

| | |
|--|--|
|   | Utgitt med støtte av:  HelseDirektoratet |
| Norm for informasjonssikkerhet www.normen.no | |
| <h2>Bruk av SMS i pasientkontakt</h2> | Støttedokument Faktaark nr. 42 Versjon: 1.1 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 type="checkbox"/> Databehandler <input checked="" type="checkbox"/> Personvernombud |
| Ansvar | Virksomhetens leder er ansvarlig for at bruk av SMS i pasientkontakt skjer iht etablerte prosedyrer og at det blir skapt forståelse for en sikker løsning. | | |
| Gjennomføring | Regler og prosedyrer skal etableres før løsning for SMS i pasientkontakten benyttes. | | |
| Formål | Sikre god, enkel og effektiv pasientkontakt, samtidig som hensynet til konfidensialitet og integritet for helse- og personopplysninger ivaretas. | | |
| Omfang | Omfatter bruk av SMS (eller lignende melding) fra en virksomhet i helsesektoren til pasientens mobiltelefon eller andre løsninger hvor SMS er tilgjengelig for bruker. For eksempel Internettisider med meldingssystemer. | | |
| Hjemmel | Personopplysningsforskriften §§ 2-11, 2-12 og 2-13. | | |
| Referanser | Pasientrettighetsloven §§ 3-4 og 4-4 vedr samtykke for barn under 16 år. | | |

Innledning

SMS benyttes i mange sammenhenger i kommunikasjon mellom pasient og helsetjenestetilbyder. I den anledning er det viktig å etablere løsninger som ikke benyttes til overføring av informasjon som bryter med kravet til personvern og informasjonssikkerhet.

Helsevirksomheten som benytter løsningen er ansvarlig og skal påse at krav til informasjonssikkerhet ivaretas. Leverandør og eventuell tjenesteyter er kun ansvarlig for at deres løsning fungerer som avtalt.

For all bruk av SMS kreves det samtykke fra pasienten. Se Referanser over.

Definisjoner

Med ”**leverandør**” menes i Normen juridisk enhet som yter tekniske og/eller administrative tjenester til virksomheten. Eksempler er EPJ-leverandør, røntgenleverandør, leverandør av løsning for SMS-meldinger, IKT-leverandør mv.

Med ”**meldingskode**” menes kode som SMS inneholder for å angi rett meldingstype (for eksempel standardmeldinger med timebestilling eller melding med passord. Hver av disse meldingene vil ha en tilhørende meldingskode; for eksempel ”2300” og ”2301”. Dette er koder som IT-systemet benytter for å behandle meldingene ved generering, utsendelse og mottak).

Med ”**tjenesteyter**” menes den som leverer SMS-tjenesten, dvs den som sender meldingene på vegne av virksomheten. Det er en rekke systemer som ikke krever bruk av tjenesteyter.

Eksempler på informasjon som kan sendes som SMS

- Navn, helst kun fornavn
- Fødselsdato
- Bekreftelse på timeavtale (“..minner om timeavtale hos oss tir. 5. jan kl 1430. mvh tannlege <tannlegenavn>.”)
- Aksept av timeavtale (svar tilbake til avsender at avtalen er OK – Ja/Nei)
- Endring av timeavtale (Time 5. jan kl 1200 utgår. Du er satt opp med ny time 18. januar kl 1700. Bekreft om foreslått tidspunkt passer – Ja/Nei)

- Forespørsel om blodgiving
- Aksept av blodgiving (Ja/Nei)
- Engangspassord for pålogging til kommunikasjonsløsninger som inneholder helseopplysninger
- Varsling om nye meldinger i andre systemer
- Annet som er relatert til praktiske forhold vedr. kontakten mellom helsetjenestetilbyder og pasient, og som ikke inneholder sensitive personopplysninger ("...vi har flyttet til...", "...møt fastende...")
- Hvis det ikke skal eller kan sendes svar på SMS skal det opplyses om det i meldingen som sendes til pasienten, f. eks kan meldingen utvides med: "Du kan ikke sende svar på denne SMS"

Eksempler på informasjon som ikke kan sendes som SMS

- Fødselsnummer (11 siffer)
- Helseopplysninger. For eksempel diagnose i form av kode eller tekst som viser pasientens helsetilstand
- Reseptinformasjon

Eksempler på informasjon som ikke bør sendes som SMS

- Avdelingsnavn (som kan knyttes til diagnose eller helseforhold. Unngå for eksempel "...psykiatrisk poliklinikk...", "...gynekologisk avdeling...")
- Telefonnr til avsender (slik at det ikke er mulig å identifisere avsender/avdeling med navn som kan angi helseforhold eller diagnose)

Den samlede informasjonen i SMS må vurderes ut fra om innholdet totalt sett kan medføre brudd på taushetsplikten.

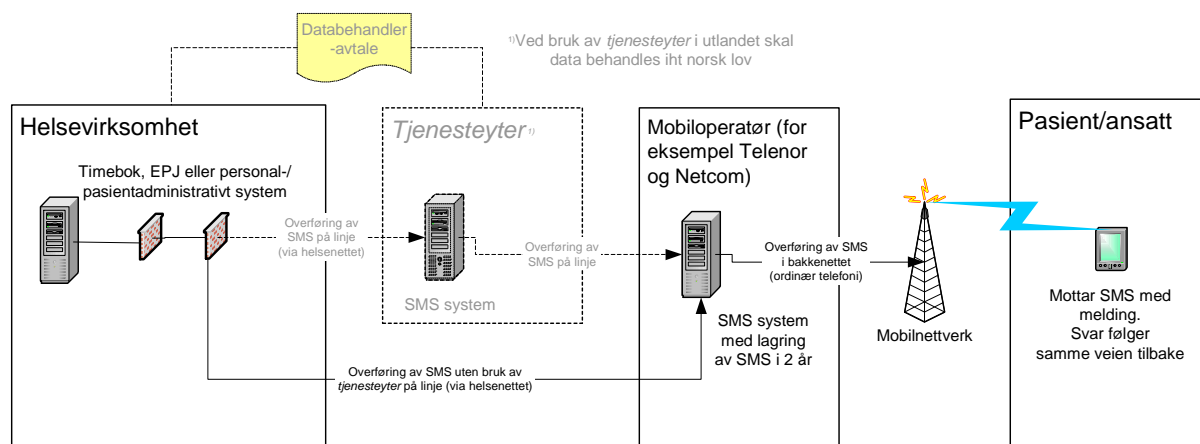
Etablering av SMS-løsning

| Trinn | Handling |
|-------|--|
| 1. | <p>Fastsette bruk av SMS</p> <p>a) Virksomhetens leder skal beslutte om SMS skal benyttes ved kontakt med pasienten og beskrive formålet med bruk av SMS</p> <p>b) Regler for utplukk av pasient som skal motta SMS og løsning for utsendelse og mottak av SMS skal beskrives. Hvilke data som skal sendes og mottas som SMS skal dokumenteres og danne grunnlag for beslutningen. Endring av formål (se eksemplene over) og beskrivelsen skal godkjennes av virksomhetens leder</p> <p>c) Det er spesielt viktig å beskrive hvilke meldingskode som benyttes i ulike SMS slik at de er entydige. Det skal være unik meldingskode for de forskjellige bruksområdene (se eksemplene over)</p> <p>d) Prosedyrer for drift av SMS-løsning skal utarbeides; beskrivelse av teknisk løsning, behandling av stans i SMS-løsningen og analyse av hendelsesregistre</p> |
| 2. | <p>Avtale med tjenesteyter (punktet utgår om tjenesteyter ikke benyttes)</p> <p>a) Det skal etableres skriftlig databehandleravtale med tjenesteyter dersom en slik benyttes. Sender virksomheten ut meldingene selv skal det ikke etableres databehandleravtale</p> <p>b) Ved bruk av tjenesteyter skal denne sørge for at det ikke opprettes felles registre for flere kunder. Dette skal klart fremgå av databehandleravtalen</p> <p>c) Databehandleravtalen bør inneholde et slettekrav når SMS er vellykket viderefremmet</p> |
| 3. | <p>Samtykke fra pasient</p> <p>a) Virksomheten skal utarbeide informasjon om bruk av SMS som gis skriftlig eller muntlig til pasienten. Bl.a. skal det nevnes at pasienten ikke skal sende sensitive personopplysninger / helseopplysninger via SMS (se vedlagte eksempel på samtykkeerklæring)</p> |

| Trinn | Handling |
|-------|--|
| | <ul style="list-style-type: none"> b) Den enkelte pasient skal gi samtykke til bruk av SMS i pasientkontakt. Det anbefales avkryssingsboks (i skjema eller direkte i fagsystemet) der pasienten godtar bruk av SMS c) For blodbank innarbeides samtykke i avtale med blodgiver d) Behandlende helsepersonell skal innhente mobilnummer direkte fra pasienten/pårørende ifm samtykke |
| 4. | <p>Teknisk generering av SMS</p> <ul style="list-style-type: none"> a) Systemet skal kontrollere at pasient har gitt sitt samtykke før SMS genereres og sendes ut |
| 5. | <p>Hendelsesregistrering i virksomheten ved utsendelse og mottak av SMS</p> <ul style="list-style-type: none"> a) All generering av SMS skal hendelsesregistreres med brukernavn, oppgaven eller funksjonen som initierer oppgaven, meldingskode, fortløpende løpenummer, innhold som sendes som SMS, mobilnummer som SMS sendes til, tidsstempel (dato og klokkeslett) b) All utsendelse bør hendelsesregistreres med løpenummer, meldingskode, mobilnummer, tidsstempel c) Feil ved utsendelse av SMS bør hendelsesregistreres med løpenummer, meldingskode, mobilnummer, tidsstempel d) Kvittering fra tjenesteyter (om tjenesteyter benyttes) bør hendelsesregistreres med mobilnummer, meldingskode, tidsstempel e) Mottak av svar bør hendelsesregistreres med mobilnummer, meldingskode, mottatt svar, tidsstempel f) Masseutsendelse følger de samme reglene som for generering, utsendelse og mottak over g) Hendelsesregistre skal kunne analyseres for å avdekke sikkerhetsbrudd (hendelsesregistre skal oppbevares i minimum 2 år) |
| 6. | <p>Teknisk utsendelse av SMS</p> <ul style="list-style-type: none"> a) SMS skal kontrolleres for ondsinnet programkode før utsendelse b) SMS skal kun sendes til norske mobilnummer |
| 7. | <p>Teknisk mottak av SMS</p> <ul style="list-style-type: none"> a) SMS-svaret skal ikke sendes direkte inn til nettverk/fagsystem (for eksempel timebok eller EPJ) som benyttes til behandling av helse- og personopplysninger b) SMS-svaret skal kontrolleres for ondsinnet programkode ved mottak og før SMS-svaret <u>hentes</u> inn i fagsystem |
| 8. | <p>Behandling av mottatt svar fra pasient</p> <ul style="list-style-type: none"> a) Svar fra pasient skal kontrolleres mot utsendt SMS. Kontrollen baseres på mobilnummeret i svaret og meldingskode i utsendte SMS b) Ved manglende match mellom utsendt SMS og mottatt mobilnummer og meldingskode stanses svaret og hendelsen hendelsesregistreres c) Godkjente svar skal kontrolleres mot pasientens samtykke. Ved manglende samtykke stanses svaret og hendelsen hendelsesregistreres d) Godkjente svar registreres i fagsystem iht dokumenterte regler e) Bruker som har initiert utsendelse av SMS til pasient skal få tydelig beskjed om at SMS-svar er mottatt fra pasient |

Skisse som viser informasjonsflyten ved bruk av SMS

Merk at det ikke er nødvendig å benytte tjenesteyter.



Eksempel på samtykkeerklæring for bruk av SMS

Jeg godkjenner bruk av SMS i kontakt med meg som pasient/pårørende til pasient ved <virksomhet>.

Samtykket gjelder frem til samtykket trekkes tilbake.

Samtykket gjelder for bruk av SMS til følgende formål:

| Formål | Samtykke | Ikke samtykke |
|----------------------------------|--------------------------|--------------------------|
| Varsel om timeavtale | <input type="checkbox"/> | <input type="checkbox"/> |
| Aksept av timeavtale | <input type="checkbox"/> | <input type="checkbox"/> |
| Forespørsel om blodgivning | <input type="checkbox"/> | <input type="checkbox"/> |
| Aksept av blodgivning | <input type="checkbox"/> | <input type="checkbox"/> |
| Engangspassord for pålogging | <input type="checkbox"/> | <input type="checkbox"/> |
| Varsel om melding i annet system | <input type="checkbox"/> | <input type="checkbox"/> |
| | <input type="checkbox"/> | <input type="checkbox"/> |
| | <input type="checkbox"/> | <input type="checkbox"/> |
| | <input type="checkbox"/> | <input type="checkbox"/> |

| | |
|--------------|--|
| Dato: | |
| Navn: | |
| Mobilnr: | |
| Fødselsdato: | |

Samtykkeerklæringen arkiveres (elektronisk eller manuelt) i pasientens journal.