

Informasjonssikkerhet - Bruk av mobiltelefon

Gjelder for: Hele SiV
Dokumenttype: Prosedyre
Sist endret: 10.09.2019

1. HENSIKT

- Denne prosedyren omhandler administrative rutiner for bruk av mobilt utstyr, og supplerer den overordnede [Informasjonssikkerhetsinstruks](#)
- Prosedyren gjelder også nettbrett dersom nettbrettet er satt opp for kommunikasjon ved hjelp av virksomhetens systemer.

2. ANSVAR

- **Administrerende direktør:** Er databehandlingsansvarlig og har det overordnede ansvaret for dette dokumentet.
- **Informasjonssikkerhetsleder:** Har det utøvende ansvar for sykehusets informasjonssikkerhetsarbeid, blant annet ved å godkjenne risikovurderinger og utføre internkontroll med informasjonssikkerheten i sykehuset.
- **Personvernombudet:** Har en rolle i å sikre at den enkeltes personvernrettigheter blir ivaretatt, at all bruk av personopplysninger skjer i samsvar med gyldig behandlingsgrunnlag og følger sykehusets retningslinjer for informasjonssikkerhet.
- **Ledere** innen ulike enheter og områder har ansvar for å påse at dette dokumentet implementeres og etterleves innen eget ansvarsområde. Det vil si at dokumentet er kjent, tilgjengelig og blir brukt.
- **Alle ansatte og innleide** ved sykehuset som skal lagre og behandle helse- og personopplysninger, skal forholde seg til dette dokumentet. Dette gjelder uavhengig av organisatorisk plassering og yrkesgruppe.

3. FREMGANGSMÅTE

1. Bruk av mobiltelefon i foretaket skal være et arbeidsverktøy for å forenkle kommunikasjon for medarbeidere.
2. Mobiltelefon må ikke brukes slik at den er til sjenanse for pasienter og medarbeidere.
3. Det oppfordres til minst mulig privat bruk i arbeidstiden.
4. Vis hensyn ved å bruke varsling via vibrasjon eller ringetone på laveste nivå.
5. Mobiltelefoner som eies av foretaket skal fortrinnsvis være tilknyttet MDM, med muligheter for fjernsletting, hvis MDM finnes for virksomheten.
6. Mobiltelefon med synkronisering krever minimum registrering og godkjenning fra nærmeste leder
7. Mobiltelefon eller nettbrett med synkronisering skal
 - a. kun synkronisere e-postens innbokser, kalenderen, notater, kontaktpersoner og oppgaver
 - b. ha aktivisert automatisk tastelås
 - c. ha aktivisert kodelås for åpning av telefonen når tastelåsen er aktiv
8. For å ivareta personvernet og taushetsplikten er det ikke lov å ta bilder av pasienter eller pårørende med mobiltelefon. Ved behov for bilder i pasientbehandling skal foretakets fotoapparat benyttes og foretakets retningslinjer for bruk av dette skal følges. For lagring av bildemateriale, se dokumentet [Informasjonssikkerhet - Lagring, arkivering og sletting av helse- og personopplysninger](#)
9. Det skal ikke lagres noen form for helse- eller personopplysninger mottatt i egenskap av å være helsepersonell/ansatt i sykehuset på mobiltelefonen. Dette

inkluderer sendte meldinger, mottatte meldinger, dokumenter og bilder med tekstlig eller visuell informasjon med helse- eller personopplysninger.

10. Bilder av medarbeidere følger prinsippet om forhåndssamtykke fra den avbildede.

11. Sykehuset har ikke ansvaret for private opplysninger (f.eks. private bilder) som eventuelt lagres på mobiltelefonen.

Definisjoner:

- Privat mobiltelefon
 - Eies og benyttes av brukeren. Benyttes ikke i pasientbehandling og synkroniseres ikke med sykehusets systemer.
- Personlig mobiltelefon
 - Eies av sykehuset og benyttes av brukeren. Følger sykehusets interne rutiner for bestilling, oppsett, bruk og vedlikehold.
- Rollebasert mobiltelefon
 - Eies av sykehuset og benyttes av flere brukere. Følger sykehusets interne rutiner for bestilling, oppsett, bruk og vedlikehold.

4. GENERELT

5. INTERNE REFERANSER

1.1.11.1.4	Informasjonssikkerhetsinstruks
1.1.11.2.1	Informasjonssikkerhet - Lagring, arkivering og sletting av helse- og personopplysninger
1.1.11.2.12	Informasjonssikkerhet - Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet
1.4.6.3.1	Bruk av mobiltelefon, nettbrett og bærbar PC i nærhet til MTU

6. EKSTERNE REFERANSER

7. VEDLEGG