Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Sikring av mobilt utstyr utenfor virksomheten

Støttedokument
Faktaark nr 30
Versjon: 3.1
Dato: 01.10.2018

Formål	Sikre konfidensialitet, integritet og tilgjengelighet for helse- og personopplysninger som registrerer, endres og lagres på mobilt utstyr.		
Ansvar	Virksomhetens leder skal beslutte bruk av mobilt utstyr. IKT-ansvarlig skal påse at det blir etablert teknisk løsning og utarbeidet nødvendige prosedyrer som ivaretar kravet til sikkerhet.		
Gjennomføring	Regler og prosedyrer skal etableres før mobilt utstyr benyttes til behandling av helse- og personopplysninger.		
Omfang	Omfatter alle typer mobilt utstyr; bærbar PC, nettbrett, mobiltelefon, digitalt kamera og video som brukes av ansatte i tjeneste utenfor virksomheten (for eksempel hjemmetjeneste).		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Leverandør ☒ IKT-ansvarlig ☐ Forsker ☒ Prosjektleder	☒ Sikkerhetsleder / sikkerhetskoordinator ☒ Virksomhetens leder/ledelse ☐ Forskningsansvarlig	☐ Medarbeider/ansatt ☒ Databehandler ☐ Personvernombud
Hjemmel	Personvernforordningen artikkel 32		
Referanser	• Norm for informasjonssikkerhet kpt. 5.3.4 • Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, april 2008		

Merknad 01.10.2018: Utdaterte hjemler og referanser er fjernet, men dokumentet kan inneholde tekst som er foreldet ut fra siste versjon av Normen, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

Definisjoner

Med "***Apparatlås***" menes en kode eller et passord som benyttes til å låse en mobiltelefon eller nettbrett. Apparatlåsen kan sammenlignes med en skjermsparer med passord.

Med "***PIN-kode***" menes koden som benyttes til å autentisere seg overfor SIM-kort hver gang mobiltelefonen eller nettbrettet startes.

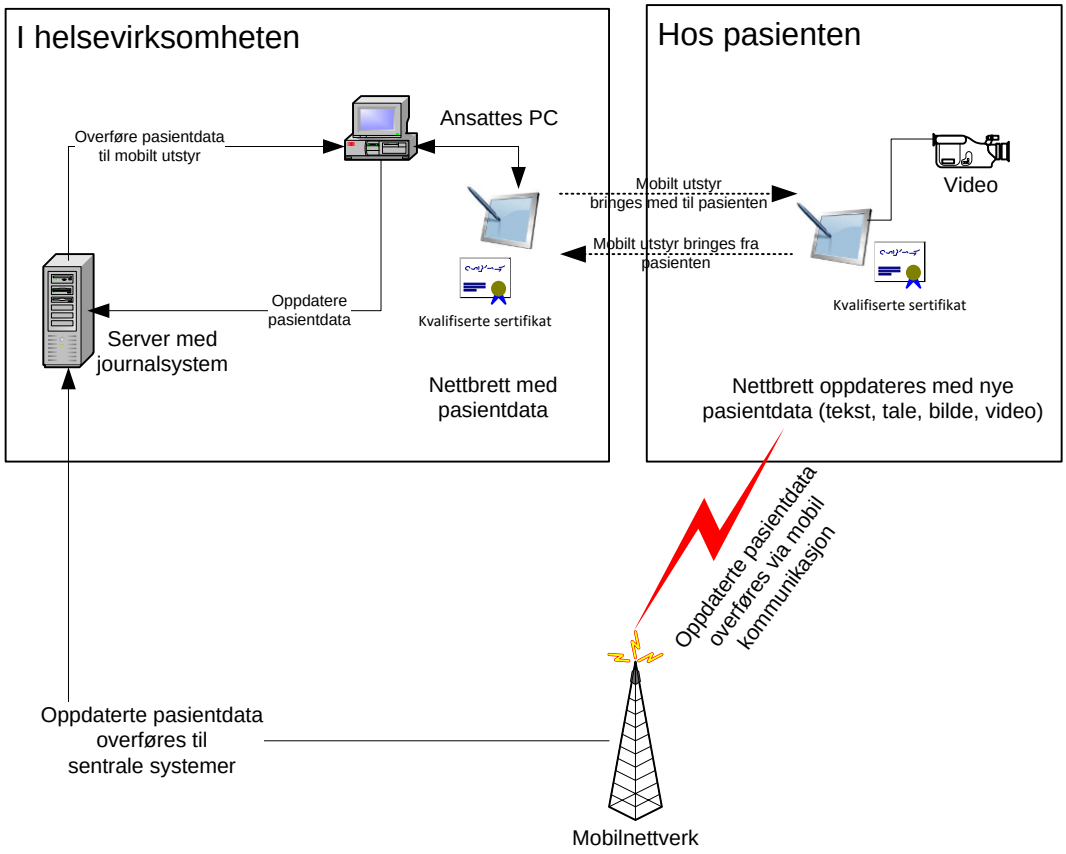
Med "***Sikkerhetskode for elektronisk ID***" menes den personlige koden som benyttes til å autentisere på sikkerhetsnivå 4 ved hjelp av mobiltelefon eller nettbrett.

Nr.	Handling/Utførelse
1	**Bestemme bruksområder for mobilt utstyr** a) Avgjøre ved hvilke tjenester utenfor virksomheten mobilt utstyr skal benyttes; besøkstjenester, hjemmetjeneste, legevakt, akuttmedisinske tjenester, osv b) Avgjøre om mobilt utstyr skal benyttes til å: - Motta helse- og personopplysninger fra sentrale systemer - Mellomlagre helse- og personopplysninger - Bearbeide helse- og personopplysninger - Overføre helse og personopplysninger til annet utstyr - Overføre helse- og personopplysninger til sentrale systemer - Utføre administrative funksjoner (for eksempel avtalebok) c) Avgjøre hvilken type informasjon mobilt utstyr skal benyttes til - Tekst - Tale/lyd

Nr.	Handling/Utførelse
	- Bilder - Video - Strukturert datafangst via strekkode, rfid eller annen dedikert teknologi
2	**Bestemme tekniske sikkerhetsregler** a) Fastsette nivå for akseptabel risiko. Virksomheten skal vurdere hva som er nødvendige sikringsmekanismer ift den faktiske bruken; omfang av data på utstyret, sletteprosedyrer, sannsynligheten for at utstyret kommer på avveie, muligheten for 3. part å få innsyn, hvor lett det er å identifisere enkeltpersoner, osv. b) Gjennomføre risikovurdering av bruk av mobilt utstyr c) Prioritere tiltak som ivaretar forholdsmessig sikring
3	**Etablere tekniske sikkerhetstiltak** a) Innføre relevante tekniske tiltak - Kryptering av lagringsmedium eller data - Autorisasjon og autentisering - Sikkerhetsnivå 4 for autentisering ved pålogging til sentrale systemer som inneholder helseopplysninger - Fjerne funksjoner / tjenester som ikke skal benyttes (om dette er mulig. Alternativt må slike tiltak avtales med bruker) - Antivirusprogram - Sikker datakommunikasjon inklusive behandling av bilder og film med hensyn til SMS og MMS
4	**Etablere prosedyrer for bruk av mobilt utstyr** a) Opplæring i bruk av mobilt utstyr slik at bruker er fortrolig med hvordan det skal brukes b) Utlevering og innlevering av mobilt utstyr slik at behandlingsansvarlig har god kontroll med hvem som benytter mobilt utstyr til hva c) Sikker oppbevaring. Utstyret transporteres fra virksomhet til pasient / bruker og kan utsettes for tyveri, tap og ødeleggelse d) Regler for registrering, endring, retting og sletting av helse- og personopplysninger på mobilt utstyr e) Regler for overføring av helse- og personopplysninger til/fra sentrale systemer. Slik overføring anbefales utført på kontoret/arbeidsplassen til den enkelte og ikke fra hjemmekontor f) Regler for beskyttelse av sikkerhetskode for elektronisk ID på mobiltelefoner og nettbrett. Sikkerhetskode for elektronisk ID på mobiltelefon og nettbrett er personlig og skal være utilgjengelig for andre. Sikkerhetskode for elektronisk ID skal ikke være det samme som PIN-koden til SIM-kortet eller apparatlåsen g) Brukeravtale. Det skal her presiseres at dette er dedikert utstyr til definerte oppgaver og skal ikke benyttes til annet enn predefinerte oppgaver h) Avhende eller overføre mobilt utstyr til annen bruker, herunder sletting av data

Eksempel

Eksempelet under illustrerer bruk av mobilt utstyr i en hjemmetjeneste hvor det lagres helse- og personopplysninger som bringes med hjem til pasienten/bruker. Illustrasjonen er ment å gi innspill på områder som må fokuseres på i en risikovurdering. Viktige områder som må vurderes er bl.a. overføring av helse- og personopplysninger via plugg i veggen eller mobil kommunikasjon, data på lokalt utstyr (ansattes PC), mellomlagring av data på mobilt utstyr og oppdatering av sentralt lagrede helse- og personopplysninger.


I helsevirksomheten
Hos pasienten
Overføre pasientdata til mobilt utstyr
Ansattes PC
Mobilt utstyr bringes med til pasienten
Mobilt utstyr bringes fra pasienten
Video
Oppdatere pasientdata
Server med journalsystem
Kvalifiserte sertifikat
Kvalifiserte sertifikat
Nettbrett med pasientdata
Nettbrett oppdateres med nye pasientdata (tekst, tale, bilde, video)
Oppdaterte pasientdata overføres via mobil kommunikasjon
Oppdaterte pasientdata overføres til sentrale systemer
Mobilnettverk