

 Foretaksnivå				Retningslinje
Bruk av e-post, chat, telefaks og SMS for kommunikasjon med og om pasienter				Side 1 av 3
Dokumentplassering: I.5.9.2-2	Godkjent dato: 19.02.2025	Revideres innen: 19.02.2027	Sist endret: 31.07.2026	Revisjon: 3.01

Foretaksnivå/Virksomhetsstyring/Informasjonssikkerhet og personvern/Utøvende - alle brukere
ENDRINGER FRA FORRIGE VERSJON: Mindre tekstlig justering og tilpasninger.

KILDE

Basert på HSØ fellesregionalt ledelsessystem for informasjonssikkerhet, dokument NO-27 v1.0: «Bruk av e-post, telefaks og SMS for kommunikasjon med og om pasienter». Oppdatert etter personopplysningslov av 20. juli 2018.

HENSIKT

Denne retningslinjen omfatter all kommunikasjon med og om pasienter ved bruk av virksomhetens e-postsystem, chat-funksjoner, telefaks, SMS og andre tilsvarende¹ løsninger for kommunikasjon og samhandling. Dette dokumentet supplerer SSHF sitt dokument [Bruk av e-post i SSHF: overordnet retningslinje](#), samt dokumentet [Forenklet sikkerhetsinstruks \(med signaturl\)](#).

MÅLGRUPPE

Alle medarbeidere ved Sørlandet sykehus HF (SSHF).

FREM GANGSMÅTE

Bruk av løsning for kommunikasjon som nevnt ovenfor anses som usikre kommunikasjonskanaler da vi som avsender ikke har kontroll på sikkerheten i løsningen eller skjermingen av informasjonen hos mottaker. Dette kan sammenlignes med å sende de samme opplysninger på et postkort, og brudd på taushetsplikten kan forekomme.

Det må derfor utvises stor varsomhet når disse løsningene benyttes for å kommunisere med og om pasienter. Dette gjelder også om det sendes internt i sykehusets nettverk. Videre har ikke e-post som tjeneste leveransegaranti, og avsender kan dermed oppfatte at e-posten er sendt og mottatt, uten at mottaker faktisk har mottatt e-posten. Sykehuset har ingen garanti for at avsender faktisk er den vedkommende gir seg ut for å være, e-postadresse gir ingen slik garanti og kan manipuleres.

Retningslinjer for intern bruk av sykehusets e-postsystem, evt Teams chat

Hovedregelen er at personidentifiserende opplysninger ikke sendes sammen med helserelaterte opplysninger. Person- og pasientidentifiserbare data/opplysninger er:

- Fullt eller unikt navn
- Navn med fødselsdato
- Fødselsnummer (11 siffer, dvs fødselsdato + personnummer)
- Pasientnummer, eks. NPR-id, hjelpenummer, løpenr etc.
- Annet som entydig identifiserer pasienten, direkte eller indirekte f.eks. helt spesielle diagnoser og hendelsesforløp eller kombinasjon av slik informasjon.

Dersom de helserelaterte opplysningene er anonyme, kan helserelaterte opplysninger sendes på e-post. Se dokumentet [Anonymisering av helse- og personopplysninger](#),

Ved bruk av intern e-post og chat kan NPR-id, evt prøvenummer eller initialer og fødselsdato benyttes som personidentifikasjon når andre personopplysninger ikke sendes samtidig.

¹ Med «tilsvarende» må her forstås alle former for tjenester, applikasjoner og utstyr, selv en leverandør eller tjenesteyter hevder at innholdet og løsninger ivaretar sikkerheten. Hver enkelt tjeneste hvor personopplysninger inngår skal ROS'es og godkjennes. For ytterligere informasjon om bruk henvises det til Normens [veileder i digital pasientkommunikasjon](#). Her er gjengitt eksempler, problemstillinger og innspill relevant for utarbeidelse av ROS og personvernkonsekvensvurdering (DPIA).

Utarbeidet av: Geir Hovind	Fagansvarlig: Geir Hovind	Verifisert av: []	Godkjent av: Kjetil Nyhus	Dok.nr: D52529
--------------------------------------	-------------------------------------	-----------------------------	-------------------------------------	--------------------------

 SØRLANDET SYKEHUS		Bruk av e-post, chat, telefaks og SMS for kommunikasjon med og om pasienter			Side: 2 Av: 3
Dokument-id: 1.5.9.2-2	Utarbeidet av: Geir Hovind	Fagansvarlig: Geir Hovind	Godkjent dato: 19.02.2025	Godkjent av: Kjetil Nyhus	Revisjon: 3.01

Foretaksnivå/Virksomhetsstyring/Informasjonssikkerhet og personvern/Utøvende - alle brukere

Informasjon om pasient kan sendes i 2 separate kommunikasjonskanaler dersom også identifikasjon må formidles, men slik at hovedregelen ikke brytes. Det må vises aktsomhet slik at e-post med sensitive personopplysninger ikke kommer uvedkommende i hende. Ved kommunikasjon via 2 separate kanaler/medium må

- det må sikres at den samlede mengde informasjon ikke kan knyttes til pasient
- det sikres at kun autoriserte mottakere mottar e-postene
- bruk NPR-id som identifikator eller prøvenummer (entydig), evt initialer og fødselsdato (ikke entydig)
- e-post slettes når informasjonen er sendt og mottatt, slik at det ikke ligger unødvendig informasjon i e-postkontoene
- e-post ikke sendes til eksterne mottakere
- e-post ikke sendes til felles e-postkonto
- ikke opplysninger i "emne-feltet" gis slik at utenforstående enkelt kan tilegne seg personopplysninger. Her er det viktig å være klar over at alle som ikke har direkte med til den enkelte er å betrakte som utenforstående, selv om de er ansatt og jobber i sykehuset.

Retningslinjer for bruk av e-post (evt Teams chat) i kommunikasjon med ekstern part

I kommunikasjon med pasienten eller pårørende:

Dersom pasienter stiller spørsmål eller på annen måte kontakter virksomheten via e-post, kan ikke pasientens helse, diagnose eller behandling kommuniseres på e-post.

- Om pasienten eller pårørende likevel sender slike spørsmål på e-post, må svaret som gis på e-post begrenses til at helseopplysninger ikke kan kommuniseres på e-post og så henvise pasienten til hvor og hvordan svarene vil bli gitt.
 - Ved slik svar på e-post, husk på å slette personens eget spørsmål, slik at ikke sykehuset sender tilbake svar som inneholder sensitive personopplysninger, selv om disse ble lagt inn av den som spør.
- Pasienten eller pårørende kan ikke samtykke til at sensitive opplysninger sendes åpent med vanlig e-post. Lovens krav er uansett gjeldende.

Det som kan kommuniseres på e-post er enkel timebestilling, dersom informasjonen ikke gir noe om diagnose eller hva som skal gjøres. Også angivelse av poliklinikk eller sted på sykehuset for oppmøte, kan gi diagnose og må derfor besvares med varsomhet. Bruk av e-post for denne typen dialog forutsetter at pasienten selv har tatt første initiativ til kommunikasjon via e-post.

Særlige kategorier av personopplysninger og personnummer/fødselsnummer kan heller ikke med pasientens samtykke sendes på e-post. Selv om pasienten selv sender slike opplysninger i et ønske om å få avklart et helsemessig spørsmål, er det ikke lov å besvare slike spørsmål på e-post dersom svaret gir noe informasjon om pasientens helse. Loven setter krav til sikring som det ikke kan samtykkes bort fra.

I kommunikasjon om pasienten, eksempelvis med eksternt helsepersonell

Kommunikasjon via ekstern e-post må ikke inneholde identifiserbare personopplysninger. Ta kontakt med informasjonssikkerhetsleder dersom det er behov for avklaring og valg av løsning.

Siden bruk av e-post krever at direkte (entydig) identitet fjernes, kan alternativt initialer og fødselsdato benyttes, men du må da i parallell ringe (eller på annen tilsvarende måte) kontakte mottaker for å opplyse om fullstendig og entydig personidentifikasjon.

Merk at det ved SSHF kan gis tillatelse til å benytte e-post for å utveksle særlige kategorier personopplysninger (sensitive data) med en definert ekstern part når teknologi er til en hinder eller når tid på døgnet og behandlingstid ved postmottak gir grunnlag for å akseptere unntak fra retningslinjene ovenfor, gitt visse forutsetninger. Dette skal avtales og godkjennes av Informasjonssikkerhetsleder.

 SØRLANDET SYKEHUS	Bruk av e-post, chat, telefaks og SMS for kommunikasjon med og om pasienter				Side: 3 Av: 3
Dokument-id: I.5.9.2-2	Utarbeidet av: Geir Hovind	Fagansvarlig: Geir Hovind	Godkjent dato: 19.02.2025	Godkjent av: Kjetil Nyhus	Revisjon: 3.01

Foretaksnivå/Virksomhetsstyring/Informasjonssikkerhet og personvern/Utøvende - alle brukere

Retningslinjer for bruk av telefaks

Telefaks benytter kommunikasjon over åpne linjer og skal derfor vurderes som et usikret medium uegnet for kommunikasjon om helse – og personopplysninger.

Helse- og personopplysninger kan kun sendes på telefaks dersom faksmaskinen både hos avsender og mottaker har krypteringsfunksjon og denne er slått på. Dersom krypteringsfunksjon ikke finnes eller kan slås på, gjelder følgende:

- Opplysningene skal anonymiseres før de sendes, se dokumentet [Anonymisering av helse- og personopplysninger](#).
- Eller tilsvarende som beskrevet for e-post ovenfor.

Siden telefaks krever at direkte identitet fjernes, og kun initialer og fødselsdato kan sendes med, må det i parallell ringes mottaker for å opplyse om fullstendig personidentifikasjon.

Retningslinjer for bruk av SMS

I kommunikasjon med pasienten eller pårørende:

- Pasienter skal gjøres oppmerksom på sikkerhetsfaren og frarådes å sende SMS med sensitive opplysninger.
- Medarbeidere skal ikke sende SMS som inneholder sensitive opplysninger.
- Dersom du mottar SMS med sensitive opplysninger som er journalverdig/arkivverdig, må du loggføre informasjonen deretter og slette SMS. Kontakt pasienten og gjør oppmerksom på at sykehuset ikke besvarer SMS med sensitive opplysninger pga manglende sikkerhet i SMS-løsningen. Oppfordre vedkommende til å ta videre kontakt pr telefon eller brev. Oppgi kontaklinformasjon.
- Poliklinikker og andre som bruker løsninger for innkalling til time med SMS, må etablere egen prosedyre for forsvarlig bruk. Bruk av SMS til pasientadministrasjon ble tidligere fortolket til å kreve samtykke. Dersom pasient/bruker har oppgitt digital kontaklinformasjon til sykehuset kan dette anses som et samtykke til at virksomheten kan sende timepåminnelse per SMS. Vi må likevel forsikre oss om at innhold ikke inneholder sensitiv informasjon og at det sendes til riktig mottaker.

I kommunikasjon om pasienten, eksempelvis med eksternt helsepersonell

- Dersom du mottar SMS med sensitive opplysninger fra en kollega, skal den slettes. Avsender varsles om at den ikke besvares og at hun/han må ta initiativ til videre oppfølging på annen måte.
- Siden SMS krever at direkte identitet fjernes, og kun initialer og fødselsdato kan sendes med, må det i parallell ringes mottaker for å opplyse om fullstendig personidentifikasjon.

Kryssreferanser

[I.5.9.1-7](#)

[I.5.9.2-1](#)

[I.5.9.2-4](#)

[Forenklet sikkerhetsinstruks \(med signaturdelt\)](#)

[Bruk av e-post i SSHF: overordnet retningslinje](#)

[Anonymisering av helse- og personopplysninger](#)

Eksterne referanser