tilbyr kontrollerte tjenester (Internett-tilgang, viruskontroll) og sikkerhetsmekanismer i helsenettet kan ses på som en sikkerhetsbarriere mot eksterne nettverk. Ved at primærhelsetjenesten oppretter en egen barriere er kravet til to uavhengige barrierer ivaretatt.

Fordeler: En kommunikasjonspart å forholde seg til.

Ulemper: Krever kompetent bistand for oppsett og drift av løsningen. Avhengig av helsenettet for å nå egne systemer.



Leger som deler journalsystem, barrierer, servere, osv skal ha en inndeling slik at helse- og personopplysninger er skjermet ift hverandre. Den enkelte lege skal ikke kunne bryte administrative regler for å få tilgang til en annen leges pasientjournaler. Løsningen må ha elektroniske skiller slik at det ikke er mulig å bryte reglene. Det må for eksempel kunne defineres flere praksiser i det samme journalsystemet og behov for innsyn skal reguleres av en forespørsel om innsyn med påfølgende utlevering av en enkeltjournal.

d) Bruk av kommunens tekniske løsning med kommunen som databehandler. Internett og helsenettet nås via kommunens nettverk

Legekantoret benytter kommunen som databehandler og har tilgang til helsenettet via kommunens nettverk. For nærmere beskrivelse av denne løsningen, se "Veileder i informasjonssikkerhet ved tilknytning mellom kommuner, fylkeskommuner og helsenettet", kapittel 3.4.

