SYKEHUSET I VESTFOLD

Bruk av e-post, SMS, telefaks (digital kommunikasjon)

Gjelder for:	Hele SiV
Dokumenttype:	Prosedyre
Sist endret:	26.03.2024

Innholdsfortegnelse

1. HENSIKT

- Beskrive ansattes digitale kommunikasjon via e-post, SMS og telefaks
- Supplere de overordnede prosedyrene Informasjonssikkerhetsinstruks og Informasjonssikkerhet - Bruk av mobiltelefon
- Beskrive hvilke personopplysninger som *ikke kan/kan* formidles digitalt (e-post, SMS og telefaks) i kommunikasjon om og med pasient/pårørende. Dette skal bidra til at taushetsplikten overholdes.

Prosedyren **omfatter ikke** digital kommunikasjon i IKT-løsninger godkjent for deling av alle typer personopplysninger (eks. gule lapper i DIPS, godkjente digitale løsninger for brev).

2. ANSVAR

Hvem	Ansvar
Ledere på alle nivåer	• Gjøre retningslinjen kjent for alle sine ansatte • Følge opp at de ansatte etterlever kravene i denne retningslinjen
Alle ansatte uansett arbeidsforhold (ansatte)	• Følge denne retningslinjen

3. FREMGANGSMÅTE

3.1 Digital kommunikasjon

3.1.1 E-post

- All e-post anses i utgangspunktet som virksomhetsrelatert
- Privat e-post skal begrenses. Legges i egen mappe merket "Privat"
- Tildelt e-postadresse er personlig, og skal ikke benyttes av andre
- Alle som har tilgang til sykehusets e-postsystem og står oppført i sykehusets adresseliste, er forpliktet til å holde seg løpende oppdatert på innkomne e-poster
- Ved lengre fravær skal automatiske fraværsmeldinger benyttes med henvisning til hvem som kan kontaktes i ditt fravær
- Av hensyn til konfidensialitet, er det sperret for automatisk videresending til eksterne e-postløsninger
- E-post adressert til rolle eller funksjon bør rettes til felles e-postbokser som flere har tilgang til, for å unngå innsynsforespørsler i personlige e-postbokser
- For innsyn i ansattes e-post vises det til dokumentet Informasjonssikkerhet - Innsyn i ansattes epost og personlige hjemmekatalog
- Ved avslutning av arbeidsforholdet bør medarbeider sette opp fraværsmelding med informasjon om hvem som kan kontaktes (for å eliminere behov for innsyn etter at medarbeider har sluttet)
- Etter endt ansettelsesforhold slettes innholdet i e-post-konto etter 7 dager jf. sikkerhetsinstruksen

3.1.2 SMS

SMS skal ikke brukes til kommunikasjon med personopplysninger som ikke kan deles. Det gjelder både sykehuseid og privat IKT-utstyr med løsning for SMS.

Kontakt e-helse@siv.no ved behov for IKT-løsning for digital kommunikasjon via SMS.

3.1.3 Telefaks

Telefaks benytter kommunikasjon over åpne linjer og skal derfor anses som et usikret medium uegnet for kommunikasjon om personopplysninger som ikke kan deles

Personopplysninger kan 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 Informasjonssikkerhet - Anonymisering av helse- og personopplysninger

3.1.4 Vis varsomhet

- Dersom medarbeider mottar e-post fra ukjente avsendere og e-post som oppfattes som mistenkelig, skal Sykehuspartner eller informasjonssikkerhetsleder kontaktes. Lenke til intranettet: Vær varsom på mistenkelig e-post (fisp.no)
- Hvis eksterne kontakter oss og etterspør e-postadressen/mobiltelefonnummer til ansatte, skal dette ikke utleveres uten særskilt avtale med den enkelte
- Ikke spre SiV e-postadressen din ukritisk. Skill klart mellom e-post i jobbsammenheng og privat e-post
- Massedistribusjon av e-post til alle eller store deler av ansatte skal være jobbrelatert og godkjent av nærmeste leder, eventuelt kommunikasjonsavdelingen.
- Ansvarlig for distribusjon skal være kritisk til innholdet i informasjonen og hvem den sendes til. E-postmeldinger skal i utgangspunktet kun sendes til mottakere som har tjenstlig behov for informasjonen

3.1.5 Særlige kategorier personopplysninger (sensitive)

- Opplysninger som omfattes av lovbestemt taushetsplikt eks. sensitive personopplysninger, skal ikke sendes i e-post, SMS eller telefaks
- Mottas e-post, SMS eller telefaks med særlige kategorier personopplysninger gjør følgende:
    - Ved journalverdig/arkivverdig informasjon; dokumenter i EPJ/P360
    - Slett innholdet og evt vedlegg i sendingen og svar at kommunikasjon med sensitive opplysninger ikke besvares på e-post, sms, telefaks pga manglende sikkerhet.
    - Oppfordre vedkommende til å ta videre kontakt pr. telefon, brev eller sikker digital melding og oppgi kontaktinformasjon. Vis til Kontakt oss - Sykehuset i Vestfold (siv.no)
- Hvis ingen annen mulighet til dialog med mottaker, ikke besvar eller videresend før de særlige kategorier personopplysninger er fjernet eller tilfredsstillende anonymisert/kryptert, se Ofte stilte spørsmål - personvern og informasjonssikkerhet (fisp.no)
- Dersom du ved en feil sender sensitive personopplysninger på e-post, SMS eller telefaks skal du kontakte mottaker som skal bekrefte sletting. Avviket skal registreres i avvikssystemet (EQS)

3.2 Digital kommunikasjon om og med pasient/pårørende

Kontakt e-helse@siv.no ved behov for digital kommunikasjon og spørsmål om godkjente IKT-løsninger for sikker kommunikasjon.

Det anbefales ikke å bruke e-post/sms til kommunikasjon med pasient/pårørende f eks. ved påmelding til kurs, tilbakemelding fra forskningsdeltakere etc. Ved å åpne for det er det en risiko for at enkelte kan sende sensitive opplysninger i slike usikre IKT-løsninger selv om det er opplyst at det ikke skal sendes slike opplysninger der. Fortrinnsvis bør kontakt foregå på en annen måte enn e-post/sms, eksempel løsninger for tilbakemeldinger (eks Questback), eller telefon.

3.2.1 Følgende kan ikke deles/kan deles i eks e-post, sms, telefaks

Opplysninger	Kan ikke deles	**Kan deles**
Navn	x	
Fødselsnummer (11 siffer)	x	
Personnummer (de 5 siste siffer i fødselsnummer)	x	
Pasientnummer (NPR) sammen med personidentifiserende opplysninger og/eller helseopplysninger	x	
Alt som entydig identifiserer pasienten, direkte eller indirekte f.eks. helt spesielle diagnoser og hendelsesforløp eller kombinasjon av slik informasjon	x	
Pasientens initialer		x
Pasientens initialer + fødselsdato (uten de 5 siste sifre i fødselsnummeret), forutsatt at ikke andre detaljer likevel identifiserer personen		x
Fødselsdato		x
Pasientnummer (NPR) uten personidentifiserende opplysninger og/eller helseopplysninger (Det skal så langt det er mulig benyttes kommunikasjon via DIPS)		x

Vis varsomhet

- Unngå personopplysninger i «emne-feltet»
- Sikre riktig mottaker for sendingen
- Ikke bruk felles e-post-konto/postmottak ved sending til og fra SiV
- Sørg for å slette meldinger med personopplysninger som ikke skal deles digitalt

Når det er strengt nødvendig å dele helseopplysninger og personidentifikasjon, må dette gjøres i 2 separate sendinger slik at disse opplysningene ikke kan knyttes til hverandre.

3.3. Sikkerhetsgraderte opplysninger

Korrespondanse som er unntatt offentlighet og som inneholder opplysninger som omfattes av sikkerhetsloven skal følge foretakets egne prosedyrer for dette, jf. Sikkerhetsloven.

Ta kontakt med sikkerhetsleder eller informasjonssikkerhetsleder hvis noe uklart.

4. GENERELL

5. INTERNE REFERANSER

1.1.11.1.4	Informasjonssikkerhetsinstruks
1.1.11.2.3	Informasjonssikkerhet - Anonymisering av helse- og personopplysninger
1.1.11.2.5	Informasjonssikkerhet - Innsyn i ansattes epost og personlige hjemmekatalog
1.1.11.2.6	Informasjonssikkerhet - Bruk av mobiltelefon

1.1.11.3.1	Informasjonssikkerhet - Loggføring av aktivitet og kontroll av logger

6. EKSTERNE REFERANSER

Datatilsynet – Anonymisering av personopplysninger:
https://www.datatilsynet.no/Sikkerhet-internkontroll/Hvordan-anonymisere-personopplysninger/

7. VEDLEGG