NORMEN

Hjemmekontor og annet fjernarbeid (faktaark 29)

Versjon 3.0

11.06.2021

Utarbeidet med støtte fra direktoratet for e-helse

Vedtatt av styringsgruppen for Normen

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Dette faktaarket omhandler hjemmekontor og annet fjernarbeid og hvordan virksomheten skal og bør implementere organisatoriske og tekniske sikkerhetstiltak ved bruk av hjemmekontor og ved annet fjernarbeid. I tillegg gis det anbefalinger til krav og vilkår som virksomheten bør stille til brukerne som arbeider utenfor virksomhetens lokaler.
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er IKT-ansvarlige, sikkerhetsleder og IT-driftspersonell i virksomheten som er ansvarlig for å tilrettelegge for sikkerhet på hjemmekontor eller utarbeide administrative prosedyrer for brukerne av hjemmekontor.
Krav i Normen	Faktaarket gjelder følgende kapitler i Normen • Kapittel 3.4 Risikovurdering og risikohåndtering • Kapittel 5.1.1 Vilkår og betingelser • Kapittel 5.1.3 Opphør av arbeidsforhold • Kapittel 5.2.2 Autentisering • Kapittel 5.3.4 Mobilt utstyr og hjemmekontor • Kapittel 5.3.5 Kryptering • Kapittel 5.4.1 Konfigurasjonskontroll
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser, standarder og andre rammeverk er spesielt relevante for faktaarket: • Pasient- og brukerrettighetsloven § 3-6 Rett til vern mot spredning av opplysninger • Pasientjournalloven § 15 Taushetsplikt & § 21 Personopplysninger fra Folkeregisteret • Spesialisthelsetjenesteloven § 2-2. Plikt til forsvarlighet • Forskrift om ledelse og kvalitetsforbedring §§ 6 – 9, jf. § 5 • NSMs Grunnprinsipper for IKT-sikkerhet 2.0 • ISO/IEC 27001 & ISO/IEC 27002 • CIS Controls

Hjemmekontor og annet fjernarbeid

Det skal iht. Normen etableres administrative rutiner for bruk av mobilt utstyr og hjemmekontor i virksomheten[1]. I tillegg vil det alminnelige kravet[2] i Normen om sikkerhetstiltak også gjelde tekniske tiltak relevante for hjemmekontor. Virksomhetens ansvar for informasjonssikkerheten gjelder også for sikkerheten på hjemmekontor og ved annet fjernarbeid. I dette faktaarket gis det anbefalinger om hvilke tiltak som bør etableres og hvilke forhold som bør beskrives i styringssystemet til virksomheten ved etablering av og arbeid på hjemmekontor, samt ved annet fjernarbeid.

Med «hjemmekontor» menes i Normen behandling av helse- og personopplysninger på PC som virksomheten har stilt til disposisjon, fra f.eks. hjem, hytte, hotellrom eller lignende. Bruk av PC som virksomheten ikke har stilt til disposisjon (for eksempel PC på internettkafé, hotell-PC, flyplass-PC), er ikke definert som hjemmekontor[3]. Anbefalingene i dette faktaarket vil i tillegg gjelde ved bruk av annet sluttbrukerutstyr enn PC som benyttes ifm. hjemmekontor eller annet fjernarbeid, som f.eks. datamaskiner, eksterne lagringsenheter og printer. Faktaarket adresserer også anbefalinger til tiltak dersom datamaskin som benyttes på hjemmekontor eller til annet fjernarbeid ikke er stilt til disposisjon av virksomheten (for eksempel bruk av private datamaskiner til arbeid på hjemmekontor).

Faktaarket omhandler ikke forhold som er særskilte for mobile enheter som benyttes i det daglige arbeidet, som for eksempel mobiltelefon og nettbrett. Denne typen enheter brukes ikke bare på hjemmekontor, men i stor grad også av helsepersonell som utfører oppgaver for eksempel hjemme hos pasienter eller ambulansetjeneste. Mobile enheter er derfor nærmere omtalt i et eget faktaark, *Sikring av mobilt utstyr utenfor virksomheten (faktaark 30).*

Faktaarket tar utgangspunkt i at brukeren skal etablere hjemmekontor innenfor EU/EØS-området. Det bør utarbeides en egen reisepolicy i virksomheten for bruk av hjemmekontor på reiser og opphold i utlandet, basert på relevante veiledere[4]. Ved behov for å etablere hjemmekontor i land utenfor EU/EØS og dermed aksessering av helse- og personopplysninger utenfor EU/EØS, vil det være behov for å gjøre særskilte vurderinger omtalt i Normen 6.0[5].

Risikovurdering som grunnlag - også for hjemmekontor og annet fjernarbeid

Det er et krav i Normen at virksomheten skal gjennomføre risikovurderinger. Når risikovurderingen gjøres bør virksomheten også vurdere behovet for bruk av hjemmekontor, samt annet fjernarbeid og sikkerhetsnivået som da skal etableres.

Et sentralt forhold virksomheten bør vurdere er i hvilken grad virksomheten skal ha kontroll med konfigurasjonen i IKT-utstyret på hjemmekontoret eller i annet fjernarbeid. I noen tilfeller kan det være en akseptabel risiko at for eksempel privat utstyr brukes til pålogging til løsninger, dersom det er innført tiltak for å hindre lokal lagring, flytting av informasjon og at skadevare gir uautoriserte tilgang til informasjonen. Normalt vil imidlertid risikoen være

[1] Normen 6.0 kapittel 5.3.4 Mobilt utstyr og hjemmekontor
[2] Normen 6.0 kapittel 3 andre avsnitt & kapittel 5 først avsnitt
[3] Normen 6.0 kapittel 6.1 Definisjoner
[4] Nettvett - Sikkerhet på reise i utlandet & *Sikker Reise - PST*
[5] Normen 6.0 kapittel 5.7.8 Overføring av opplysninger til utlandet

vesentlig høyere der virksomheten ikke har kontroll med konfigurasjonen. Dette fordi det kan finnes sikkerhetshull i løsninger for fjernaksess, kombinert med at privat IKT-utstyr normalt vil ha færre sikkerhetsmekanismer for øvrig (manglende sikkerhetsovervåkning, mindre sporbarhet i sikkerhetstilstanden, samt lavere kompetanse og bevissthet om sikring av IKT-utstyret). Det bør derfor utvises varsomhet med å tillate privat IKT-utstyr for tilgang til helse- og personopplysninger og det anbefales ikke.

Når risikoen vurderes er det spesielt viktig at behovet for konfidensialitet og tilgjengelighet vurderes.

Med hensyn til konfidensialitet vil skadepotensialet dersom uvedkommende får tilgang til helse- og personopplysninger, og muligheten for at det kan skje, være en viktig faktor. I en slik vurdering bør det tas i betraktning at også familiemedlemmer er å anse som uvedkommende.

Når det gjelder tilgjengelighet er det viktig å vurdere konsekvensen dersom opplysningene ikke er tilgjengelige for den som har hjemmekontor eller annet fjernarbeid når denne trenger det, og muligheten for at tilgjengelighetsbrudd kan oppstå. Stabiliteten til fjernaksessløsninger bør derfor vurderes. Videre bør det inngå i vurderingen at nettilgangen fra et privat hjem eller andre steder fjernarbeid skjer fra, kan være mindre stabilt enn på arbeidsplassen.

Ved valg av egnede tekniske og organisatoriske tiltak skal virksomheten alltid vurdere tiltakene opp mot virksomhetens art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv. Tiltak skal ikke gå utover virksomhetens plikt til å levere forsvarlige helsetjenester[6].

Oversikt

Anbefaleringer om sikkerhetstiltak for hjemmekontor presenteres i tabellen under, inndelt i følgende hovedpunkter:

1. Anbefalinger til tiltak ut ifra om virksomheten har kontroll med konfigurasjonen på IKT-utstyret som benyttes hjemmekontor eller til fjernarbeid.
2. Anbefalinger til forutsetninger for etablering av hjemmekontor og fjernarbeid
3. Anbefalinger til krav og vilkår som virksomheten bør stille til brukerne av hjemmekontor og fjernarbeid.
4. Anbefalinger til avvikling av hjemmekontor.

De ulike temaene er markert med overskrifter med understrek. I overskriften og underpunktene er ordet «skal» brukt om krav som står i Normen, mens «bør» er brukt om tiltak som normalt anbefales.

[6] Spesialisthelsetjenesteloven § 2-2. Plikt til forsvarlighet & Forskrift om ledelse og kvalitetsforbedring §§ 6 – 9, jf. § 5

Nr.	Aktivitet/Beskrivelse
1.	**Anbefalinger til tiltak ut ifra om virksomheten har kontroll med konfigurasjonen på IKT-utstyret som benyttes på hjemmekontor eller til annet fjernarbeid**

Det skal alltid gjennomføres risikovurdering for å avgjøre hvilke administrative og tekniske sikkerhetstiltak som skal etableres for å redusere risikoen for at eksterne får tilgang til helse- og personopplysninger.[7]

Virksomheten skal ha kontroll med konfigurasjonen i eget IKT-utstyr og programvare som er tildelt for hjemmekontor eller som brukes til annet fjernarbeid[8]

- Virksomheten er konfigurasjonsansvarlig for datamaskin slik at utstyret konfigureres på sikker måte.
- Kun godkjent utstyr og programvare skal benyttes til behandling av helse- og personopplysninger, herunder eksterne lagringsmedier. Privat utstyr kan godkjennes, men da bør kompenserende tiltak brukes, se neste avsnitt.
- Konfigurasjonen skal sikre at utstyret og programvaren kun utfører de funksjoner som er formålsbestemt.
- IKT-utstyr på hjemmekontor skal ikke ha helse- og personopplysninger lagret lokalt, så fremt dette ikke er nødvendig ut fra tjenstlig behov. Opplysningene bør kun nåes ved oppkobling til sentralt lagrede data i (i virksomheten og/eller hos databehandler).
- Det skal etableres antivirus- og brannmursikring på datamaskin.
- Sikkerhetsoppdateringer for programvare skal installeres løpende og bør automatiseres om mulig.
- Virksomheten bør aktivere tidsstyring for skjermlåsing av datamaskin tilpasset brukerens arbeidsøkt.

Dersom virksomheten har godkjent at annet enn virksomhetens eget IKT-utstyr brukes (for eksempel privat IKT-utstyr), hvor virksomheten ikke har kontroll på konfigurasjonen, bør løsningen hindre lokal lagring av helse- og personopplysninger og kompenserende sikkerhetstiltak bør etableres.[9]

- Dersom IKT-utstyret som er godkjent brukt på hjemmekontoret ikke er tildelt av virksomheten, skal virksomheten etablere programvareløsninger som likevel tilrettelegger for sikker og kryptert lagring og behandling av tilgang til helse- og personopplysninger. I tillegg bør løsningen hindre at helse- og personopplysninger lagres lokalt. Eksempler på slik løsning er desktop-virtualisering (VDI) eller Remote Desktop Services (RDS), hvor bruker kan aksessere en virtuell desktop knyttet til virksomhetens sentrale servere. Det er da viktig at løsningen settes opp til å forhindre at data hentes ut av virksomhetens nettverk (forhindre kopiering ut fra virksomhetens nettverk, utskrift og lokal lagring mm.).

[7] Normen 6.0 Kapittel 3.4 Risikovurdering og risikohåndtering

[8] Normen 6.0 Kapittel 5.4.1 Konfigurasjonskontroll

[9] En privatperson er et annet rettssubjekt enn virksomheten. Lagring av personopplysninger på privat utstyr vil derfor normalt mangle behandlingsgrunnlag etter personopplysningsloven, selv om privatpersonen er ansatt i virksomheten.

2. Anbefalinger til forutsetninger for etablering av hjemmekontor og annet fjernarbeid

Tilgang fra hjemmekontor og annet fjernarbeid skal sikres ved sikker autentiseringsløsning[10]

- Tilgang fra hjemmekontor og fjernarbeid skal sikres ved sikker autentiseringsløsning. Dette gjelder også for lokasjoner som kommuniserer ved hjelp av linjer virksomheten ikke har fysisk kontroll over.
- Det skal etableres teknisk løsning hvor brukeren autentiseres med sikkerhetsnivå betydelig eller høyt[11] dersom det skal behandles helse- og personopplysninger.
- All aksess inn mot virksomhetens infrastruktur og løsninger, inkludert skytjenester, bør benytte to-faktor autentisering når det er tilgjengelig.

Virksomheten skal ha kontroll på alt eget utstyr som benyttes i behandlingen av helse- og personopplysninger, også på hjemmekontor og ved annet fjernarbeid[12]

- Virksomhetens utstyr på hjemmekontor skal ikke brukes til annet enn det virksomheten har bestemt.
- Virksomheten skal ha oversikt over hvilket IKT-utstyr som virksomheten har stilt til disposisjon for buk på hjemmekontor for tilgang til helse- og personopplysninger[13]. IKT-utstyr som virksomheten eier bør merkes.

All kommunikasjon av helse- og personopplysninger skal være kryptert[14]

- All kommunikasjon, enten dette skjer vha. trådløst nett eller vha. datalinjer, skal sikres med kryptering[15].
- For kryptering av kommunikasjon anbefales det at virksomheten har konfigurert virtuelt privat nettverk (VPN)[16], RDS eller VDI på alle datamaskiner som benyttes for hjemmekontor eller til annet fjernarbeid[17]. Normalt er VDI og RDS sikrere enn VPN, fordi med VPN kan kopiering av data ut fra virksomhetens nettverk, utskrift og lokal lagring ikke forhindres. VDI og RDS er derfor bedre egnet enn VPN der for eksempel virksomheten ikke har kontroll med konfigurasjonen i utstyret for øvrig.
- Dersom VPN benyttes bør brukeren instrueres om å aktivere VPN med en gang utstyret tas i bruk eller automatisere påloggingsprosessen når brukeren logger seg på datamaskinen.

[10] Normen 6.0 kapittel 5.2.2 Autentisering
[11] Ulike sikkerhetsnivå
[12] Normen 6.0 kapittel 5.4.1 Konfigurasjonskontroll
[13] Normen 6.0 kapittel 5.4.1 Konfigurasjonskontroll sammenholdt med definisjonen av hjemmekontor i vedlegg til Normen 6.1
[14] Normen 6.0 kapittel 5.3.5 Kryptering
[15] Grunnprinsipper for IKT-sikkerhet 2.0 - beskyttelse av data i ro og data i transitt
[16] Virtuelt privat nettverk
[17] Hjemmekontor - hva bør virksomheten tenke på?

- Dersom VPN benyttes bør eget utstyr og kommunikasjonspartens utstyr konfigureres slik at det sikres at begge parter er den de gir seg ut for å være ved bruk sertifikater på server- og klientsiden.

Dersom virksomheten åpner for at ansatte og oppdragstakere kan få utføre oppgaver utenfor arbeidsplassen hos virksomheten, bør det sikres at nødvendige IKT-ressurser er tilstrekkelig tilgjengelige.

- Virksomheten bør utarbeide veiledning for hvordan de ansatte enkelt skal kunne koble seg til virksomhetens ressurser fra hjemmekontor eller ved annet fjernarbeid.
- Ved bruk av VPN, RDS eller VDI bør virksomheten sikre at løsningen har tilstrekkelig kapasitet til å håndtere belastningen dersom et utvidet antall ansatte jobber fra hjemmekontor eller driver fjernarbeid.
- Virksomheten bør tilrettelegge for at den ansatte får tilstrekkelige ressurser til å jobbe effektivt fra hjemmekontor. Det vil si at den ansatte har utstyr som tilrettelegger for arbeid fra hjemmekontor eller annet fjernarbeid når det er behov for det. Eksempel på slikt utstyr er en egnet datamaskin som kan kobles opp mot virksomhetens sentrale ressurser.

3. Anbefalinger til krav og vilkår som virksomheten bør stille til brukerne av hjemmekontor og annet fjernarbeid

Virksomheten skal etablere interne administrative prosedyrer for brukerne av hjemmekontor[18] og ha retningslinjer for privat bruk av informasjonssystemer og utstyr[19]. Videre bør virksomhetens prosedyrer for bruk av Internett og e-post følges i forbindelse med hjemmekontor og annet fjernarbeid.

Følgende forhold bør inngå i virksomhetens retningslinjer til brukerne:

- Ved arbeid med helse- og personopplysninger på hjemmekontor skal det iverksettes tiltak for å hindre innsyn fra eksterne (f.eks. familiemedlemmer og andre). Det bør vurderes sikring av
  - vinduer og dører (åpning og innsyn)
  - utstyret og hvordan det oppbevares
  - det aktuelle rommet hvor utstyret er plassert.
- Skjermfilter bør brukes for å hindre innsyn fra uvedkommende.
- Bruker bør sørge for at andre ikke kan overhøre samtaler i videomøter. For opplysninger det er taushetsplikt om er dette et krav.
- Ingen andre enn den som er autorisert til å bruke virksomhetens datamaskin skal benytte den.
- Papirutskrifter av helse- og personopplysninger skal ikke forekomme, så fremt det ikke er strengt nødvendig. Utskrifter som inneholder helse- og personopplysninger, skal oppbevares sikkert og/eller umiddelbart makuleres etter bruk. Uautorisert innsyn til (papir)utskrifter med helse- og personopplysninger skal forhindres.

[18] Normen 6.0 kapittel 5.3.4 Mobilt utstyr og hjemmekontor
[19] Normen 6.0 kapittel 5.1.1 Vilkår og betingelser

- Datamaskin på hjemmekontor bør låses med skjermlås med en gang brukeren forlater datamaskinen.
- Datamaskin på hjemmekontor skal til enhver tid være oppdatert med sikkerhetsoppdateringer, både for operativsystem og annen programvare[20].
- Kun lagringsenheter som er godkjent av virksomheten skal benyttes i arbeidet (f.eks. eksterne harddisker og minnepinner).
- Virksomheten bør beskrive om det er tillatt å lagre helse- og personopplysninger lokalt på datamaskinen og i så fall i hvilke tilfeller.
- Helse- og personopplysninger skal ikke lages i skylagringsløsninger for privat bruk eller på privat eide datalagringsmedia.
- Virksomheten bør fraråde eller blokkere nedlastning av ikke godkjent programvare.
- Brukeren bør kun koble opp mot nettverk som er sikret[21]
    - Trådløst hjemmenett bør sikres med passord (WPA2 eller helst WPA3[22])
    - Ved behandling av helse- og personopplysninger bør bruk av åpne og offentlige nettverk unngås (f.eks. på hotell, cafeer, offentlige transportmidler og flyplasser). Dersom sikkert nettverk ikke er tilgjengelig, bør bruker søke å benytte 4G (eller nyere) for tilkobling (f.eks. tilkobling via mobiltelefon).

4. Anbefalinger til avvikling av hjemmekontor og annet fjernarbeid

Når utstyr som brukes i en hjemmekontorløsning eller til annet fjernarbeid skal avvikles (f.eks. ved opphør av behov, avslutning av arbeidsforhold, skifte av utstyr, mv.) gjelder følgende[23]:

- Lagringsmedier som kan inneholde helse- og personopplysninger skal leveres tilbake til virksomheten
    - Alle helse- og personopplysninger på hjemmekontor skal leveres tilbake til arbeidsgiver, slettes eller makuleres
    - Ved en eventuell privat overtakelse av virksomhetens utstyr bør virksomheten sikre at datamaskinen nullstilles og lisenser for medfølgende programvare avklares.
- Dersom avvikling skjer i forbindelse med endring av roller eller avslutning av arbeidsforhold, skal tilganger til informasjonssystemer og lagringsområder endres eller fjernes.

[20] Nettvett - ti tips sikker pc bruk
[21] Nettvett - Sikkerhet på hjemmekontor
[22] Grunnprinsipper for IKT-sikkerhet 2.0 - Beskytt virksomhetens nettverk
[23] Normen 6.0 kapittel 5.1.3 Opphør av arbeidsforhold