NORMEN

Veileder for fjernaksess mellom virksomhet og leverandør

Versjon 3.0
Juni 2022

Utgitt av

Direktoratet for e-helse

Innhold

1 Innledning

1.1 Bakgrunn

Virksomheter som har ansvar for at behandling av helse- og personopplysninger skal ivareta informasjonssikkerhet, taushetsplikt og sikre pasientenes personvern. Dette samtidig som opplysningene er tilgjengelige for personell som trenger det.

For de fleste virksomheter i sektoren, er det nødvendig at leverandører bistår ved hjelp av fjernaksess. Dokumentet skal veilede virksomheten i etablering av avtalefestede sikrings- og kontrolltiltak mellom virksomheten og leverandøren, for å ivareta sikkerhet og akseptabel risiko i IKT-løsninger og tjenester som ytes for fjernaksess til helse- og personopplysninger.

Med «virksomhet» menes i Normen juridisk enhet som helseforetak, helseforvaltning, kommune, sykehus, legepraksis, tannklinikk, apotek, apotekkjede, røntgeninstitutt, frittstående laboratorium, universitet, høyskole, stiftelse mv.[1] I denne veilederen presiseres det at «virksomheten» er dataansvarlig for helse- og personopplysninger som løsning for fjernaksess behandler eller gir tilgang til, og oppdragsgiver for «leverandøren».

Med «leverandør» menes i Normen juridisk enhet som yter tekniske og/eller administrative tjenester til virksomheten.[1] I denne veilederen presiseres det at «leverandøren» er tjenesteleverandør for IKT-tjenester som ytes for å oppnå fjernaksess til helse- og personopplysninger som virksomheten er dataansvarlig for. Leverandøren er normalt databehandler.

1.2 Tema for veilederen

Virksomheten er (som dataansvarlig) ansvarlig for at fjernaksess til helse- og personopplysninger, teknisk løsning og tjenestene som ytes, oppfyller krav i norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen). Leverandøren (som databehandler) skal oppfylle krav i Normen, og avtalen som tas frem med grunnlag i denne veilederen, skal tilrettelegge for dette.

Oppgaver som utøves i sammenheng med fjernaksess kan deles mellom virksomheten og leverandøren, etter skriftlig avtale. Dokumentet gir veiledning i etterlevelse av krav, med teknologiske og administrative tiltak som skal eller anbefales oppfylt av virksomheten og leverandøren i henhold til Normen. Teknisk fjernaksessløsning skal ivareta Normens gjeldende krav, uavhengig av valgt løsning, tjenesteleverandør eller organisering. Dette gjelder f.eks. uavhengig om virksomheten inngår kundeavtale med Norsk Helsenett SF eller ikke.

Veilederen gjelder fjernaksess til alle typer informasjonssystemer som brukes til å behandle helse- og personopplysninger. Eksempler kan være fagsystemer[2], medisinsk teknisk utstyr[3] (MTU) og IKT-infrastruktur[4].

[1] Definisjonen i vedlegg til gjeldende utgave av Normen
[2] F.eks. elektronisk pasientjournal (EPJ), pasientadministrative systemer og laboratoriesystemer.
[3] F.eks. medisinsk billeddiagnostikk.
[4] F.eks. servere, sluttbrukermaskiner, nettverk, lagringsutstyr, kommunikasjonsutstyr, sikkerhetsteknologi, m.fl. Jfr. definisjonen av «infrastruktur» i Normen.

1.3 Målgruppe

Målgruppen for veilederen er virksomheter og leverandører som omfattes av Normen, ved etablering og sikring av fjernaksess til helse- og personopplysninger.

Veilederen gir *virksomheten* grunnlag for valg av løsning for fjernaksess samt etablering av løsningen og organisering iht. krav i Normen. Virksomheten kan bruke veilederen som et hjelpemiddel for utarbeidelse av krav til og avtale med leverandører.

Veilederen gir *leverandøren* av systemer og tekniske løsninger, som benyttes til behandling av helse- og personopplysninger, et grunnlag for å etablere løsning for fjernaksess iht. Normen. Leverandøren kan også vise til veilederen overfor virksomheter, slik at personell med helhetlig bestillerkompetanse[5] i virksomheten involveres.

1.4 Krav i Normen

I Normen er flere krav relevante for fjernaksess mellom virksomhet og leverandør, men omtales spesifikt i følgende kapitler:

- 5.4.1 Konfigurasjonskontroll,
    - Vedlikehold og oppdateringer (av enheter- og programvare)
    - Bruk av tiltrodde kanaler for fjernaksess (som virksomheten har kontroll med)
- 5.7.2 Generelt om avtaler og leverandøroppfølging
- 5.7.5 Vedlikehold, fjernaksess eller fysisk service
    - IT-infrastruktur, herunder
        - Leverandørens (IT-)utstyr
        - Medbrakt (IT-)utstyr
        - Kommunikasjonsnett(verk)
    - Tilgangsstyring, herunder
        - Autoriserte tilganger,
        - Logging av tilganger,
        - Kontroll av tilganger
    - Tilgjengelighet til opplysninger (når leverandøren utfører arbeid).

I tillegg til overnevnte kapitler, som omtaler fjernaksess spesifikt, er også følgende krav i Normen 6.0 relevante for fjernaksess:

- Leverandørforhold og avtaler (kapittel 5.7),
- Tilgangsstyring (kapittel 5.2),
- Sikker IT-drift (kapittel 5.4),
- Kommunikasjonssikkerhet (kapittel 5.5),
- Fysisk sikkerhet og håndtering av utstyr (kapittel 5.3)
- Håndtering av informasjonssikkerhetsbrudd (kapittel 5.8)

Ved etablering og endring av løsninger for behandling av helse- og personopplysninger (herunder løsninger for fjernaksess) er også følgende krav aktuelle:

[5] Normen 6.0 kapittel 5.7.7 Leverandøroppfølging.

- Risikostyring (kapittel 3), herunder risikovurdering og risikohåndtering
- Endringsstyring (kapittel 5.4.2), jfr. konfigurasjonskontroll og konfigurasjonsendringer

1.5 Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk

Lov- og forskriftsbestemmelser:

- Personvernforordningen artikkel 5, 24, 28 og 32 (Prinsipper, ansvar og sikker behandling av personopplysninger)
- Pasientjournalloven §§ 22 og 23 (Informasjonssikkerhet og internkontroll)
- Helseregisterloven §§ 17, 18, 21 og 22 (Behandling av helseopplysninger)
- Helsepersonelloven § 17 (Taushetsplikt. Referert til fra helseregisterloven)
- Forvaltningsloven § 13 (Taushetsplikt)
- e-IDAS-forordningen (Krav til elektroniske tillitstjenester)

Standarder og andre rammeverk:

- ISO/IEC 27001 og 27002
- NSMs grunnprinsipper for IKT-sikkerhet 2.0[6]
- Centre for Internet Security (CIS) Controls v.8[7]

1.6 Avgrensninger

Virksomheter som etablerer informasjonssystemer som behandler helse- og personopplysninger, skal legge alle relevante krav i Normen til grunn for å etablere og ivareta tilstrekkelige sikringstiltak. Tiltakene skal bidra til akseptabel risiko i og i tilknytning til informasjonssystemene. Relevante krav finnes i følgende kapitler i Normen:

- Kapittel 2: Ledelse og ansvar
- Kapittel 3: Risikostyring
- Kapittel 4: Grunnleggende om behandling av helse- og personopplysninger
- Kapittel 5: Informasjonssikkerhet.

Teknisk løsning for fjernaksess vil kunne anses som et eget IKT-system, avhengig av valgt løsning. Fjernaksessløsningen må uansett anses å utgjøre en mindre del av en større helhet i et informasjonssystem[8] hvor helse- og personopplysninger behandles.

Veilederen omhandler *ikke* informasjonssystem(er) i sin helhet eller virksomhetens helhetlige styringssystem for informasjonssikkerhet og personvern. Kun utstyr, infrastruktur, løsninger eller systemer som enten introduseres og utgjør del av fjernaksessløsningen, eller påvirkes direkte[9] av fjernaksessløsningen, som f.eks. fagsystemer fjernaksessløsningen gir tilgang til

[6] NSMs grunnprinsipper for IKT-sikkerhet omtaler normalt informasjon (som verdi) i generell form. Leser må ved bruk av rammeverket forstå *informasjon* som helse- og personopplysninger.
[7] Rammeverk for operativ IKT-sikkerhet, som er offentlig tilgjengelig, men krever brukerregistrering.
[8] Definisjonen av *informasjonssystem* i vedlegg 6.2 til Normen. Det presiseres at informasjonssystemer kan bestå av ett eller flere IKT-systemer, men er ikke avgrenset til digitale enheter og grensesnitt, og kan i prinsippet være helt manuelt.
[9] Veilederens kapittel 3 Risikostyring ved fjernaksess (og involvering av gjeldende system- og risikoeiere)

(for databehandling[10] eller vedlikehold), er dekket av veilederen. Stedlige (on-site) IT-støttetjenester (som ikke krever bruk av fjernaksessløsning) dekkes ikke[11]. Veilederen avgrenses derfor til kontekstspesifikke krav og anbefalinger til fjernaksess. Dette inkluderer funksjonalitet og tjenester som fjernaksessløsningen introduserer i informasjonssystem(er), og som er av teknologisk art, men også tilhørende menneskelige og organisatoriske aspekter i behandlingen av helse- og personopplysninger. Veilederen bør derfor leses sammen med Normens vedlegg 6.1 «Oversikt over Normens krav»[12], som gir en samlet oversikt over Normens krav. Vedlegget utdyper blant annet sikkerhetskrav til informasjonssystemer som fjernaksess og tjenesten som ytes, gir tilgang til eller utgjør en del av. Temaer som utdypes i annet veiledningsmateriell eller rammeverk, blir i veilederen henvist[13] til og ikke beskrevet i detalj.

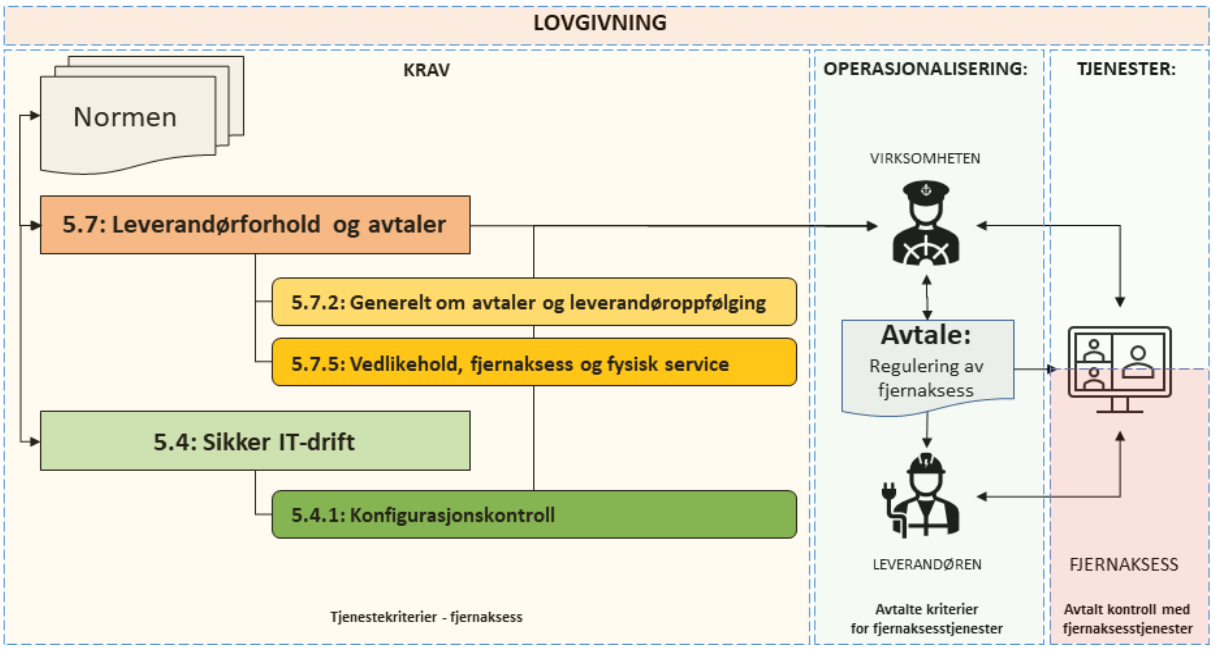
[10] Av helse- og personopplysninger
[11] Med mindre tildelt adgang eller tilgang kan direkte påvirke sikkerhet og risiko i fjernaksessløsningen
[12] Oversikt over normens krav og mapping mellom ISO, CSA og Normen
[13] Se f.eks. henvisninger til Veileder for tilgang til helse- og personopplysninger (basert på Normen) eller NSMs grunnprinsipper for IKT-sikkerhet (der grunnprinsipper eller tiltak kan bidra til å oppfylle krav i Normen)

2 Ansvar for fjernaksess

2.1 Ansvarsfordeling mellom virksomheten og leverandøren

Virksomheter som etablerer informasjonssystemer som behandler helse- og personopplysninger, skal legge alle relevante krav i Normen til grunn for å etablere og ivareta tilstrekkelige sikringstiltak. Ansvar for å sikre fjernaksess iht. Normen deles mellom virksomheten og leverandøren. Virksomheten har ansvaret for at krav til informasjonssikkerhet og personvern følges gjennom hele leveransekjeden. Der leverandøren er databehandler, skal den tilrettelegge for at virksomheten (dataansvarlig) som tar i bruk leverandørens produkter og tjenester, kan oppfylle krav i lovverk og Normen.

Figur 1 nedenfor viser en forenklet skisse over krav i Normen, som eksplisitt omtaler og er styrende for fjernaksess mellom virksomhet og leverandør. Figuren viser samtidig til virksomhetens ansvar for å operasjonalisere kravene ved valg av leverandør samt etablering og oppfølging av avtalevilkår.



Figur 1: Oppfyllelse av krav gjennom avtalte vilkår for leverandør og tjenester

Figuren gir et oversiktsbilde, men viser ikke til alle relevante sammenhenger mellom krav i Normen som påvirker tjenesteleveranser for fjernaksess, og oppfølging av tjenestene mellom virksomhet og leverandør. I de neste kapitlene utdypes anbefalt tilnærming til etterlevelse av kravene.

I *Vedlegg for veileder for fjernaksess* gis en sjekkliste med oppgaver, som fordeles mellom virksomheten og leverandøren. Oppgavene baseres på og bør ses i sammenheng med beskrevne krav og anbefalinger i kapitlene kravene og anbefalingene peker til i veilederen.

Vedlegget kan utgjøre et startpunkt[14] for nødvendige avtalekrav til fjernaksesstjenester. Det er viktig å påpeke at fordeling av ansvar og oppgaver (i vedlegget) er veiledende, og det kan være behov eller ønskelig å delegere oppgaver annerledes. Dette kan avhenge av ulike løsningsscenarioer[15], der f.eks. eierskap og drift av løsningen i sin helhet ivaretas av enten leverandøren eller virksomheten selv, eller at ansvaret er delt. Virksomheten er, uavhengig av oppgavefordeling, ansvarlig for informasjonssikkerhet og personvern, og må sørge for at avtalen(e) er dekkende for å ivareta gjeldende krav og behov.

2.2 Løsningsscenarioer

Ved etablering av fjernaksess til helse- og personopplysninger vil ulike løsninger være aktuelle. Dette avhenger av den enkelte virksomhets behov og hvorvidt løsninger som tilbys (av ulike leverandører) er relevante for formålet.

Løsningsscenarioer vil hovedsakelig være avgrenset til følgende valg:

1. Fjernaksessløsning driftes hos leverandøren (i sin helhet)
2. Fjernaksessløsning driftes hos leverandøren og virksomheten (i to delsystemer)
3. Fjernaksessløsning driftes hos virksomheten av leverandøren

Leverandørene har normalt sine egne løsninger for fjernaksess, noe som også gjelder felles nasjonal løsning gitt ved Norsk Helsenett (NHN). Et annet eksempel som kan være aktuelt, er:

4. Både fjernaksessløsning og driftsmiljøet (som det gis fjernaksess til) eies og driftes av leverandøren

Da alternativ 4 omhandler både fjernaksess i seg selv og et helt informasjonssystem og driftsmiljø, dekkes ikke alle relevante temaer innen sikkerhet av denne veilederen alene. For en slik løsning gjelder ytterligere krav i Normen og anbefalinger i *Veileder i bruk av skytjenester til behandling av helse- og personopplysninger*. Det gis i kapittel 8 eksempler på anbefalte løsninger, men andre løsninger kan også være aktuelle.

Selv om virksomheten har overordnet ansvar for informasjonssikkerhet og personvern, vil valgt løsning påvirke hvilket ansvar partene har for utøvelsen av oppgaver og rutiner som er nødvendige for å etterleve Normens krav. Det er særskilt viktig at virksomheten sørger for at de krav virksomheten må etterleve, men som ivaretas i daglig drift av leverandøren, må dekkes gjennom fastsatte avtalevilkår med leverandøren. Det presiseres at behov for å avtalefeste tiltak for å etterleve krav, øker proporsjonalt med andelen av systemer og infrastruktur som eies av og driftes hos leverandøren.

2.3 Tjenesteutsetting

Bestillerkompetanse og oppfølging av leverandør

Fjernaksess mellom virksomhet og leverandør vil normalt innebære en tjenesteutsetting av IKT-funksjoner eller -tjenester, som Normen stiller minimumskrav[16] til. Følgende tiltak i NSMs grunnprinsipper for IKT-sikkerhet, bør brukes ved tjenesteutsettelse av IKT-funksjoner eller

[14] Listen bør vurderes i det enkelte tilfelle, for å sikre at gjeldende krav i Normen etterleves
[15] Veilederens kapittel 2.2 Løsningsscenarioer
[16] Normen 6.0 kapittel 5.7.3 spesifikt og 3.2 generelt

tjenester som bidrar til fjernaksess, som sådan, eller utøvelsen av tjenester forbundet med fjernaksess:

- 2.1.9 *Ta ansvar for sikkerhet også ved tjenesteutsetting*
- 2.1.10 *Undersøk sikkerheten hos tjenesteleverandør ved tjenesteutsetting*

Tiltakene gjelder bl.a. bestillerkompetanse, som er avgjørende for tilstrekkelig informasjonssikkerhet og personvern, og kan brukes for å oppfylle Normens krav[17] til oppfølging av leverandøren. Når tiltakene utføres, bør virksomheten se til at aktivitetene (spesielt tiltak 2.1.9 c) og d)) tar innover seg Normens spesifikke krav om tjenesteutsetting[18] og skytjenester[19].

2.4 Avtaler og rutiner

Avtaler

Ved fjernaksess skal skriftlig avtale inngås mellom virksomheten og leverandøren.

Når virksomheten inngår avtale med leverandøren, så må den sikre at avtalen[20] i tilstrekkelig grad regulerer partenes plikter og rettigheter. Hvilke av Normens krav som gjennom avtale gjelder for leverandøren er avhengig av hva slags type leveranse det er snakk om, for eksempel:

- Databehandling (i form av f.eks. driftstjenester eller skytjenester)
- Vedlikehold (f.eks. ved fysisk service og fjernaksess)
- Leveranse av løsninger og systemer

Offentlige virksomheter bør normalt bruke statens standardavtaler som maler for å oppnå formålet. Virksomheten skal påse at avtalen mellom virksomheten og leverandøren ivaretar krav i Normen, og at hvilke krav det er kommer frem i et eget bilag. I kapittel 10.1 er det gitt eksempel på avtaletekst, som kan benyttes som bilag til statens standardavtaler.

Ved utforming av avtaler om fjernaksess bør virksomheten benytte seg av bistand fra personell med juridisk kompetanse, og ikke minst fagkompetanse innen anskaffelser, personvern, informasjonssikkerhet samt IT og fagsystem.

Rutiner

Det skal utarbeides dokumenterte rutinebeskrivelser[21] for daglig praksis og enkeltoppgaver knyttet til fjernaksessløsningen. Dette kan f.eks. være rutiner for opplæring, bruk og drift av fjernaksessløsningen, autentisering, autorisasjon, logging, sikkerhetsrevisjon, og risikovurderinger av sikringstiltak, avvik og hvordan de håndteres m.fl. Rutinene må tilpasses og være dekkende det enkelte tilfelle og løsning. Personell som benytter eller utfører oppgaver i eller i sammenheng med fjernaksessløsningen skal inneha nødvendig kompetanse og opplæring[22] til å utøve sin funksjon. Dette gjelder både leverandøren og virksomheten.

[17] Normen 6.0 kapittel 5.7.7
[18] Normen 6.0 kapittel 5.7.3
[19] Normen 6.0 kapittel 5.7.9
[20] Normen 6.0 kapittel 5.7.2
[21] Normen 6.0 kapittel 2.4 (sjette avsnitt). Se i sammenheng med alle aktuelle sikringstiltak.
[22] Normen 6.0 kapittel 5.1.2

Se kapittel 10.2 og 10.3 for eksempler på rutiner som bør etableres. Virksomheten bør vurdere behovet for ytterligere rutinebeskrivelser, avhengig av tjenestene som avtalen er ment å regulere, sett opp imot Normens krav til rutiner for ulike[23] forhold.

2.5 Databehandler

Ved fjernaksess til helse- og personopplysninger mellom virksomhet og leverandør, er leverandøren databehandler. Når dataansvarlig benytter databehandlere, så må partene inngå databehandleravtale. Personvernforordningen artikkel 28 nr. 3 stiller krav til avtalens innhold, som blant annet skal bestå av instrukser for databehandler og krav til sikkerheten ved databehandlers behandling av personopplysninger.

Dersom det eksempelvis foreligger et faglig behov for at leverandøren flytter helse- og personopplysninger til leverandørens sikre nettverksområder, eller at leverandøren av annen grunn behandler opplysningene i eget driftsmiljø, skal dette uføres iht. en databehandleravtale. Databehandleravtalen skal være skriftlig[24], og kan fremkomme enten som en frittstående avtale mellom partene eller som en integrert del av annet avtaleverk[25]. Ytterligere krav til databehandler og databehandleravtalen beskrives[26] i Normen, og presiseres i Faktaark (FA) 10 *Bruk av databehandler.*

Dersom databehandler behandler helse- og personopplysninger fra flere virksomheter, skal databehandler ved hjelp av tekniske tiltak ivareta at det er etablert skiller mellom virksomhetene i henhold til gjennomført risikovurdering.

Overføring av opplysninger til tredjeland

Tjenesteutsettelse som innebærer overføring av opplysninger til land som er tredjeland etter personvernforordningen (land utenfor EU og EØS-området) skal reguleres[27] i avtale om fjernaksess. Dataansvarlig må være oppmerksom på at både å oppbevare personopplysninger i tredjeland og å gi en aktør etablert i et tredjeland tilgang til opplysningene, vil regnes som overføringer til tredjeland. Et eksempel som *kan* utgjøre en slik overføring, er bruk av en underleverandører som har kontorer i tredjeland som sikrer døgnåpne IT-støttetjenester.

2.6 Krav til leverandørers taushetsplikt

Leverandøren skal, som del av tjenesten for fjernaksess, forsikre at de har rutiner som pålegger alle medarbeidere taushetsplikt om helse- og personopplysninger, og annen taushetsbelagt informasjon. Leverandøren kan selv administrere og oppbevare taushetserklæringer for eget personell, men virksomheten skal sikres innsyn ved behov. Eksempler på rutiner som bør tas frem er gitt i kapittel 10.2.

[23] Se f.eks. Normen 6.0 kapittel 5.4.2, 5.4.4, 5.4.5, 5.4.6, 5.5.5, m.fl.
[24] Normen 6.0 kapittel 5.7.4.2
[25] Veilederens kapittel 2.4
[26] Normen 6.0 kapittel 5.7.4
[27] Normen 6.0 kapittel 5.7.8

3 Risikostyring ved fjernaksess

3.1 Generelt

Risikostyring er koordinerte aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko. Det omfatter å få oversikt over informasjon og teknologi i virksomheten, identifisere trusler og mulige uønskede hendelser for både virksomheten og de registrerte, analysere risikoen og etablere tiltak for å opprettholde fastsatt nivå for akseptabel risiko.[28]

Virksomheten skal iht. krav i Normen[29] etablere risikostyring for å vurdere og håndtere risiko i virksomhetens informasjonssystemer, som også omfatter fjernaksessløsningen med gjeldende integrasjon(er). Kravstilling og nødvendige sikkerhetstiltak ved bruk av leverandører og løsninger skal bygge på en dekkende risikovurdering som forankres i virksomhetens styringssystem. Risikovurderingen skal *alltid* omfatte scenarioer som omfatter leverandørens[30] autoriserte og ev. uautoriserte tilgang til helse- og personopplysninger og annen taushetsbelagt informasjon. Nærmere detaljer om risikostyring gis i Veileder om risikostyring i informasjonssikkerhet og personvern

3.2 Risikovurdering før fjernaksess etableres

Valg av løsning og tjenester for fjernaksess skal risikovurderes og dokumenteres[31], og skal inkludere alle sikkerhetstiltak[32] som påvirker[33] risiko i informasjonssystemer ved fjernaksess. Dette innebærer å risikovurdere sikkerhetstiltak, som delelementer i en helhet, og inkluderer tiltak under f.eks. tilgangsstyring[34], kommunikasjonssikkerhet[35], sikker IT-drift[36] m.fl. (som omtales videre i veilederen). Risikovurdering skal være gjennomført før leverandøren gis tilgang til fjernaksess, og skal legge virksomhetens fastsatte akseptable risiko til grunn.

Risikofaktorer og aktuelle scenarioer varierer fra løsning til løsning. Risikovurderingen er grunnlag for å vurdere løsningens sikkerhetsmessige tilstrekkelighet og eventuelle behov for ytterligere sikkerhetstiltak (som f.eks. økt behov for logging og analyse av logger).

Aktuelle risikofaktorer ved fjernaksess er eksempelvis knyttet til ivaretakelse av tjenstlig behov og kontroll med tilganger til løsningen, samt hvilke tjenester som ytes og tillates. Andre eksempler er løsningens kapasitet til å begrense mulighet for flytting av filer, «klipp og lim» av tekst, skjermbilder eller på annen måte kopiere innhold. Også hvorvidt fjernaksessløsningen eller systemer og infrastruktur det gis fjernaksess til er sikkerhetsoppdatert, og kapasitet og evne til logging og analyse av logger, er relevante risikofaktorer.

---

[28] Normen 6.0 kapittel 3
[29] Normen 6.0 kapittel 3
[30] Normen 6.0 kapittel 5.7.7
[31] Normen 6.0 kapittel 3.4
[32] Normen 6.0 kapittel 5 første ledd
[33] Se krav til risikovurdering av alle sikkerhetstiltak, som f.eks. tilgang, logging, konfigurasjonsstyring m.fl. som omtales videre i denne veilederen (og i Normen)
[34] Veilederens kapittel 4
[35] Veilederens kapittel 5
[36] Veilederens kapittel 6

Det er viktig at risiko- og systemeiere for informasjonssystem(er) som påvirkes[37] blir involvert[38] i arbeidet med risikovurderinger og identifisering av aktuelle tiltak. Dette for å tilrettelegge for at integrasjon med informasjonssystem(er) sikres uten å skape funksjonelle utfordringer, at fastsatt nivå for akseptabel risiko ivaretas, og at interessenter kan etterleve krav til sikring av sine verdier[39], selv om fjernaksess introduserer nye risikofaktorer. Ved behov skal tiltak for å håndtere risiko iht. fastsatt nivå for akseptabel risiko, gjennomføres.

Risikovurdering i drift av fjernaksessløsning

Normen fastsetter at risikovurdering bør oppdateres i henhold til trusselbildet. I tillegg skal virksomhetens ledelse jevnlig gjennomføre risikovurderinger som ledd i sitt arbeid med å kontrollere informasjonssikkerheten[40]. Det betyr at ved endringer i eller avdekking av (nye) sårbarheter i fjernaksessløsningen bør risikoen og tiltak revurderes.

[37] Dvs. de som er risiko- og systemeiere for systemer og infrastruktur det gis fjernaksess til.
[38] Andre interessenter kan også være relevante, og bør vurderes for det enkelte tilfelle.
[39] Avgrenses ikke til helse- og personopplysninger, men sees i større sammenheng, der verdier både er informasjonsverdier samt systemer og tjenester som kan være kritiske for liv og helse, der helhetlig sikring av informasjonssystemer, og her omtalte fjernaksessløsninger, kan påvirke verdiene.
[40] Normen 6.0 kapittel 3.4

4 Tilgangsstyring ved fjernaksess

4.1 Generelt

Tilgangsstyring skal etableres for alle informasjonssystemer[41], herunder løsninger og IKT-utstyr i bruk for fjernaksess. Krav til tilgangsstyring dekkes i Normen[42] og *Veileder for tilgang til helse- og personopplysninger*.

Den følgende beskrivelsen av spesifikke krav og anbefalinger til tilgangsstyring ved fjernaksess bør sees i sammenheng med overnevnte krav til og veiledningsmateriell for tilgang. I tillegg anbefales[43] det å legge følgende grunnprinsipper til grunn for å strukturert styre og kontrollere at tjenstlig behov ivaretas i fjernaksessløsningen (se spesielt i sammenheng med kapittel 4.2 og 4.4 nedenfor):

Eksempler fra NSM på grunnprinsipper (med underliggende tiltak) som bør vurderes for tilgangsstyring:

- ***1.3*: Kartlegg brukere og behov for tilgang**
- ***2.6*: Ha kontroll på identiteter og tilganger**

4.2 Autorisering ved fjernaksess

Virksomheten er ansvarlig for at autorisasjoner tildeles, administreres og kontrolleres. Kun personell med tjenstlig behov skal autoriseres for bruk av fjernaksess til behandling av helse- og personopplysninger, eller andre[44] tilganger i sammenheng med fjernaksessløsningen. All tildelilng av autorisasjon skal registreres i et autorisasjonsregister[45].

4.3 Autentisering ved fjernaksess

Ved oppkobling[46] for fjernaksess til systemer med helse- og personopplysninger skal det brukes sikkerhetsnivå høyt, som krever sikker autentiseringsløsning[47]. Det er mulig[48] å velge en annen type autentiseringsløsning, dersom risikovurdering (av autentiseringsløsningen) er gjennomført og kan vise at valgt autentiseringsløsning innehar tilstrekkelig sikkerhet.

[41] Normen 6.0 kapittel 5.2
[42] Normen 6.0 kapittel 5.2.
[43] Se anbefalte grunnprinsipper og tiltak i sammenheng med ordlyd i Normen og Veileder for tilgang til helse- og personopplysninger, slik at tiltak, aktiviteter og dokumenterte leveranser gjennomføres og tilpasses for å etterleve Normens krav og vedtatt praksis for tilgangsstyring.
[44] F.eks. drift- og administrasjon av fjernaksessløsningen, som sådan, eller tjenester som oppdatering og vedlikehold av informasjonssystemet fjernaksessløsningen integreres med
[45] Normen 6.0 kapittel 5.2.1.1.
[46] I likhet med tilganger fra hjemmekontor eller mobilt utstyr eller trådløse nettverk
[47] Veileder for tilgang til helse- og personopplysninger, for nærmere beskrivelse av krav til sikkerhetsnivå høyt og sikker autentiseringsløsning
[48] Definisjon av *sikker autentiseringsløsning* i vedlegg 6.2 til Normen 6.0

4.4 Kontroll av tilganger til fjernaksess

Det skal jevnlig[49] gjennomføres kontroll[50] av tilganger i fjernaksessløsningen. Dette innebærer både gjennomføring av sikkerhetsrevisjoner, men også (mer hyppige) periodiske gjennomganger av tilganger som finnes i fjernaksessløsningen, for å validere tilgangene.

Kontroll av tilganger til fjernaksess utgjør en viktig del av jevnlige sikkerhetsrevisjoner (jfr. kapittel 6.4), som minimum skal gjennomføres årlig. Kontroll av tilganger til fjernaksess bør følge prinsippene i tiltak 2.6.1 e) i NSMs grunnprinsipper for IKT-sikkerhet. Periodisk gjennomgang av tilganger bør dekkes av en rutinebeskrivelse, og anbefales gjennomført minimum kvartalsvis[51] og gjerne oftere. Nærmere anbefalinger om kontroll av tilganger er spesifisert i *Veileder for tilgang til helse- og personopplysninger*.

[49] Minimum årlig, men dette kan være oftere og påvirkes av flere faktorer
[50] Normen 6.0 kapittel 5.2.3
[51] CIS Controls tiltak 5.1 *Establish and maintain an inventory of Accounts* (siste setning)

5 Kommunikasjonssikkerhet

5.1 Generelt

Virksomheten skal sørge for at leverandørens utstyr som benyttes ved hjelp av *kommunikasjonsnett* ikke har ondsinnet programvare[52]. Samtidig bør god praksis for kommunikasjonssikkerhet legges til grunn for kommunikasjonsnett. Dette for å unngå uautorisert tilgang til helse- og personopplysninger i transitt eller avlytting av kommunikasjon som kan gi mulighet for andre uautoriserte tilganger til eller målrettede angrep mot fjernaksessløsning eller integrerte informasjonssystemer. Se veilederens kapitler sammen med Normens krav[53] til kommunikasjonssikkerhet, og FA 24 *Kommunikasjon over åpne nett*.

5.2 Styring av nettverkssikkerhet

Virksomheten skal tydelig definere[54] hvilke krav som gjelder for nettverkssikkerheten som angår fjernaksessløsningen, og tiltak skal være basert på en risikovurdering. Følgende grunnprinsipper[55] anbefales lagt til grunn for nettverkssikkerhet i fjernaksessløsningen:

Eksempler på grunnprinsipper (med underliggende tiltak) som bør vurderes for nettverkssikkerhet:

- **2.2*: Etabler en sikker IKT-arkitektur***
- **2.4: *Beskytt virksomhetens nettverk***
- **2.5: *Kontroller dataflyt***

Grunnprinsippene gir viktige beste praksis tiltak for nettverkssikkerhet, som kan benyttes som underlag for risikovurdering og valg av tiltak. Grunnprinsipp 2.2[56] består av tiltak som strekker seg utover nettverkssikkerhet, men bør vurderes for fjernaksessløsningen i sin helhet. Se også grunnprinsipp 2.3[57] (som dekkes av veilederens kapittel 6.1 om konfigurasjonskontroll).

5.3 Tilkoblinger til eksterne nett

Avsnittet beskriver krav til teknisk løsning ved oppkobling av *fjernaksess,* gjennom *helsenettet* eller utenfor. Se kravene i sammenheng med løsningseksempler i veilederens kapittel 8.

Virksomheten skal påse at fjernaksess etableres med tekniske tiltak som ivaretar at kun eksplisitt angitt tillatt trafikk[58] kan passere utenfra og inn eller ut, og at annen trafikk stoppes. Tiltak i grunnprinsipp[59] 2.4 *Beskytt virksomhetens nettverk* og 2.5 *Kontroller dataflyt*[60] anbefales lagt til grunn for å oppfylle formålet. Grunnprinsippene består av flere tiltak som bør vurderes for å etablere og ivareta fastsatt nivå for akseptabel risiko (i det enkelte tilfelle).

---

[52] Normen 6.0 kapittel 5.7.5
[53] Normen 6.0 kapittel 5.5
[54] Normen 6.0 kapittel 5.5.1
[55] NSMs grunnprinsipper for IKT-sikkerhet
[56] Etabler en sikker IKT-arkitektur
[57] Ivareta en sikker konfigurasjon
[58] Normen 6.0 kapittel 5.5.2
[59] NSMs grunnprinsipper for IKT-sikkerhet
[60] Jfr. avhengighet til grunnprinsipp 2.2 Etabler en sikker IKT-arkitektur

Normen presiserer at tiltaket skal bestå av minst to uavhengige tekniske tiltak for å unngå uautorisert tilgang til, endring av og/eller sletting av helse- og personopplysninger.

Eksempler på tiltak (fra NSMs grunnprinsipper for IKT-sikkerhet) som bør etableres:

- ***2.4.1: Etabler tilgangskontroll på flest mulig nettverksporter***
- ***2.5.1: Styr datatrafikk mellom nettverkssoner***
- ***2.5.8: Styr all trafikk til og fra mobile klienter via virksomhetens nettverk***

I eksemplene gis spesifikke tiltak som kan bidra til å begrense og filtrere nettverkstrafikk, nettverkstjenester og enheter som gis tilganger til fjernaksessløsningen. Det bidrar til at enheter ikke kobles til direkte fra internett, men omfattes av sikkerhetsfunksjonalitet i teknisk løsning. Logging[61] bør etableres og analyseres for å kontrollere at regler ikke brytes.

5.4 Terminering av fjernaksess

Dette kapitlet gir presiseringer til nettverkssikkerhetsprinsipper i kapittel 5.2 og 5.3, som bør ses i sammenheng med tiltak i NSMs grunnprinsipper for IKT-sikkerhet, spesielt tiltak 2.2.3, 2.5.1, 2.5.2, 2.5.7 og 2.5.8.

Infrastruktur og utstyr som benyttes til å yte eller konsumere fjernaksesstjenester som del av fjernaksessløsningen, kan, i likhet med annet IKT-utstyr, bli kompromittert[62]. Dersom fjernaksessløsningen eller deler av denne kompromitteres, medfører dette risiko for at også infrastruktur, systemer og opplysninger det gis fjernaksess til kan bli kompromittert. Potensialet for kompromittering øker avhengig av utstyrets eksponering[63] mot usikre[64] nettverk og tjenester. Av denne grunn bør fjernaksessløsninger som reduserer utstyr og infrastrukturs eksponering mot usikre nettverk og tjenester foretrekkes. Dette betyr eksempelvis at dersom VPN planlegges brukt bør site-to-site[65] VPN-løsninger foretrekkes foran VPN-løsninger som etablerer fjernaksessforbindelser utenfor[66] sikre nettverkssoner og kontroll (som ved hjemmekontor e.l.).

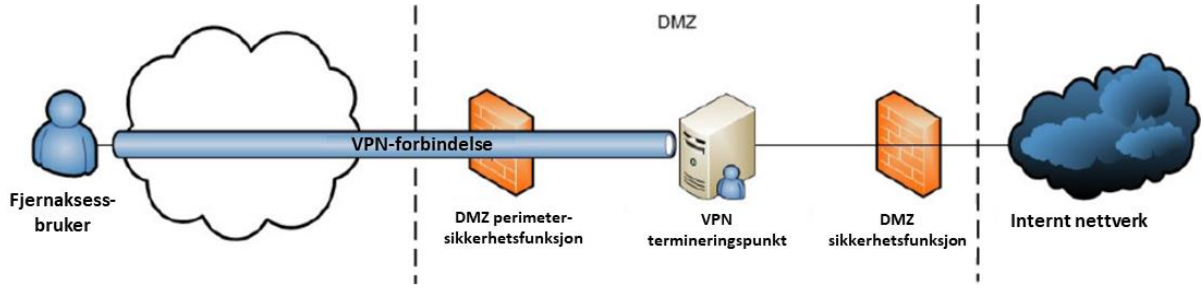
Ved soneinndeling av nettverk bør ytre[67] terminering av fjernaksess skje gjennom en brannmur og i en egen DMZ-sone[68]. Samtidig bør datainnholdet i nettverkstrafikken, som går gjennom DMZ-sonen, kunne (systemteknisk) inspiseres ukryptert. Det vil redusere muligheten for at krypterte (ukjente) data inneholder skadevare eller andre angrepsvektorer uten at det oppdages, stoppes eller logges. Dette er viktig for å øke kapasitet og evne til å identifisere, logge og håndtere uønskede hendelser, før nettverkstrafikk (og tilhørende datainnhold) går inn eller ut fra internt nettverk. Avhengig av kritikaliteten til infrastruktur,

[61] Veilederens kapittel 6.3
[62] Se f.eks. veilederens kapittel 6.2
[63] NSMs grunnprinsipper for IKT-sikkerhet, tiltak 2.2.3 og 2.3.6 ii)
[64] Internett og/eller usikre interne nettverk hvor god praksis for nettverkssikkerhet ikke er etablert
[65] Se løsningseksempel i kapittel 8.4 (i eksempler på tekniske løsninger).
[66] Se løsningseksempel i kapittel 8.2 (i eksempler på tekniske løsninger).
[67] Dvs. i ytre nettverksperimeter/-sone, som er direkte eksponert for internett og mest eksponert for eksterne trusler
[68] Veileder i Personvern og informasjonssikkerhet – medisinsk utstyr

systemer og opplysninger det gis fjernaksess til, bør det vurderes om trafikk bør valideres[69] i DMZ-sonen.

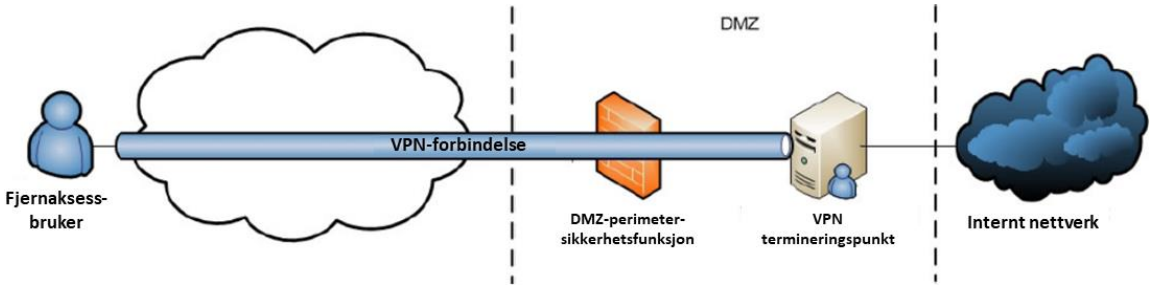
Trafikk over fjernaksessforbindelser[70] bør behandles som usikker og potensielt skadelig, som annen ekstern nettverkstrafikk (med tilhørende datainnhold). Kryptert trafikk[71] bør dekrypteres før den inspiseres (ukryptert) og logges i DMZ (som vist i figur 2) før den videresendes. Ingen nettverkstrafikk bør gå kryptert gjennom alle sikkerhetsfunksjoner som skal beskytte intern infrastruktur, systemer og opplysninger det gis fjernaksess til uten at det er gjennomført en risikovurdering. Dette er avgjørende for å hindre at (tilsynelatende) autorisert trafikk fra autorisert/hvitelistet utstyr kan anvendes til angrep, spredning av skadevare eller på annen måte å kompromittere infrastruktur, systemer og opplysninger det gis fjernaksess til.

Figur 2 viser en forenklet skisse av anbefalt praksis i en løsning hvor ytre terminering av fjernaksess skjer i en DMZ-sone. I løsningen er god IKT-sikkerhet ivaretatt og risiko redusert med etablerte kapasiteter som kan inspisere og logge datainnhold (som passerer kryptert gjennom perimeter-brannmur) ukryptert på innsiden av VPN-termineringspunktet.



Figur 2: Anbefalt etablering av DMZ-sone med kontroll av og sporbarhet med inn- og utgående trafikk og data

Figur 3 viser en forenklet skisse over en løsning med mangelfull kapasitet til å inspisere og logge datainnhold (som passerer gjennom en DMZ-sone eller på annen måte inn i virksomhetens interne nettverk). Løsningen medfører økt risiko for at informasjonssikkerhetsbrudd ved fjernaksess ikke oppdages og håndteres hensiktsmessig.



Figur 3: DMZ-sone med liten grad av kontroll og sporbarhet med inn- og utgående trafikk og data

[69] Med validering menes at inn- og/eller utgående trafikk og data systemteknisk godkjennes (basert på fingranulerte regelsett) på t.o.m. applikasjonslaget (lag 7), ved bruk av applikasjonsbrannmur e.l. Jfr. NSMs grunnprinsipper for IKT-sikkerhet, tiltak 2.5.6 b).

[70] Dette gjelder uavhengig av løsning (selv om enkelte løsninger reduserer risiko), da utstyr (og spesielt på klientsiden) normalt er eksponert for trusler, tidvise sårbarheter og risiko.

[71] Dette uavhengig av fjernaksessløsning og teknologibruk.

Merk at VPN-løsninger i figur 2 og 3 kun benyttes som eksempler. Prinsippene i figur 2 bør legges til grunn uavhengig av teknisk løsning og teknologivalg.

Dekryptering av trafikk og (systemteknisk) inspeksjon i en DMZ-sone (som vist i figur 2) er normalt uproblematisk om infrastruktur det gis fjernaksess til, er fysisk plassert i adgangskontrollerte rom. For eksempel dersom fjernaksess til serverinfrastruktur oppfyller formålet. Det kan imidlertid være tilfeller der figur 3 eller annen løsning er nødvendig. Et eksempel er om formålet krever direktetilgang til medisinsk utstyr (dvs. at servertilgang ikke dekker formålet), og at gjeldende utstyr ikke kan plasseres på et adgangskontrollert rom som f.eks. et serverrom. Om dette er tilfelle og helse- og personopplysninger blir behandlet, kan dekryptering av nettverkstrafikk i en DMZ-sone medføre at opplysninger sendes ukryptert på internt nettverk eller at formålet (f.eks. fjernsupport direkte på medisinsk utstyr) ikke oppfylles funksjonelt.

Dersom omstendighetene, som f.eks. fysisk plassering av infrastruktur og utstyr, teknisk løsning, formål og teknologier, gjør at anbefalt god praksis for IKT-sikkerhet (i figur 2) skaper utfordringer for personvern (pga. ukryptert trafikk på internt nettverk) må risiko forbundet med dette vurderes og håndteres. Tilsvarende må risiko forbundet med mangelfull ivaretakelse av god praksis for IKT-sikkerhet i fjernaksessløsning vurderes og håndteres. Omstendighetene kan medføre at personverninteresser og informasjonssikkerhet av andre grunner enn personvern, trekker i ulike retninger og avveies mot hverandre. Økt risiko for informasjonssikkerheten påvirker ofte også risikoen for personvernet.

6 Sikker IT-drift

6.1 Konfigurasjonskontroll

Virksomheten skal ha konfigurasjonskontroll[72] [73] med alt eget utstyr og programvare som utgjør del av fjernaksessløsningen. I forbindelse med fjernaksess kan leverandøren utøve oppgaver som databehandler eller vedlikeholde og oppdatere løsninger (fjernadministrasjon). Ved fjernaksess mellom virksomhet og leverandør er leverandøren databehandler. Avhengig av tjenestene som ytes, skal tjenestene reguleres[74] gjennom avtale.

Forutsetninger for konfigurasjonskontroll

Virksomheten skal etablere og ivareta konfigurasjonskontroll (iht. Normens krav) på egen IKT-infrastruktur og utstyr som utgjør del av fjernaksessløsningen og driftes internt (on-site) hos virksomheten. Samtidig skal virksomheten gjennom avtalefestede vilkår sikre at leverandøren etterlever krav til konfigurasjonskontroll av infrastruktur og utstyr som driftes eller håndteres (som del av fjernaksessløsningen) hos leverandøren. Virksomheten kan også, etter avtale, selv ivareta konfigurasjonskontroll av fjernaksessløsningen som driftes eller håndteres hos leverandøren, men det avhenger av løsningen og tjenestene som ytes. I tillegg bør virksomheten sørge for at det tas inn avtalevilkår som gir rett til sikkerhetsrevisjon av leverandørens utøvelse av konfigurasjonskontroll.

Krav til konfigurasjonskontroll i teknisk løsning

For å etablere konfigurasjonskontroll for fjernaksessløsningen, anbefales det å benytte grunnprinsipp[75] 2.3 *Ivareta en sikker konfigurasjon* for å etterleve kravene.

Følgende krav i Normen er ikke dekket av grunnprinsipp 2.3:

- Virksomheten skal sørge for at all dataflyt, datakommunikasjon og integrasjoner kartlegges og dokumenteres.
- Kun godkjent utstyr og programvare skal benyttes til behandling av helse- og personopplysninger. Virksomheten skal fastsette hvem som har godkjenningsmyndighet.
- Det skal benyttes separate miljøer for utvikling, test og produksjon slik at helse- og personopplysninger som benyttes ved ytelse av helsehjelp, ikke blir påvirket ved feil i utvikling og test.

Overnevnte krav som ikke dekkes av grunnprinsipp 2.3, kan oppfylles med følgende tiltak:

- ***1.1.6: Kartlegg informasjonsbehandling og dataflyt i virksomheten***
- ***1.2.2: Fastsett retningslinjer for godkjente enheter og programvare i virksomheten***
- ***2.1.6: Benytt separate miljøer for utvikling, test og produksjon***

Krav til konfigurasjonskontroll ved konfigurasjonsendringer

[72] Normen 6.0 kap. 5.4.1
[73] Med konfigurasjonskontroll menes her *styring* av konfigurasjonen (og ikke det å foreta kontroller i betydningen revisjon)
[74] Normen 6.0 kapittel 5.4.1 siste ledd
[75] NSMs grunnprinsipper for IKT-sikkerhet

Konfigurasjonsendringer skal håndteres strukturert før endringene driftsettes. Håndtering av konfigurasjonsendringer, dokumentering og involvering av personell anbefales oppfylt med grunnprinsipp *2.10 Integrer sikkerhet i prosess for endringshåndtering.* Det vises igjen til tiltak *2.1.6* for å etablere en implementasjon som sikrer mot uforutsette hendelser. Tiltak 2.10.1 d) og 2.10.2 skrives generelt, men kan oppfylle følgende spesifikke krav i Normen:

- Risikovurdering som viser at nivå for akseptabel risiko oppfylles
- Ny konfigurasjon er dokumentert
- Konfigurasjonsendringer er godkjent av virksomhetens leder eller den ledelsen bemyndiger

Ved etablering av tiltak i grunnprinsipp 2.10 skal virksomheten påse at det etableres rutiner for endringsstyring iht. Normen, som er tilpasset aktuell fjernaksess og fjernaksessløsning.

Fjernaksess skal *kun* gjøres over sikre[76] kanaler, som kan oppfylles med grunnprinsipp 2.3, herunder tiltak 2.3.6 *Utfør all konfigurasjon, installasjon og drift på en trygg måte*.

Virksomheten skal i tillegg påse at krav til styring og håndtering av tekniske sårbarheter[77], gjennom rutiner og operative tiltak, etableres og følges opp i fjernaksessløsningen. Styring og håndtering av IKT-utstyr og programvare (som del av kravet) kan oppfylles med grunnprinsipp 1.2, herunder tiltak 1.2.3 *Kartlegg enheter i bruk i virksomheten* og tiltak 1.2.4 *Kartlegg programvare i bruk i virksomheten*.

6.2 Forhindre ondsinnet programvare

Virksomheten skal gjennom avtale sørge for at leverandørens utstyr[78] som benyttes ved online oppkobling ved hjelp av kommunikasjonsnett, eller medbrakt utstyr som knyttes til virksomhetens fjernaksessløsning, ikke har ondsinnet programvare. Dette inkluderer virus eller lignende som kan medføre tyveri, endring eller sletting av helse- og personopplysninger eller som kan bidra til å skade systemer og infrastruktur som fjernaksessløsningen gir tilgang til. Se også FA 19 *Tiltak for å forhindre ondsinnet programvare*.

Flere tiltak kan påvirke mulighet for å oppdage og forhindre kjøring av og eventuell spredning av ondsinnet programvare. Følgende tiltak i NSMs grunnprinsipper for IKT-sikkerhet anbefales lagt til grunn for å etterleve Normens krav:

[76] Normen 6.0 kapittel 5.4.1 siste ledd
[77] Normen 6.0 kapittel 5.4.5
[78] Normen 6.0 kapittel 5.7.5

Tiltak som bør etableres for å forhindre ondsinnet programvare:

- ***2.1.2: Kjøp moderne og oppdatert maskin- og programvare***
- ***2.2.1: Etabler og vedlikehold en helhetlig sikkerhetsarkitektur*** *(v/ eksempelvis:)*
  - *d) Funksjonalitet for å ha kontroll over programvare (spesielt på klienter)*
  - *g) Nettverksenheter (svitsjer, rutere, aksesspunkter) og brannmurer*
  - *h) Mekanismer for å håndtere skadevare (antivirus)*
- ***2.4.4: Aktiver brannmur på alle klienter og servere***
- ***3.1.3: Benytt automatisert og sentralisert verktøy for å håndtere kjente trusler (som skadevare)***

Både virksomheten og leverandøren skal ha løsninger for å stanse og hindre overføring av ondsinnet programvare fra leverandøren eller virksomhetens nettverk og utstyr, som kontinuerlig oppdateres med nye sikkerhetsoppdateringer[79].

6.3 Logging

Med «logg» menes i Normen et logisk register der hendelser i informasjonssystemet (herunder fjernaksessløsningen) er nedtegnet. Normen stiller minimumskrav[80] til logging for å oppdage (forsøk på) brudd som kan bidra til kompromittering av løsningen som sådan eller av helse- og personopplysninger. Se også FA 15 *Logging og innsyn i logg*, som gir nærmere beskrivelser av krav til og rutiner for logging, analyse og behandling av logger i informasjonssystemer, som fjernaksessløsninger utgjør del av eller integreres med, samt krav til fjernaksess spesifikt.

Med hensyn til å etablere god systemteknisk praksis for logging og logganalyser i løsning for fjernaksess, anbefales det å se krav i Normen og FA 15 i sammenheng med grunnprinsipp[81] 3.2 *Etabler sikkerhetsovervåkning* og 3.3 *Analyser*[82] *data fra sikkerhetsovervåkning*.

6.4 Sikkerhetsrevisjon

Sikkerhetsrevisjon er avgjørende for å kontrollere om etablerte sikringstiltak, herunder teknologiske, organisatoriske og menneskelige, fungerer og ivaretar tilstrekkelig sikkerhet. Normens krav[83] til sikkerhetsrevisjon er også relevante for revisjon av fjernaksessløsningen, samt gjeldende rutiner, prosesser og organisering av sikkerhetsarbeidet, for å ivareta fastsatt nivå for akseptabel risiko.

Når sikkerhetsrevisjon skal gjennomføres bør det planlegges med både kontroll med sikkerhetsarbeid på fjernaksessløsningen (som sådan), klienter i bruk (til formålet) og servere (det gis tilgang til). Dette for en helhetlig revisjon og vurdering av aktuell risiko. Avtaler[84] bør tilrettelegge for sikkerhetsrevisjon av fjernaksessløsningen iht. Normens krav (bl.a. minimum årlig), samt gi mulighet for at sikkerhetsrevisjoner kan gjennomføres i regi[85] av virksomheten. Det er avgjørende at virksomheten avtalefester krav til innsyn, som f.eks.

---

[79] Se også NSMs grunnprinsipper for IKT-sikkerhet, tiltak 2.3.1
[80] Normen 6.0 kapittel 5.4.4
[81] NSMs grunnprinsipper for IKT-sikkerhet
[82] Legg merke til at grunnprinsipp 3.3 legger grunnprinsipp 2.5 Kontrollert dataflyt (basert på grunnprinsipp 2.2 Sikker IKT-arkitektur) til grunn for analyse opp imot normaltilstand i løsningen
[83] Normen 6.0 kapittel 5.4.6
[84] Veilederens kapittel 2.4
[85] Gjennomført av virksomheten selv eller valgt tredjepart

bør dekke behov for innsyn og tilgang til logger i fjernaksessløsningen der hele eller deler av løsningen driftes hos leverandøren. Logger er et viktig eksempel på noe som ikke uten videre utleveres uten avtale, og er spesielt viktig å stille krav om for driftsmiljøer (skytjenester) der andre kunders data behandles i samme applikasjon, plattform og/eller infrastruktur.

Ved sikkerhetsrevisjon av fjernaksessløsninger er det ofte behov for spesialkompetanse på området. Dersom virksomheten ikke besitter slik kompetanse selv, bør en kompetent leverandør av sikkerhetsrevisjoner gis i oppdrag å gjennomføre revisjonen.[86]

For fjernaksessløsningen skal eksisterende tilganger[87] til fjernaksess jevnlig kontrolleres. Samtidig bør andre sikringstiltak, som f.eks. tiltak under veilederens kapittel 5 *Kommunikasjonssikkerhet*, 6. *Sikker IT-drift* og 7. *Fysisk sikkerhet og håndtering av utstyr*, utgjøre del av regelmessige sikkerhetsrevisjoner. Se også FA 06 Sikkerhetsrevisjon som utdyper hvordan kravene kan oppfylles.

[86] Normen 6.0 kapittel 5.7.3 andre avsnitt
[87] Normen 6.0 kapittel 5.2.3 og veilederens kapittel 4.4

7 Fysisk sikkerhet og håndtering av utstyr

7.1 Fysisk utstyr og infrastruktur

Virksomheten og leverandøren skal tilrettelegge for å etterleve Normens krav[88] til bl.a. *nøkler/adgangskort*, *IKT-utstyr*, *infrastruktur*, *mobilt utstyr og hjemmekontor* og *medisinsk utstyr.* I kravene fremgår det spesifikt at utstyret[89] skal[90] sikres mot adgang fra uvedkommende, at tilgang skal logges og at fysisk adgang skal kontrolleres. Det henvises til følgende veiledningsmateriell for nærmere beskrivelser:

Tiltak som bør etableres for å sikre adganger og håndtering av utstyr:

- ***FA 17*: Fysisk sikring av områder og utstyr**
- ***FA 18*: Sikring av bærbart utstyr**
- ***FA 29*: Hjemmekontor og annet fjernarbeid**

7.2 Kryptering

All kommunikasjon av helse- og personopplysninger utenfor virksomhetens kontroll skal krypteres Kommunikasjonen skal, enten denne skjer via trådløst samband eller fysiske linjer, sikres med kryptering. Krav og anbefalinger om kryptering bør sees i sammenheng med veilederens kapittel 0 Kommunikasjonssikkerhet.

For å etterleve Normens krav[91] anbefales bruk av følgende tiltak[92]:

Tiltak som bør etableres for å sikre kommunikasjon og lagring av helse- og personopplysninger:

- ***2.7.1*: Strategi for håndtering av kryptografi i virksomheten**
- ***2.7.2*: Aktiver kryptering i tjenester og benytt anbefalte algoritmer og nøkkellengder**
- ***2.7.4*: Benytt kryptering når konfidensiell informasjon overføres**
- ***2.7.5*: Definer krav til ulike typer informasjon med ulikt behov for beskyttelse**
- ***2.4.2*: Krypter alle trådløse og kablede forbindelser**

Normen beskriver at kryptering av lagrede helse- og personopplysninger *kan* vurderes[93] som sikkerhetstiltak. Helse- og personopplysninger som lagres lokalt på mobilt utstyr skal alltid lagres kryptert, og kun når det er nødvendig ut fra tjenstlig behov[94]. Ved behov for å kryptere data i ro, bør tiltak 2.7.3[95] etableres for å oppfylle krav[96] om kryptert lagring av direkte personidentifiserende kjennetegn.

---

[88] Normen 6.0 kapittel 5.3
[89] Her vil det si utstyr for bruk til fjernaksess og som del av fjernaksessløsningen
[90] Normen 6.0 kapittel 5.7.5
[91] Normen 6.0 kapittel 5.3.5
[92] NSMs grunnprinsipper for IKT-sikkerhet, grunnprinsipp 2.7 *Krypter data i ro og transitt* samt 2.4 *Beskytt virksomhetens nettverk*.
[93] I registre etablert med hjemmel i helseregisterloven §§ 10 og 11 skal direkte personidentifiserende kjennetegn lagres kryptert.
[94] Normen 6.0 kapittel 5.3.4
[95] Krypter lagringsmedier som holder konfidensielle data og som lett kan mistes eller kompromitteres
[96] Normen 6.0 kapittel 5.3.5

8 Eksempler på tekniske løsninger

Eksempler på godkjennbare løsninger for fjernaksess:

1) **Teknisk løsning levert av Tredjepart** (kapittel 8.1)
2) **Site-to-site VPN-løsning, via Norsk helsenett *eller* internett** (kapittel 8.2)
3) **VPN-løsning med klient levert av virksomheten** (kapittel 8.3)
4) **Teknisk løsning med kontrollsone hos virksomheten, ved f.eks. VDI eller TS** (kapittel 8.4)
5) **Teknisk løsning levert som skytjeneste**

Dette kapitlet gir eksempler på et utvalg[97] tekniske løsninger som er ment å oppfylle krav i Normen. Eksemplene viser løsninger der leverandøren kobler seg opp til virksomheten, ved at leverandøren selv initierer oppkoblingen med fjernaksess. Løsning for automatisk[98] kontakt beskrives ikke i eksemplene, men bør betraktes som ethvert informasjonssystem i virksomheten som har forbindelser til eksterne nett.

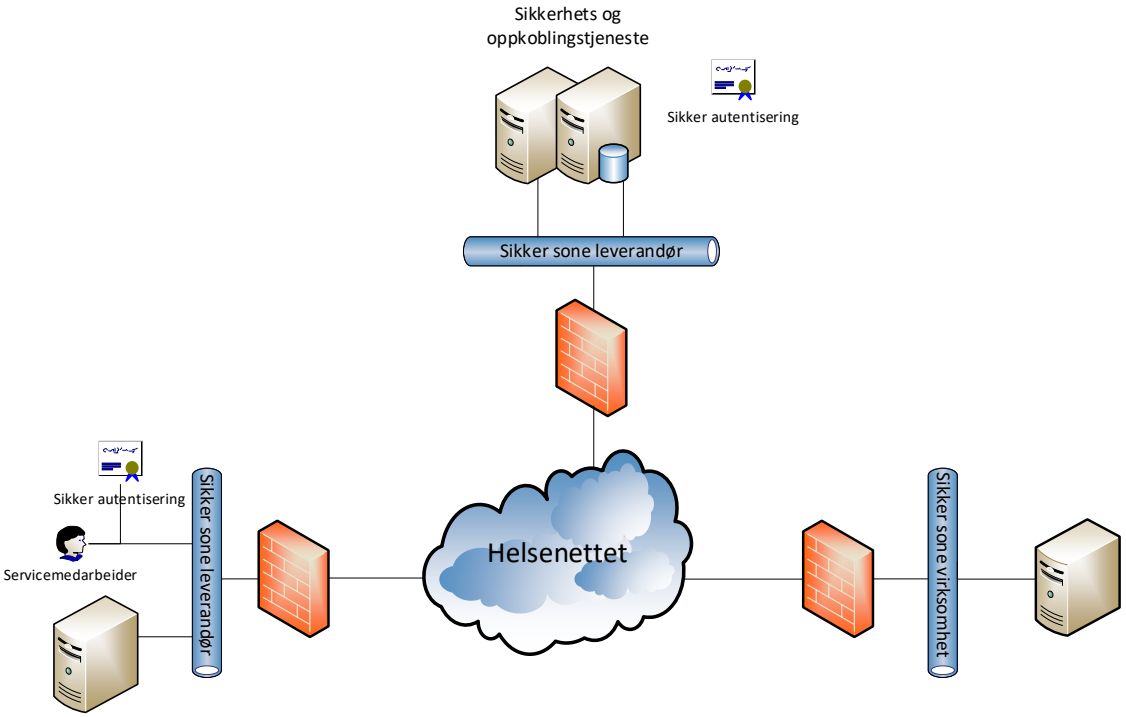
8.1 Eksempel 1: Løsning levert av Tredjepart

Første eksempel viser bruk av verktøy for *fjernadministrasjon* levert av *Tredjepart*[99].

Figuren i eksempel 1 illustrerer at:

1) **Virksomheten har installert klient for fjernadministrasjon på en arbeidsstasjon**
2) **Virksomheten har åpnet opp for utgående IP-adresse og portnummer til Tredjepart sin fjernadministrasjonstjeneste**
3) **Virksomheten og leverandøren initierer oppkobling mot en definert server hos Tredjepart**
4) **Leverandøren autentiserer seg mot tjenesten hos Tredjepart på sikkerhetsnivå høyt**
5) **Trafikken krypteres med funksjonalitet i fjernadministrasjonsverktøyet**
6) **Tredjepart har på vegne av virksomheten konfigurert fjernadministrasjonsverktøyet slik at leverandørens tilgang er sterkt begrenset og kun til det aktuelle formålet**
7) **All trafikk skal logges automatisk eller manuelt i fjernadministrasjonsverktøyet**
8) **Leverandøren har supportmaskiner stående i sikkert nett**
9) **Internett (eller Helsenettet) benyttes for kommunikasjon**

[97] Det kan også være andre løsninger som oppfyller kravene
[98] Flere løsninger kan automatisk initiere kontakt med leverandørens tekniske løsning, f.eks. for rapportering om status på systemer og infrastruktur, oversendelse av feilmeldinger mv.
[99] Tredjepart kan her være Norsk Helsenett eller andre nasjonale leverandører av spesifisert løsning.



Figur 4: Eksempel på løsning levert av Tredjepart.

Tabellen nedenfor viser hvem som ivaretar sikkerhetsoppgavene i eksempelet i figur 4. I de tilfellene hvor både virksomhet og leverandør er angitt så vil oppgavefordelingen avhenge av hvilke varianter av løsninger som tas i bruk.

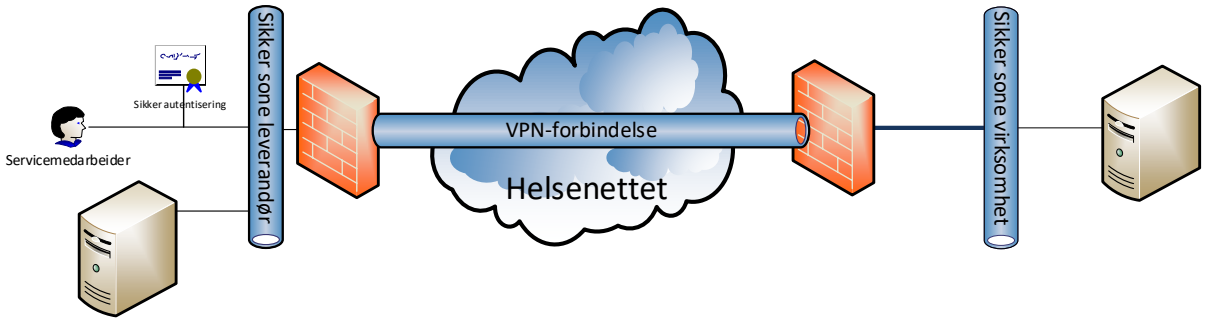
Kap. nr	Oppgaver	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.3	Tjenesteutsetting (Normen kap. 5.7.3)	☒	☐	☐
2.4	Avtaler og rutiner (Normen kap. 5.7.2)	☒	☒	☐
2.5	Databehandler (Normen kap. 5.7.4 og 2.3)	☒	☒	☐
2.6	Krav til leverandørens taushetserklæring (Normen kap. 5.1.1 og 5.7.1)	☒	☒	☐
6.4	Sikkerhetsrevisjon og håndtering av informasjonssikkerhetsbrudd (Normen kap. 5.4.6 og 5.8)	☒	☒	☐
3.2	Risikovurdering før fjernaksess etableres og i sikker IT-drift (Normen kap. 3, 5.4 m.fl.)	☒	☒	☐
2.4	Opplæringstiltak (Normen kap. 5.1.2)	☒	☒	☐
5.3	Begrensning av trafikk (Normen kap. 5.5.2)	☒	☒	☐

Kap. nr	Oppgaver	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
7.2	Kryptering (Normen kap. 5.3.5)	☒	☒	☐
6.2	Forhindre ondsinnet programvare (Normen kap. 5.4.1 og 5.7.5)	☒	☒	☐
7.1	Adgangsregulering til fysisk utstyr og infrastruktur (Normen kap. 5.3)	☒	☒	☐
7.1	Fysiske sikkerhetstiltak (Normen kap. 5.3 og 5.7.5)	☒	☒	☐
2.4, 4.2	Tildele autorisasjon (Normen kap. 5.2.1)	☒	☐	☐
4.2	Rutine for tildeling av autorisasjon (Normen kap. 5.2.1)	☒	☐	☐
4.2	Autorisasjonsregister (Normen kap. 5.2.1.1)	☒	☐	☐
4.3	Sikker autentiseringsløsning (Normen kap. 5.2.2)	☒	☒	☐
4	Tilgangsstyring (Normen kap. 5.2)	☒	☐	☐
4	Bruk av autorisasjon (Normen kap. 5.2 og 5.5.2)	☐	☒	☐
2.5	Overføring av helse- og personopplysninger til utland (Normen kap. 5.7.8)	☒	☒	☐
2.5	Skille helse- og personopplysninger fra flere virksomheter (Normen kap. 5.7.4.4)	☐	☒	☐
6.1	Konfigurasjonskontroll (Normen kap. 5.4.1)	☒	☒	☐
6.3	Logging (Normen kap. 5.4.4)	☒	☒	☐
6.3	Analyse av logger (Normen kap. 5.4.4)	☒	☒	☐
6.4	Innsyn i leverandørens logger (Normen kap. 5.4.4)	☒	☒	☐

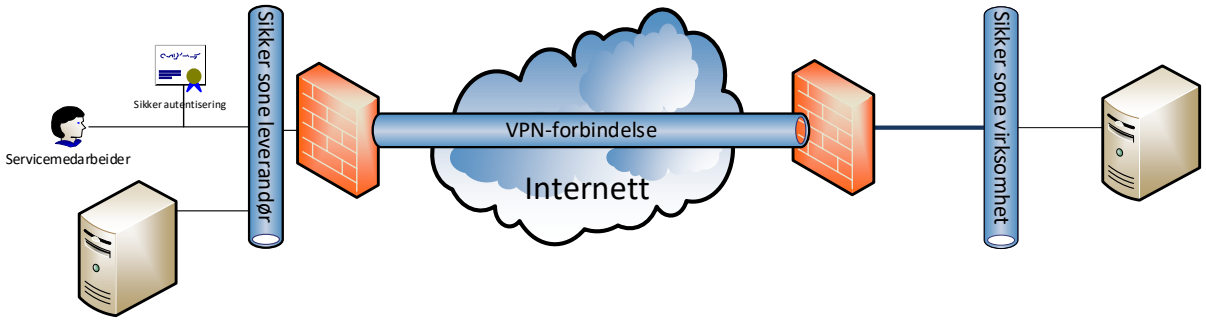
For oppgaver og roller vises det til tjenestebeskrivelsen av fjernaksessløsningen.

8.2 Eksempel 2: Site-to-site VPN

Andre eksempel viser Site-to-site VPN-løsning, via Norsk helsenett eller Internett.



Figur 5: Eksempel på VPN-løsning over Helsenettet.



Figur 6: Eksempel på VPN-løsning over Internett.

Figurene 5 og 6 illustrerer at:

- Kommunikasjon mellom virksomheten og leverandøren skjer på en IPsec-sikret VPN forbindelse.
- Kommunikasjonen kan gå enten via Norsk Helsenett eller via Internett.
- Autentisering av medarbeider skjer med sikkerhetsnivå høyt hos leverandøren. F.eks. PKI pålogging.

Eksempel på bruk:

1. Kunde melder feil på et system til en leverandør

   Medarbeider hos leverandør logger på systemet via leverandørens fjerndiagnosesystem. Denne påloggingen gir en begrenset tilgang til systemet. Ved hjelp av verktøy på systemet kan Medarbeider så analysere feillogger. Etter noe analyse avdekkes at det må utføres en jobb på systemet. Kunde åpner så opp for utvidet tilgang slik at Medarbeider kan utføre de nødvendige oppgavene. Dette kan være endring i konfigurasjonen, opplasting av programvarepatcher eller nedlasting av spesielle filer. Etter endt service settes systemet tilbake til begrenset tilgang og Medarbeider logger seg av.

2. System hos kunde trenger oppdatering av programvare

   Leverandøren har en oppdatering til programvaren på kundens system. Dette kan være en antiviruspatch, en Windows hotfix eller en annen bugfix til systemet. Leverandørens fjerndiagnosesystem sender oppdateringen til kundens system. Kunden får opp melding på systemet at det er en oppdatering tilgjengelig og må aktivt velge om denne skal installeres eller ikke. Etter installasjon melder kunden systemet automatisk tilbake til leverandørens fjerndiagnosesystem at oppdateringen er utført.

3. Proaktiv overvåking av viktige parametere

   Kundens system sender jevnlig rapporter til leverandørens fjerndiagnosesystem med informasjon om tilstanden på systemet. Disse rapportene kan inneholde data om temperatur, trykk, nivå, fyllingsgrad i databaser, feilmeldinger som oppstår etc.

Tabellen nedenfor viser hvem som ivaretar sikkerhetsoppgavene i dette eksempelet. I de tilfellene hvor både virksomhet og leverandør er angitt så vil oppgavefordelingen avhenge av hvilke varianter av løsninger som tas i bruk.

Kap. nr	Oppgaver	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.3	Tjenesteutsetting (Normen kap. 5.7.3)	☒	☐	☐
2.4	Avtaler og rutiner (Normen kap. 5.7.2)	☒	☒	☐
2.5	Databehandler (Normen kap. 5.7.4 og 2.3)	☒	☒	☐
2.6	Krav til leverandørens taushetserklæring (Normen kap. 5.1.1 og 5.7.1)	☒	☒	☐
6.4	Sikkerhetsrevisjon og håndtering av informasjonssikkerhetsbrudd (Normen kap. 5.4.6 og 5.8)	☒	☒	☐
3.2	Risikovurdering før fjernaksess etableres og i sikker IT-drift (Normen kap. 3, 5.4 m.fl.)	☒	☒	☐
2.4	Opplæringstiltak (Normen kap. 5.1.2)	☒	☒	☐
5.3	Begrensning av trafikk (Normen kap. 5.5.2)	☒	☒	☐
7.2	Kryptering (Normen kap. 5.3.5)	☒	☒	☐
6.2	Forhindre ondsinnet programvare (Normen kap. 5.4.1 og 5.7.5)	☒	☒	☐
7.1	Adgangsregulering til fysisk utstyr og infrastruktur (Normen kap. 5.3)	☒	☒	☐

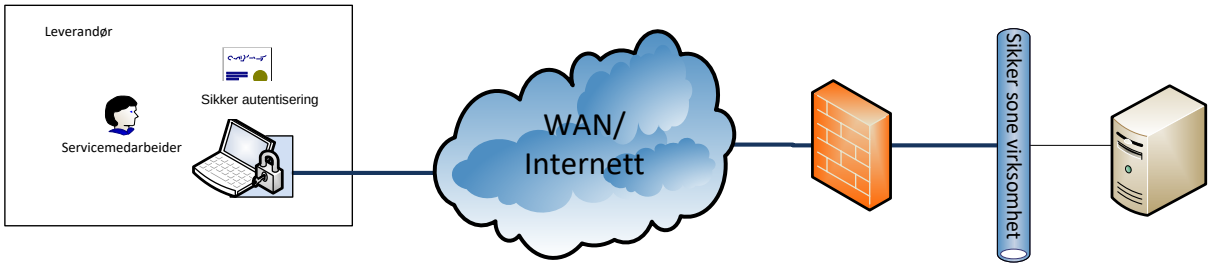
Kap. nr	Oppgaver	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
7.1	Fysiske sikkerhetstiltak (Normen kap. 5.3 og 5.7.5)	☒	☒	☐
2.4, 4.2	Tildele autorisasjon (Normen kap. 5.2.1)	☒	☐	☐
4.2	Rutine for tildeling av autorisasjon (Normen kap. 5.2.1)	☒	☒	☐
4.2	Autorisasjonsregister (Normen kap. 5.2.1.1)	☒	☐	☐
4.3	Sikker autentiseringsløsning (Normen kap. 5.2.2)	☒	☒	☐
4	Tilgangsstyring (Normen kap. 5.2)	☒	☒	☐
4	Bruk av autorisasjon (Normen kap. 5.2 og 5.5.2)	☐	☒	☐
2.5	Overføring av helse- og personopplysninger til utland (Normen kap. 5.7.8)	☒	☒	☐
2.5	Skille helse- og personopplysninger fra flere virksomheter (Normen kap. 5.7.4.4)	☐	☒	☐
6.1	Konfigurasjonskontroll (Normen kap. 5.4.1)	☒	☒	☐
6.3	Logging (Normen kap. 5.4.4)	☒	☒	☐
6.3	Analyse av logger (Normen kap. 5.4.4)	☒	☒	☐
6.4	Innsyn i leverandørens logger (Normen kap. 5.4.4)	☒	☒	☐

8.3 Eksempel 3: Klient-VPN

Eksemplet under viser oppkobling over Internett der virksomheten har kontroll basert på VPN. Løsningen kan omtales som en hjemmekontorløsning. Som beskrevet i kapittel 5.4 bør VPN-løsningen i kapittel 8.2 foretrekkes foran denne løsningen dersom det er mulig. Dette fordi klientutstyret i bruk vil være betydelig mer eksponert mot usikre nettverk, noe som kan medføre større risiko for infrastruktur, systemer og opplysninger som klientutstyret har fjernaksess til. Løsningen kan imidlertid vurderes benyttet dersom andre løsninger ikke er aktuelle eller dekker formålet.

Figur 7 illustrerer at:

- Leverandøren får en PC av virksomhetene og benytter virksomhetens hjemmekontorløsning
- *Virksomheten* har kontroll på eller har godkjent *leverandørens* lokale sikkerhetsmekanismer. Eks. lokalt installerte VPN-klient med *virksomhetens* policy
- All kommunikasjon foregår kryptert
- Tilgang til helse- og personopplysninger krever at bruker identifiserer seg med sikkerhetsnivå høyt



Figur 7: Eksempel på oppkobling der virksomheten har kontroll basert på VPN (hjemmekontorløsning).

Ettersom løsningen kan medføre økt risiko er det viktig å følge tiltakene i kapittel 2 t.o.m. 7. For å redusere risiko bør det legges spesielt vekt på god praksis for nettverkssikkerhet (kapittel 5), for å sikre tjenester og kontrollere dataflyt, tilgangsstyring (kapittel 4). Det er spesielt viktig at NSMs grunnprinsipp 2.3 innføres for å ivareta sikkerhet på klientutstyret. Noen aktuelle tiltak for sikkerhetsherding av klientutstyr kan være:

- CIS Benchmarks for aktuell operativsystemversjon (f.eks. Windows 10, 11 e.l.)
- Se Device management NCSC UK

Tabellen nedenfor viser hvem som ivaretar sikkerhetsoppgavene i dette eksempelet. I de tilfellene hvor både virksomhet og leverandør er angitt så vil oppgavefordelingen avhenge av hvilke varianter av løsninger som tas i bruk.

Kap. nr	Oppgaver	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.3	Tjenesteutsetting (Normen kap. 5.7.3)	☒	☐	☐
2.4	Avtaler og rutiner (Normen kap. 5.7.2)	☒	☒	☐

Kap. nr	Oppgaver	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.5	Databehandler (Normen kap. 5.7.4 og 2.3)	☒	☒	☐
2.6	Krav til leverandørens taushetserklæring (Normen kap. 5.1.1 og 5.7.1)	☒	☒	☐
6.4	Sikkerhetsrevisjon og håndtering av informasjonssikkerhetsbrudd (Normen kap. 5.4.6 og 5.8)	☒	☒	☐
3.2	Risikovurdering før fjernaksess etableres og i sikker IT-drift (Normen kap. 3, 5.4 m.fl.)	☒	☒	☐
2.4	Opplæringstiltak (Normen kap. 5.1.2)	☒	☒	☐
5.3	Begrensning av trafikk (Normen kap. 5.5.2)	☒	☒	☐
7.2	Kryptering (Normen kap. 5.3.5)	☒	☐	☐
6.2	Forhindre ondsinnet programvare (Normen kap. 5.4.1 og 5.7.5)	☒	☒	☐
7.1	Adgangsregulering til fysisk utstyr og infrastruktur (Normen kap. 5.3)	☒	☒	☐
7.1	Fysiske sikkerhetstiltak (Normen kap. 5.3 og 5.7.5)	☒	☒	☐
2.4, 4.2	Ansvar for å tildele autorisasjon (Normen kap. 5.2.1)	☒	☐	☐
4.2	Rutine for tildeling av autorisasjon (Normen kap. 5.2.1)	☒	☐	☐
4.2	Autorisasjonsregister (Normen kap. 5.2.1.1)	☒	☐	☐
4.3	Sikker autentiseringsløsning (Normen kap. 5.2.2)	☒	☐	☐
4	Tilgangsstyring (Normen kap. 5.2)	☒	☐	☐
4	Bruk av autorisasjon (Normen kap. 5.2 og 5.5.2)	☐	☒	☐
2.5	Overføring av helse- og personopplysninger til utland (Normen kap. 5.7.8)	☒	☒	☐
2.5	Skille helse- og personopplysninger fra flere virksomheter (Normen kap. 5.7.4.4)	☒	☒	☐

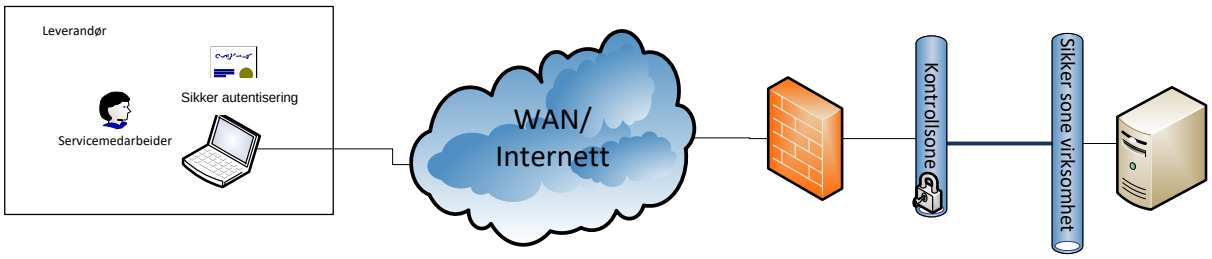
Kap. nr	Oppgaver	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
6.1	Konfigurasjonskontroll (Normen kap. 5.4.1)	☒	☐	☐
6.3	Logging (Normen kap. 5.4.4)	☒	☐	☐
6.3	Analyse av logger (Normen kap. 5.4.4)	☒	☐	☐
6.4	Innsyn i leverandørens logger (Normen kap. 5.4.4)	☐	☐	☒

8.4 Eksempel 4: Klient-til-VPN med kontrollsone

Eksemplet under viser oppkobling over Internett. Sikkerheten håndteres i en kontrollsone i virksomheten.

Figur 8 illustrerer at:

- Virksomheten ikke har noe kontroll med leverandørens brukerutstyr
- All kommunikasjon foregår kryptert
- Virksomheten har en kontrollsone som innehar nødvendige sikkerhetsmekanismer, og forhindrer direkte kommunikasjon fra leverandørens brukerutstyr til foretakets systemer. F.eks. VDI/TS.
- Tilgang til pasientdata krever at bruker identifiserer seg med sikkerhetsnivå høyt.



Figur 8: Eksempel på oppkobling over Internett der sikkerheten håndteres i en kontrollsone i virksomheten.

Tabellen nedenfor viser hvem som ivaretar sikkerhetsoppgavene i dette eksempelet. I de tilfellene hvor både virksomhet og leverandør er angitt så vil oppgavefordelingen avhenge av hvilke varianter av løsninger som tas i bruk.

Kap. nr	Kapittel tittel	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.3	Tjenesteutsetting (Normen kap. 5.7.3)	☒	☐	☐
2.4	Avtaler og rutiner (Normen kap. 5.7.2)	☒	☒	☐
2.5	Databehandler (Normen kap. 5.7.4 og 2.3)	☒	☒	☐
2.6	Krav til leverandørens taushetserklæring (Normen kap. 5.1.1 og 5.7.1)	☒	☒	☐
6.4	Sikkerhetsrevisjon og håndtering av informasjonssikkerhetsbrudd (Normen kap. 5.4.6 og 5.8)	☒	☒	☐
3.2	Risikovurdering før fjernaksess etableres og i sikker IT-drift (Normen kap. 3, 5.4 m.fl.)	☒	☒	☐
2.4	Opplæringstiltak (Normen kap. 5.1.2)	☒	☒	☐
5.3	Begrensning av trafikk (Normen kap. 5.5.2)	☒	☒	☐
7.2	Kryptering (Normen kap. 5.3.5)	☒	☒	☐
6.2	Forhindre ondsinnet programvare (Normen kap. 5.4.1 og 5.7.5)	☒	☒	☐
7.1	Adgangsregulering til fysisk utstyr og infrastruktur (Normen kap. 5.3)	☒	☒	☐
7.1	Fysiske sikkerhetstiltak (Normen kap. 5.3 og 5.7.5)	☒	☒	☐
2.4, 4.2	Tildele autorisasjon (Normen kap. 5.2.1)	☒	☐	☐
4.2	Rutine for tildeling av autorisasjon (Normen kap. 5.2.1)	☒	☐	☐
4.2	Autorisasjonsregister (Normen kap. 5.2.1.1)	☒	☐	☐
4.3	Sikker autentiseringsløsning (Normen kap. 5.2.2)	☒	☐	☐
4	Tilgangsstyring (Normen kap. 5.2)	☒	☐	☐
4	Bruk av autorisasjon (Normen kap. 5.2 og 5.5.2)	☐	☒	☐

Kap. nr	Kapittel tittel	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.5	Overføring av helse- og personopplysninger til utland (Normen kap. 5.7.8)	☒	☒	☐
2.5	Skille helse- og personopplysninger fra flere virksomheter (Normen kap. 5.7.4.4)	☒	☒	☐
6.1	Konfigurasjonskontroll (Normen kap. 5.4.1)	☒	☒	☐
6.3	Logging (Normen kap. 5.4.4)	☒	☒	☐
6.3	Analyse av logger (Normen kap. 5.4.4)	☒	☒	☐
6.4	Innsyn i leverandørens logger (Normen kap. 5.4.4)	☒	☒	☐

9 Eksempler på risikofaktorer ved fjernaksess

Kapitlet gir eksempler på risikofaktorer, uønskede hendelser og tiltak som kan være aktuelle ved risikovurderinger, gjennomført av virksomheten og leverandøren. Listen er ikke uttømmende. Eksemplene er veiledende og bør ikke benyttes som et fullt ut dekkende sett med scenarioer, risikofaktorer eller tiltak. Risikovurderinger må tilpasses det enkelte tilfelle, dvs. for den enkelte interessent, formål, valgt løsning, drift, tilganger og bruk av fjernaksess. Nærmere beskrivelser av metodisk gjennomføring av risikovurdering beskrives i *Veileder for risikostyring i informasjonssikkerhet og personvern.*

Uønsket hendelse / scenario		Beskrivelse av tiltak	Betydning / kommentar
1	Uautorisert tilgang **til** virksomhet*ens* nettverk pga manglende autentisering med sikkerhetsnivå høyt.	Etabler løsning for autentisering på sikkerhetsnivå høyt. (Annen løsning kan vurderes, såfremt løsningen er risikovurdert og ivaretar fastsatt nivå for akseptabel risiko)	• Utrede teknisk løsning • Installere og sette i verk rutiner • Påse at leverandørene bestiller sikkerhetsnivå høyt
2	Manglende eller for svak kryptering av helse- og personopplysninger i transitt.	Etablere sikker kryptering fra brannmur mottak	• Påse at utstyr støtter sikker kryptering (se f.eks. utstyr, protokoller og programvarebiblioteker) • Ved behov, oppdater eller oppgrader programvare og eventuelt maskinvare • Konfigurer utstyr til å bruke sikker kryptering
3	Manglende eller mangelfull logging i brannmur i DMZ-sonen	Etabler DMZ-sone med sikkerhetsfunksjonalitet for inspeksjon og logging av datainnhold i nettverkstrafikk (som omtalt i veilederens kapittel 5.4.). (Dersom løsningen ivaretas av leverandøren må virksomheten påse at tiltak i høyre kolonne avtales med leverandøren)	• Etabler DMZ-sone med aktuelle sikkerhetsfunksjoner (f.eks. Lag 3-brannmur for perimetersikring og applikasjonsbrannmur for inspeksjon og logging. Flere alternativer kan være aktuelle) • Etabler og implementert systemteknisk policy for inspeksjon og logging • Etabler rutiner samt verktøy og kapasiteter for å følge opp logger og hendelser.
4	Manglende innsyn i logger i fjernaksessløsningen hos leverandøren	Avtal innsyn i logger i fjernaksessløsning (og driftsmiljø dette utgjør del av) hos leverandøren, og gjør betingelsene til del av avtalen	• Avtal innsyn i nødvendige logger • Etabler rutiner for innsyn i logger

Uønsket hendelse / scenario		Beskrivelse av tiltak	Betydning / kommentar
		som regulerer leverandørforholdet.	• Spesifiser innsyn nærmere ved behov for logger fra driftsmiljø
5	Manglende konfigurasjonsstyring/ endingsstyring, med konsekvens for utilsiktet nedetid	Etablere rutine for konfigurasjonsendringer og endringshåndtering, og dokumentering av eventuelle avvik eller feil	• Ny rutine i styringssystemet for informasjonssikkerhet og personvern • Opplæring av ansvarlig personell og medarbeidere
6	Manglende sikring av leverandørens driftsmiljø	Fastsett mulighet i avtale og rutiner for å periodisk revidere avtalefestede betingelser, samt gjøre sikkerhetsrevisjon av etterlevelse av betingelsene (her sikring av leverandørens driftsmiljø) for avtaleperioden	• Fastsett dekkende avtalebetingelser • Ny rutine for sikkerhetsrevisjon av etterlevelse av avtalebetingelser • Ny rutine for oppfølging av avtale • Gjør overnevnte del av styringssystem for informasjonssikkerhet og personvern
7	Uautorisert utlevering av helse- og personopplysninger med konsekvens for konfidensialitet	Utarbeide og dokumentere rutine for bruk av fjernaksess samt gjennomføre opplæring	• Involvere alle relevante medarbeidere (i virksomheten og eventuelt hos leverandøren). Se Normen 6.0 kap. 5.7.7.
8	Overføring av ondsinnet programvare fra leverandør til virksomheten	Antivirus på egen og leverandørens datamaskin. Inspeksjon av trafikken. Sikre at maskinene som skal ha fjernaksess er oppdatert/patchet (herdet). Vurdere behov for egen kanal for slusing av filer med kontroll av HASH på filer.	
9	Manglende eller for svak kryptering av datakommunikasjon med konsekvens av at autentiseringsdata og helse- og personopplysninger kan komme på avveie	Etablere sikker kryptering	• Påse at utstyret støtter sikker kryptering (se pkt.2) • Konfigurer og iverksett sikker kryptering i VPN
10	Manglende eller mangelfull logging	Etabler avtale med leverandør om hvilken informasjon det er behov for at virksomheten skal ha logger på.	

Uønsket hendelse / scenario		Beskrivelse av tiltak	Betydning / kommentar
11	Behandling av helse- og personopplysninger hentet fra virksomheten blir gjennomført på åpent nettverk hos leverandøren pga manglende logisk adskillelse i leverandørens nett	Etablere logisk adskillelse i nettverket / fjernaksessløsningen mellom de ulike kundene og mellom leverandørens egen virksomhet. Virksomhetens forventninger til logisk adskillelse bør være avklart.	• Utrede teknologi • Anskaffe og installere løsning • Iverksette rutine og opplæring
12	Manglende fysisk sikring av infrastruktur og utstyr i leverandørens driftsmiljø		
13	Fjernaksessesjon blir stående pålogget i lang tid, utover det som anses å være normal bruk.	Avklar og fastsett hensiktsmessige terskelverdier for etablering og bruk av sesjoner for fjernaksess. Avslutt sesjoner som overskrider fastsatte verdier.	• Avklar terskelverdier (og eventuelle behov for unntak) • Konfigurer infrastruktur basert på fastsatte terskelverdier.

10 Eksempler på avtale, rutiner og sikkerhetsinstruks

10.1 Eksempel 1: Avtale mellom virksomhet og leverandør

Dette forslaget kan benyttes som bilag til Statens standardavtaler.

I teksten nedenfor brukes begrepet kunden om *virksomheten* slik at det aktuelle bilaget er riktig i forhold til den øvrige avtaleteksten.

Forslag til tekst til bilag i vedlikeholdsavtaler:

Under etablering og bruk av løsning for fjernaksess skal krav i gjeldende versjon av "Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren" (Normen) av legges til grunn.

Både *leverandøren* og *kunden* har et selvstendig ansvar for at Normen følges.

Kunden bør ha full innsynsrett i *leverandørens*:

- Sikkerhetsmål og -strategi
- Teknologiske og organisatoriske løsninger for fjernaksessen
- Rutiner som gjelder for fjernaksessen
- Resultat av risikovurdering og sikkerhetsrevisjoner
- Logger

Krav i Normen som skal ivaretas av *leverandøren*:
Jf. kap. 5.7 i Normen

- *leverandørens* personale har undertegnet taushetserklæring som innebærer en absolutt taushetsplikt med henblikk på alle helse- og personopplysninger.
- *leverandøren etterlever Normen med tanke på databehandlingsansvarliges* plikter vedrørende sikkerhetsrevisjoner og avviksbehandling.
- *leverandørens* utstyr som benyttes ved online oppkobling ved hjelp av kommunikasjonsnett eller medbrakt utstyr som knyttes til *virksomhetens* utstyr, ikke har ondsinnet programvare som inneholder virus e.l. og at utstyret er sikret mot *adgang* fra uvedkommende.
- tilgjengelighet til helse- og personopplysninger så vidt mulig skal opprettholdes når *leverandøren* utfører arbeid på *virksomhetens* utstyr/programvare, slik at *virksomhetens* oppgavebehandling ivaretas.

Forslag til innhold i avtalen:
Følgende elementer bør innarbeides som del av avtalen mellom virksomheten og leverandøren:

- Hvem avtalepartene er
- Formålet med avtalen eller særavtalen
- Ansvarlige personer/roller
- Virksomheten skal ha tilgang til leverandørens dokumentasjon av sikkerhetsmål og strategi
- Virksomheten skal ha innsynsrett i leverandørens løsning for ivaretakelse av Normen

- Virksomheten skal ha rett til innsyn i leverandørens logger
- Taushetsplikt for leverandørens personale
- Hvilke rutiner som gjelder for fjernaksessløsningen
- Rutine for avviksbehandling
- Konsekvenser ved brudd på avtalen
- Oversikt over hvilke systemer det gis fjernaksess til
- Beskrivelse av utstyr leverandøren kan benytte til fjernaksess og eierforholdet til utstyret
- Konsekvensutredning ved tilsiktet brudd under bruk av fjerntilkoblingen

10.2 Eksempel 2: Rutiner knyttet til avtale mellom virksomhet og leverandør

Følgende er viktige eksempler på rutiner som bør innarbeides og etterleves, som del av avtalen som regulerer tjenester for fjernaksess mellom virksomhet og leverandør:

- Signering av taushetserklæring og bekreftelse på at sikkerhetsinstruks er lest og akseptert
- Oppbevaring og innsyn i taushetserklæringer.
- Opplæring av medarbeider (jfr. Normens kapittel 5.1.2)
- Kompetanse hos medarbeider (innen):
    - Fjernaksessløsningen (som sådan), herunder teknologier, sikkerhetsmekanismer og bruk,
    - Sikkerhetsovervåkning av fjernaksessløsningen, herunder logging og analyse av logger
- Administrasjon av autorisasjon til utstyr som benyttes til fjernaksess
- Bruk av løsning for sterk[100] autentisering
- Avviksbehandling ifm. fjernaksess
- Logging og analyse av logger
- Sletting av datafiler hentet fra *virksomheten*
- Destruksjon av lagringsmedia ved utrangering
- Oppgaver som kan utføres ved oppkobling /etablering av fjernaksess (se sjekkliste i veilederens vedlegg)
- Tildele autorisasjon til nettverk, utstyr og systemer
- Autentisering av medarbeider hos *leverandør*
- Kontroll av tildelte autorisasjoner
- Oppgaver som skal utføres ved oppkobling /etablering av fjernaksess (se sjekkliste i veilederens vedlegg)

[100] Risikovurdering skal ligge til grunn for valg av autentiseringsløsning. Sikker autentiseringsløsning basert på personlig kvalifisert sertifikat (les sikkerhetsnivå høyt), er normalkrav, men kan avvikes dersom risikovurdering av annen autentiseringsløsning viser at den har tilstrekkelig sikkerhet.

10.3 Eksempel 3: Rutiner til opplæring av personell

Følgende eksempler på dokumenterte rutiner bør innarbeides til opplæringsformål.

- Krav[101] til leverandøren ifm. fjernaksess
- System- og løsning for fjernaksess (f.eks. arkitektur, komponenter, teknologier, sikkerhetsfunksjoner mv.)
- Bruk av løsning for fjernaksess (daglig praktisk anvendelse, samt drift- og administrasjon ved behov)
- Konfigurasjonskontroll (jfr. veilederens kapittel 6.1)
- Bestilling, endring og sletting av brukerkontoer[102]
- Oppretting og vedlikehold autorisasjonsregister[103] (inkl. tildeling og tilbaketrekking av autorisasjoner)
- Beskyttelsestiltak mot ondsinnet programvare (jfr. veilederens kapittel 6.2)
- Logging, analyse og kontroll (jfr. veilederens kapittel 6.3)
- Sletting av helse- og personopplysninger
- Bruk av bærbart datautstyr
- Håndtering av flyttbare datalagringsmedier - internt hos *leverandør*
- Bruk av trådløs teknologi
- Tilknytning av *leverandører* for fjernaksess
- Kontroll med bruk av fjernaksessløsning
- Taushetserklæring og skjema for autorisasjon av medarbeider til fjernaksess[104]
- Avvik- og hendelseshåndtering (inkl. avvik fra normalsituasjon[105] i fjernaksessløsningen)

10.4 Eksempel 4: Momenter i en sikkerhetsinstruks

Eksempelet gjelder sikkerhetsinstruks for leverandørens personell for fjernaksess:

Sikkerhetsinstruks

Regler for bruk av IT-utstyr og programvare:

- IT-utstyret som benyttes ifm. fjernaksess skal være tilknyttet leverandørens nettverk og skal være logisk adskilt fra leverandørens bedriftsinterne nettverk og øvrige kunder
- Det ikke tillatt å koble opp eller bruke privat IT-utstyr eller programvare mot <virksomheten>
- Du som medarbeider plikter å forhindre at uautoriserte får tilgang til løsninger som kan benyttes mot <virksomheten>

---

[101] Veilederens kapittel 2 og etablert avtale mellom virksomheten og leverandøren
[102] NSMs grunnprinsipper for IKT-sikkerhet grunnprinsipp 2.6, tiltak 2.6.2
[103] Veileder for tilgang til helse- og personopplysninger.
[104] Veileder for tilgang til helse- og personopplysninger.
[105] NSMs grunnprinsipper for IKT-sikkerhets grunnprinsipp 3.3 *Analyser data fra sikkerhetsovervåkning* (se f.eks. tiltak 3.3.2) samt grunnprinsipp 4.1 *Forbered virksomheten på håndtering av hendelser*.

- Det er ikke tillatt å laste ned helse- og personopplysninger fra <virksomheten> uten at dette er regulert av en databehandleravtale og i tråd med de metoder som framgår av databehandleravtalen

Brukerkonto og passord

- Du er forpliktet til å beskytte autentiseringsinformasjon (for eksempel brukernavn, passord og mv.) slik at dette ikke blir kjent for andre.
- Det er ikke tillatt å skaffe seg uautorisert tilgang til fjernaksess, <virksomhetens> fagsystemer eller infrastruktur ved å benytte andre medarbeideres autentisering.
- Det er regler for krav til passord i <virksomheten> som skal følges.

Arbeidsplassen – sikkerhet i lokalene - utlogging

- Logg alltid ut eller aktiver skjermsparer med passord når du forlater arbeidsstasjonen
- Sørg for å få oversikt over de helse- og personopplysningene du håndterer. Ikke la helse- og personopplysninger flyte rundt, men sikre opplysningene etter gjeldende rutine.

Feil sletting av informasjon

- Skulle du være så uheldig å feilaktig slette informasjon, skal <virksomheten> varsles uten opphold.

Logging

- <virksomheten> har plikt til å logge datatrafikk og aktiviteter i nettverket for å kunne ivareta informasjonssikkerheten.

Utskrifter og kopiering

- La ikke utskriftene bli liggende på skriver slik at uautoriserte kan få tilgang til innholdet.
- Utskifter med helse- og personopplysninger skal makuleres på en betryggende måte, når det ikke lenger er bruk for dem.

Håndtering av avvik

- Oppdager du brudd på sikkerheten eller det oppstår et uhell skal dette uten opphold meldes som et avvik til <virksomheten>. Vær oppmerksom på gjeldende rutine for avvikshåndtering.

11 Definisjoner

For forklaring på generelle ord og uttrykk benyttet i denne veilederen henvises det til vedlegg 6.2 Definisjoner i Normen 6.0. Det er imidlertid enkelte ord og uttrykk som er spesifikke for denne veilederen og dermed ikke er definert Normen 6.0. Definisjonen av disse følger i listen under.

-A-

Med ***«autorisere/autorisert/autorisasjon»*** menes at en person i en bestemt rolle kan gis eller er gitt bestemte rettigheter til lesing, registrering, redigering, retting, sletting og/eller sperring av *helse- og personopplysninger. Autorisasjon* kan bare gis i den grad det er nødvendig for vedkommendes arbeid, er begrunnet ut fra *tjenstlig behov* og er i henhold til bestemmelser om *taushetsplikt*.

Med «***adgang***» menes fysisk adkomst til utstyr og områder som benyttes til *behandling* av *helse- og personopplysninger*.

-D -

Med «**DMZ»** menes «demilitarisert sone», hvor en nettverkssone etableres for å beskytte deler av en virksomhets interne nettverk.

-F-

Med **«fagsystem»** menes en applikasjon eller et IT-system som behandler helse- og personopplysninger. Begrepet systemløsning brukes også om et fagsystem. Eksempler på fagsystem er: pleie- og omsorgssystem (PLO), legekontorsystem og barnevernsystem. Opplysninger i ulike fagsystemer kan både utgjøre elektronisk pasientjournal (EPJ) og annen tjenestedokumentasjon.

Med **«fjernaksess»** menes ekstern tilgang fra leverandør til virksomhet via kommunikasjonslinje. Eksempler på anvendelsesområder er: feilretting, feilsøking, oppdateringer, fjernadministrasjon, test- og utvikling, overføring av datafiler, driftsovervåking (databaser, servere, lagringsløsninger), behandling av feilmeldinger og datafiler hos leverandør og sending av feildiagnoser, mv. av fagsystemer og IKT-infrastruktur.

Med **«fjernadministrasjon»** menes at en bruker på et sted kan operere en arbeidsstasjon på et fysisk annet sted ved at skjermbilder, tastatur og mus fjernstyres.

-H-

Med «**Helsenettet»** menes nettverket som tilbys av Norsk helsenett SF.

-S-

Med «***sikkerhetsnivå høyt»*** menes to-faktorautentisering hvor en faktor er dynamisk basert på personlig kvalifiserte sertifikater. Jfr. Definisjoner av *sikker autentiseringsløsning* og *personlig kvalifisert sertifikat* i Normen.

-T-

Med «***tjenesteutsetting»*** menes at en virksomhet velger å anskaffe "produkter eller tjenester" fra en ekstern leverandør/virksomhet, i stedet for å levere og ivareta dem selv. I denne veilederen vil derfor produkter og tjenester for fjernaksess (som leveres av leverandøren til virksomheten) normalt innebære en tjenesteutsetting.

-V-

Med «**VPN»** menes «Virtuelt privat nettverk», hvor et privat nettverk etableres med en privat tunell over nettverk (f.eks. internett eller interne nett), for å sikre informasjonssikkerhet og personvern. VPN kan bruke kryptering for å beskytte trafikk.

12 Endringshistorikk

Dokumentets versjons- og endringshistorikk.

Dato	Versjon	Endring
28.11 2007	1.0	Tittel: Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet
31.05.2012	2.0	Tittel: Veileder Fjernaksess for leverandører
Juni 2022	3.0	Tittel: Veileder for fjernaksess mellom virksomhet og leverandør Oppdatert etter nye krav i Normen 6.0 og har ny struktur av innholdet. Veilederen er gjennomarbeidet sammen med referansegruppe fra sektoren.