Veileder for fjernaksess
mellom leverandør og virksomhet

Veilederen er et støttedokument til Norm for informasjonssikkerhet

Utgitt med støtte av:

Helsedirektoratet

Versjon 2.0

www.normen.no

Merknad 24.03.2019: Dokumentet er ikke oppdatert fra siste versjon av Normen (5.3), ny personopplysningslov, endringer i helselovgivningen, eller EUs personvernforordning

INNHOLD

1 INNLEDNING

1.1 Bakgrunn

Det er nødvendig for de fleste *virksomheter* i sektoren at *leverandører* bistår ved hjelp av *fjernaksess*. Bakgrunnen for en egen veileder for *fjernaksess* mellom *leverandør* og *virksomhet* er å gi veiledning for etablering av tekniske og organisatoriske løsninger.

Virksomheten (databehandlingsansvarlig) er ansvarlig for at fjernaksessløsningen oppfyller kravene i Normen. Oppgavene ifm *fjernaksess* kan deles mellom *virksomheten* og *leverandøren* etter skriftlig avtale.

Veilederen gir også hjelp til sektoren med å etablere løsninger som ivaretar gjeldende krav til sikkerhet.

1.2 Om veilederen

Veilederen er utarbeidet for styringsgruppen for Normen med støtte av Helsedirektoratet av selskapene INCERTUS og INFOSEC Norge AS.

Formålet med veilederen er å gi veiledning til etterlevelse av kravene i Normen til hvilke tekniske og administrative tiltak som må ivaretas i *virksomheten* og hos *leverandøren* ifm *fjernaksess*. *Virksomheten* er forpliktet av Normen ved inngåelse av kundeavtale med *Norsk Helsenett* (jf. Normens kap. 1.6). Av dette følger at løsningen for *fjernaksess* må ivareta Normens krav. *Leverandør* og *virksomhet* skal oppfylle kravene i Normen.

Veilederen er utarbeidet i samarbeid med *leverandører* i sektoren og sektorens egen referansegruppe. Se kapittel 5.6 for deltagere i referansegruppen.

Veilederen gjelder *fjernaksess* for alle typer informasjonssystemer hvor det behandles *helse- og personopplysninger*. Eksempler på informasjonssystemer er medisinsk billeddiagnostikk, elektronisk pasientjournal (EPJ), forvaltning drift og vedlikehold (FDV), medisinskteknisk utstyr (MTU), laboratoriesystemer og IKT-infrastruktur.

Veilederen må leses i sin helhet ettersom krav er dokumentert i flere kapitler.

1.3 Målgruppe og hvilken hjelp veilederen gir

Målgruppen for veilederen er *virksomheten* og *leverandøren.*

Veilederen gir *virksomheten* grunnlag for valg av løsning for *fjernaksess* slik at den etableres iht fastsatte krav i Normen. *Virksomheten* kan bruke veilederen som kravdokument ift *leverandører*.

Veilederen gir *leverandører* av systemer og tekniske løsninger som benyttes til *behandling* av *helse- og personopplysninger* et grunnlag for etablering av løsninger for fjernaksess iht Normen.

Eksempler på systemer og tekniske løsninger er:
- *Fagsystem* (for eksempel elektronisk pasientjournal, pasientadministrative systemer, laboratoriesystemer)
- Medisinsk teknisk utstyr (for eksempel billeddiagnostikk)
- IKT-infrastruktur (for eksempel servere, nettverk, lagringsutstyr, kommunikasjonsutstyr, sikkerhetsteknologi, m.v.)

Veilederen gjengir krav fra Normen og gir anbefalinger for hvordan kravene kan ivaretas ved etablering og bruk av *fjernaksess*.

Veilederen gir også veiledning når *leverandøren* yter *fjernaksess* uten at *virksomheten* er operativt involvert. Dette må være avtalt og tilkobling etablert med *virksomhetens* kjennskap.

1.4 Definisjoner

Definisjoner er hentet fra Normen. Nye begrep er definert og samlet etter definisjoner fra Normen. Definerte ord er markert i *kursiv* i teksten.

Definisjoner fra Normen (av 2. juni 2010)

-A-

Med "***administratorrettighet***" menes i *Normen* øverste tilgangsnivå til system, server, database, og sikkerhetsbarriere. Tilgangsnivået har som oftest rettigheter til å utføre alle operasjoner.

Med "***autentisering***" menes i *Normen* prosessen som gjennomføres for å bekrefte en påstått identitet.

Med "***autorisere/autorisert/autorisasjon***" menes i *Normen* 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 "***autorisasjonsregister***" menes i *Normen* et *register* over utstedte *autorisasjoner* som føres av den *databehandlingsansvarlige.*

Med "***avvik***" menes i *Normen* enhver håndtering av *helse- og personopplysninger* som ikke utføres i henhold til gjeldende regelverk, retningslinjer og/eller prosedyrer, samt andre sikkerhetsbrudd.

-B-

Med "***behandling***" menes i *Normen* enhver formålsbestemt bruk av *helse- og personopplysninger*, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter, jf. helseregisterloven § 2 nr. 5 og personopplysningsloven § 2 nr. 2).

-D-

Med "***databehandler***" menes den som *behandler helse- og personopplysninger* på vegne av den *databehandlingsansvarlige*, jf. helseregisterloven § 2 nr. 9 og personopplysningsloven § 2 nr. 5). Det presiseres at en *databehandler* er en ekstern person eller *virksomhet* utenfor den *databehandlingsansvarliges virksomhet*. Det vil si at den *databehandlingsansvarliges* egne medarbeidere ikke er dennes *databehandlere*.

Med "***databehandlingsansvarlig***" menes den som bestemmer formålet med *behandlingen* og hvilke hjelpemidler som skal brukes, hvis ikke *databehandlingsansvaret* er særskilt angitt i loven eller i forskrift i medhold av loven, jf. helseregisterloven § 2 nr. 8 og personopplysningsloven § 2 nr. 4) (her benyttes begrepet "behandlingsansvarlig"). Det presiseres at det er *virksomheten* som er *databehandlingsansvarlig* for *behandling* av *helse- og personopplysninger.* Ansvaret skal ivaretas av den daglige ledelsen av *virksomheten*, og *virksomheten* er pliktsubjekt.

-F-

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

-H-

*"**helse- og personopplysninger**"* benyttes i *Normen* som en fellesbetegnelse for *helseopplysninger* og/eller *personopplysninger* innenfor *Normens* virkeområde slik det er definert i Normens pkt. 1.5.

Med "***helsenettet***" menes i *Normen* nettverket som tilbys av Norsk Helsenett SF.

Med "***hendelsesregister***" menes i *Normen* et logisk *register* der hendelser i informasjonssystemet er nedtegnet, se neste definisjon.

Med "***hendelsesregistrering***" menes i *Normen* registrering av hendelser i et informasjonssystem, bl.a. med sikte på å forebygge, avdekke og hindre gjentagelse av sikkerhetsbrudd.

-K-

Med "***konfigurasjon***" menes i *Normen* informasjonssystemets utforming inklusive både teknisk utstyr og programvare.

-L-

Med "***leverandør***" menes i *Normen* juridisk enhet som yter tekniske og/eller administrative tjenester til *virksomheten*. Eksempler er *EPJ-leverandør*, røntgenleverandør, *leverandør* av løsning for SMS-meldinger, IKT-leverandør mv.

-N-

Med "***Norsk Helsenett***" menes i *Normen* Norsk Helsenett SF.

-S-

Med "***sikkerhetsnivå 4***" menes i *Normen* to-faktor *autentisering* hvor en faktor er dynamisk basert på kvalifiserte sertifikater og ellers tilfredsstiller kravene til *sikkerhetsnivå 4* i "Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor".

-T-

Med "***taushetsplikt***" menes i *Normen* lovpålagt eller avtalt plikt til å hindre at andre får adgang eller kjennskap til *helse- og personopplysninger*, jf. helsepersonelloven § 21, helseregisterloven § 15, helse- og omsorgstjenesteloven § 12-1 og forvaltningsloven §§ 13 til 13e, samt annen informasjon med betydning for informasjonssikkerheten, jf. personopplysningsforskriften § 2-9. *Taushetsplikt* innbefatter både en passiv plikt til å tie og en plikt til aktivt å hindre uvedkommende i å få kunnskap om taushetsbelagte opplysninger.

Med "***tekniske tiltak***" menes i *Normen* tiltak av teknisk karakter som ikke kan påvirkes eller omgås av medarbeidere, og ikke er begrenset av handlinger som den enkelte forutsettes å utføre. Eksempler på slike tiltak kan være *autentisering* på *sikkerhetsnivå 4* eller *konfigurering* av en brannmur slik at den kun tillater bestemt trafikk eller en meldingstjeneste som er laget slik at alle meldinger automatisk blir kryptert.

Med "***tilgang***" menes i *Normen* at *helse- og personopplysninger* om en eller flere bestemte *pasienter/brukere* er eller gjøres tilgjengelige for *autorisert* personell. Beslutning om *tilgang* til *behandlingsrettede helseregistre* skal treffes etter en konkret vurdering basert på at det ytes helsehjelp til *pasienten. Tilgang* til *fagsystemer* i forbindelse med ytelser til *pasient/bruker* skal iverksettes basert på *tjenstlig behov*. *Tilgang* i forbindelse med kvalitetssikring og administrative oppgaver skal også besluttes ut fra *tjenstlig behov*.

-V-

Med "***virksomhet***" menes i *Normen* juridisk enhet som helseforetak, *kommune*, sykehus, legepraksis, tannklinikk, apotek, apotekkjede, røntgeninstitutt, frittstående laboratorium, universitet, høyskole, stiftelse m.v.

Definisjoner i denne veilederen

-A-

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

-F-

Med "***fjernaksess***" menes i dette dokumentet 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, m.v. av *fagsystemer* og IKT-infrastruktur.

Med "***fjernadministrasjon***" menes i dette dokumentet at en bruker på et sted kan operere en arbeidsstasjon på et fysisk annet sted ved at skjermbilder, tastatur og mus fjernstyres.

-S-

Med "***servicemedarbeider***" menes i dette dokumentet medarbeider hos *leverandør*.

2 KRAV OG ANBEFALINGER VED FJERNAKSESS

I dette kapitlet beskrives krav hentet fra Normen som skal og bør ivaretas ifm. *fjernaksess*. Etterlevelse av de enkelte krav er det i utgangspunktet *databehandlingsansvarlig* som har ansvaret for, men dette kan ivaretas av *leverandøren* etter avtale. Tabellene nedenfor foreslår en oppgavedeling, men det er opp til *databehandlingsansvarlig* og *leverandør* å velge fordeling av oppgaver. Fordeling av oppgaver mellom *virksomheten* og *leverandøren* skal til sammen ivareta kravene i *Normen*

De enkelte krav er satt i anførselstegn.

2.1 Ansvar og avtaler

I dette avsnittet beskrives krav til avtaler og klargjøring av ansvar, herunder ivaretakelse av *taushetsplikten* gjennom taushetserklæring. I avsnittet beskrives typiske kontrollplikter som sikkerhetsrevisjon og avvikshåndtering.

Virksomheten og *leverandøren* kan inngå avtale hvor det benyttes en sikkerhetsleverandør av fjernaksessløsningen. Med sikkerhetsleverandør menes en underleverandør som utfører sikkerhetsoppgaver iht Normen (jf. Normen kap 5.8.4).

2.1.1 Skriftlig avtale med leverandør (Normen kap. 5.8)

”Det skal inngås skriftlige avtaler med *leverandør*. Avtalene skal inkludere forpliktelser om at partene skal oppfylle de krav og tiltak som følger av den til enhver tid gjeldende Norm for informasjonssikkerhet, samt regulering av sanksjoner ved brudd på Normen og avtalen for øvrig.”

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Det anbefales at avtalen som regulerer forpliktelse iht. Normen innarbeides som en del av avtalen med *leverandøren* om *fjernaksess*. Benytt utkast til avtaletekst i kapittel 5.4 som grunnlag for den konkrete avtalen. Avtalen bør revideres og oppdateres ved behov. For eksempel etter *avvik*, risikovurderinger og sikkerhetsrevisjoner. Det anbefales at det utarbeides en generell sikkerhetsinstruks som gjelder for *leverandører*	*Leverandøren* må påse at *servicemedarbeiderne* er kjent med innholdet av avtalen og eventuelt sikkerhetsinstruksen (jf. kap 5.5). *Leverandøren* kan benytte underleverandør. Dette skal i så tilfelle fremkomme av avtalen mellom *leverandør* og *virksomhet*. Underleverandøren bør ha *tilgang* til *virksomheten* gjennom *leverandørens* nettverk om ikke annet er avtalt og følge de sikkerhetskrav som gjelder for *leverandøren*. For underleverandøren gjelder de samme krav som for *leverandør*.	Faktaark 1 - Ansvar og organisering Faktaark 9 - Opplæring av ledere og medarbeidere

2.1.2 Taushetserklæring (Normen kap. 5.8.3)

"Leverandørens personale har undertegnet taushetserklæring som innebærer en absolutt *taushetsplikt* med henblikk på alle *helse- og personopplysninger*."

Det er leverandørens ansvar å ivareta taushetsplikten for sine servicemedarbeidere og sørge for at taushetserklæring er underskrevet av sine ansatte

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Som en del av avtalen med *leverandøren* bør *leverandøren* pålegges å organisere taushetserklæringer for *servicemedarbeiderne*. Benytt mal under referanser som tilpasses	*Leverandøren* organiserer signering av taushetserklæringer for alle *servicemedarbeidere*. Taushetserklæringer er individuelle og kan ikke signeres kollektivt. *Leverandøren* arkiverer taushetserklæringene som må være tilgjengelig for *virksomheten* på forespørsel. Selv om taushetserklæring ikke er underskrevet har enhver som utfører tjeneste eller arbeid for et forvaltningsorgan *taushetsplikt*, jf. forvaltningsloven § 13. Tilsvarende gjelder *taushetsplikten* iht helseregisterloven, jf. §§ 13 og 15.	Mal for taushetserklæring på: http://www.helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/dokumenter/taushetserklering/Sider/default.aspx

2.1.3 Sikkerhetsrevisjon og avviksbehandling (Normen kap. 5.8.3, 6.1 og 6.3)

"Leverandøren etterlever Normen med tanke på *databehandlingsansvarliges* plikter vedrørende sikkerhetsrevisjoner og avviksbehandling."

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Virksomheten skal jevnlig gjennomføre sikkerhetsrevisjon av løsningen for fjernaksess. *Virksomheten* skal påse at *leverandøren* gjennomfører sikkerhetsrevisjon og har prosedyrer for avviksbehandling. *Leverandørenes* sikkerhetsrevisjon og avviksbehandling kan være grunnlag for tiltak som *virksomheten* må iverksette	*Leverandøren* skal jevnlig og minst en gang per år gjennomføre en sikkerhetsrevisjon av løsningen som benyttes til *fjernaksess*. Alle avviksrapporter av betydning for avtalen om *fjernaksess* skal uten opphold rapporteres til *virksomheten*.	Faktaark 6 – Sikkerhetsrevisjon Faktaark 8 - Avviksbehandling

2.1.4 Bevisstgjøring av taushetsplikten (Normen kap. 5.1)

"For å sikre konfidensialitet for *helse- og personopplysninger* skal *virksomhetens* leder sikre at alt personell som gis *tilgang* har *taushetsplikt*, og at de er bevisst *taushetspliktens* innhold og omfang, for alle *helse- og personopplysninger* samt for annen informasjon med betydning for informasjonssikkerheten."

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Virksomheten bør i avtalen med *leverandør:* • Beskrive konsekvenser for *servicemedarbeider* ved brudd på *taushetsplikten*. • Beskrive konsekvenser for *servicemedarbeider* ved å tilegne seg eller forsøke å tilegne seg opplysninger man ikke har tjenstlig behov for (ulovlig tilegnelse). • Beskrive konsekvenser for *servicemedarbeider* ved å endre/forsøk på å endre opplysninger man ikke har *autorisasjon* til å endre.	*Leverandøren* skal lære opp *servicemedarbeider* i *taushetspliktens* innhold og konsekvenser ved brudd på *taushetsplikten*, ved å tilegne seg opplysninger man ikke har tjenstlig behov og ved å endre/forsøk på å endre opplysninger man ikke har *autorisasjon* til å endre.	

2.2 Risikovurdering

I dette avsnittet beskrives krav til gjennomføring av risikovurdering med basis i krav til akseptabel risiko til konfidensialitet, integritet, tilgjengelighet og kvalitet.

2.2.1 Risikovurdering før tilgang gis (Normen kap. 4.6)
"Risikovurdering skal som minimum gjennomføres før:

- det iverksettes *behandling* av *helse- og personopplysninger*
- etablering av nye informasjonsbehandlingssystemer eller registre som inneholder *helse- og personopplysninger*
- det iverksettes organisatoriske endringer som kan påvirke informasjonsbehandlingen
- det iverksettes tekniske endringer i utstyr og/eller programvare som kan påvirke informasjonsbehandlingen
- det iverksettes andre endringer med betydning for informasjonssikkerheten

Risikovurderingen skal dokumenteres. Dersom teknologiske tiltak for å oppnå akseptabel risiko ikke innføres umiddelbart, kan det i en overgangsperiode benyttes administrative tiltak, f.eks. i form av prosedyrer."

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Virksomheten skal sørge for at det gjennomføres en risikovurdering av den totale løsningen som benyttes før *leverandøren* gis *tilgang*. Som basis for risikovurderingen skal *virksomhetenes* krav til akseptabel risiko til konfidensialitet, integritet, tilgjengelighet og kvalitet legges til grunn. Risikovurderingen skal dokumenteres. En forenklet risikovurdering kan gjøres ved hjelp av skjemaet i vedlegg (kapittel 5.2). Det er ikke nødvendig å gjennomføre en ny risikovurdering av fjernaksessløsningen for hver ny *leverandør* som tilknyttes.	Risikovurdering som er gjennomført av *leverandøren* kan være tilstrekkelig dokumentasjon på at risikovurdering er gjennomført. Som basis for risikovurderingen skal *virksomhetenes* krav til akseptabel risiko til konfidensialitet, integritet, tilgjengelighet og kvalitet legges til grunn. Risikovurdering fra *leverandøren* kan danne grunnlag for risikovurderingen som *virksomheten* skal gjennomføre.	Faktaark nr 7 – Risikovurderinger Faktaark nr 5 - Fastsettelse av akseptkriterier for tilgjengelighet, konfidensialitet og integritet

2.2.2 Risikovurdering i driften (Normen kap. 6.2)

"Virksomhetens ledelse skal også jevnlig gjennomføre risikovurderinger for å kartlegge risikoområder og klarlegge sannsynlighet for og konsekvens av uønskede hendelser"

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Virksomheten bør etablere en plan for gjennomføring av risikovurderinger. Planen bør dekke *fjernaksess* slik at gjeldende løsninger vurderes ift nivå for akseptabel risiko.	*Leverandøren* skal gjennomføre risikovurderinger iht. avtale med *virksomheten*.	Faktaark nr 7 - Risikovurderinger

2.3 Opplæring

I dette avsnittet beskrives krav til opplæring av *virksomhetens* medarbeidere og *leverandørens servicemedarbeidere*. Det presenteres også momenter til opplæringsplan.

2.3.1 Opplæringstiltak (Normen kap. 5.6)

"Virksomheten skal iverksette tiltak som ivaretar at:

- alle som gis *tilgang* til og/eller drifter informasjonssystemene og tilhørende informasjon skal ha tilstrekkelig kunnskap til å utnytte systemene for sin rolle og til å ivareta informasjonssikkerheten.

Kompetansebygging må skje kontinuerlig og være tilpasset de ulike roller og brukergrupper. Særskilte opplæringstiltak må vurderes for nyansatte og ved endringer i informasjonssystemene eller i *behandlingen* av *helse- og personopplysninger."*

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Virksomheten skal lære opp egne medarbeidere i den tekniske løsningen og prosedyrene som skal benyttes ifm med *fjernaksess*. Opplæringen må også ivareta kompetanse i å overvåke bruk av løsningen og oppfølging av hendelsesregistre. Alle *virksomheter* skal ha en minimumskunnskap om egen fjernaksessløsningen. Dette gjelder spesielt hva *servicemedarbeider* kan utføre på teknisk utstyr som benyttes til *behandling* av *helse- og personopplysninger*. Opplæringen bør bl.a. dekke: a) Kontroll med bruk av fjernaksessløsning b) Oppfølging av hendelsesregistre c) Tildeling og tilbaketrekking av *autorisasjon* d) Avviksrapportering og -behandling	*Leverandøren* skal lære opp *servicemedarbeider* i bruk av fjernaksessløsningen og *taushetspliktens* innhold og omfang, fortrinnsvis gjennom en etablert opplæringsplan. Opplæringen bør bl.a. dekke: a) Teknisk løsning b) Bruk av fjernaksessløsningen c) Autentiseringsløsning d) e) Lagring av datafiler fra ulike *virksomheter* f) Oppfølging av hendelsesregistre g) Avviksrapportering h) Sporbarhet på endringene *leverandørene* gjør	Faktaark 9 – Opplæring av ledere og medarbeidere Faktaark 3 – Oversikt over anbefalte prosedyrer i styringssystemet

2.4 Oppkobling og begrensning av trafikk

I dette avsnittet beskrives i hovedsak krav til den tekniske løsningen ved oppkobling av *fjernaksess,* gjennom *helsenettet* eller utenfor. For feilsøking gjelder det særskilte regler som er omtalt i kapittel 2.4.2

2.4.1 Nettjenesteleverandør (Normen kap. 5.7)

"Når det benyttes datakommunikasjon skal hver enkelt *virksomhet* enten selv ivareta de påfølgende krav, eller sørge for at de som utfører oppgaven / leverer tjenesten ivaretar kravene.

All kommunikasjon med *virksomheter*/tjenester utenfor *virksomheten* bør fortrinnsvis foregå ved hjelp av en kanal, dvs. én nettjenesteleverandør. Dersom det benyttes flere nettjenesteleverandører mot systemer hvor det behandles *helse- og personopplysninger* må alle tilfredsstille kravene."

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Fjernaksess for vedlikehold og oppdateringer bør gå gjennom *helsenettet*.	*Leverandøren* må etablere en fjernaksessløsning som oppfyller kravene i Normen.	Faktaark 28 – Alternative tekniske løsninger for primærhelsetjenesten

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Selv om oppkoblingen skjer gjennom *helsenettet* har *virksomheten* et selvstendig ansvar for at det etableres sikker fjernaksess i egen *virksomhet*. *Norsk helsenett* kan stille krav, gjennom avtalebetingelsene, at samtidig *tilgang* til andre nett enn *helsenettet* må godkjennes av *Norsk Helsenett Virksomheten* har ansvaret for at denne godkjennelsen innhentes. Hensikten med "en kanal" er å sikre bedre oversikt og kontroll med kommunikasjonsløsninger når det er kun en nettjenesteleverandør.	*Leverandøren* står fritt til å velge kommunikasjon gjennom *helsenettet*, men må forholde seg til løsningen og krav i *virksomheten*.	Faktaark 36 – *Fjernaksess* for vedlikehold og oppdateringer Veileder i informasjons-sikkerhet ved tilknytning mellom kommuner, fylkeskommuner og *helsenettet*

2.4.2 Begrensning av trafikk (Normen kap. 5.7.1)

"Ved tilkobling til nett utenfor *virksomheten* skal det etableres *tekniske tiltak* som ivaretar at:

- Kun eksplisitt angitt tillatt trafikk kan passere, annet stoppes.
- Trafikk kan ikke passere direkte utenfra og inn; all slik ekstern trafikk må initieres fra *virksomhetens* systemer.

Hendelsesregistrering iverksettes for å kontrollere at regler ikke brytes; ved brudd stenges kanalen inntil ny sikker løsning finnes."

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Virksomheten skal påse at de *tekniske tiltakene* ivaretas i løsningen. I situasjoner der det åpnes opp for mer enn det avtalen bestemmer, f.eks. i situasjoner for å teste ut løsningen ved oppkobling eller ved feilsøkning og feilretting, kan det unntaksvis åpnes opp for mer trafikk. Ved slike tilfeller bør den utvidede *tilgangen* (åpningen) tidsbegrenses. Når den midlertidige oppkoblingen er aktivisert, bør denne aktivt overvåkes av *virksomheten* og all trafikk loggføres. Når problemstillingen er løst, skal åpningen for den aktuelle trafikken umiddelbart stenges og eventuelle tilleggsautorisasjoner slettes. Med "direkte utenfra og inn" menes at trafikken må passere passere via en sikkerhetsmekanisme (for eksempel proxytjeneste eller terminalserver). .	*Leverandøren* skal påse at de *tekniske tiltakene* ivaretas i løsningen.	Faktaark 15 – *Hendelsesregistrering* og oppfølging Faktaark 22 – Kontroll og sikring a ekstern *tilgang* Faktaark 24 – Kommunikasjon over åpne nett

2.5 Kryptering av ekstern kommunikasjon

I dette avsnittet beskrives krav til kryptering som virkemiddel for konfidensialitetssikring.

2.5.1 Krypteringsløsning (Normen kap. 5.4.4)
"Sikkerhetstiltak skal hindre at personer som ikke er *autoriserte* får *tilgang* til *helse- og personopplysninger* ved at:

- All kommunikasjon, enten dette skjer ved hjelp av trådløst samband eller ved hjelp av linjer sikres ved kryptering iht. Datatilsynets til enhver tid gjeldende anbefalinger."[1]

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Virksomheten må sørge for at kommunikasjonen mellom *leverandør* og *virksomhet* krypteres. Krypteringen skal gjøres fra *leverandørens* sikre nettverkssone til *virksomhetens* nettverkssone hvor *helse- og personopplysninger* behandles. Ved stans i krypteringsløsningen mellom *leverandøren* og *virksomheten* skal kommunikasjonen skrus av og det skal sendes melding til *leverandøren* om *avviket*. Videre kommunikasjon skal ikke være mulig før krypteringen er operativ igjen. Krypteringsstyrke som tilsvarer bruk av PKI eller virksomhetssertifikat iht gjeldende "Kravspesifikasjon for PKI i offentlig sektor" er tilfredsstillende. [2]	*Leverandøren* må dokumentere hvilken krypteringsløsning som benyttes og at den oppfyller kravene fastsatt i "Kravspesifikasjon for PKI i offentlig sektor".	Faktaark 24 – Kommunikasjon over åpne nett Faktaark 26 – Sikring av trådløs teknologi Faktaark 49 – Krav ved bruk av PKI ved ekstern kommunikasjon

2.6 Forhindre ondsinnet programvare

I dette avsnittet beskrives krav til å forhindre overføring av ondsinnet programvare mellom *virksomhet* og *leverandør*.

2.6.1 Løsning for ondsinnet programvare (Normen kap. 5.8.3)
"Virksomheten skal for å ivareta konfidensialitet, integritet, tilgjengelighet og kvalitet for *helse- og personopplysninger* forsikre seg om at:

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."

[1] For gjeldende anbefaling, se fotnote 2
[2] http://www.difi.no/artikkel/2010/04/kravspesifikasjon-for-pki

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Virksomheten skal ha løsning for å stanse og hindre overføring av ondsinnet programvare fra *leverandør* til eget nettverk og utstyr. Løsningen skal kontinuerlig oppdateres med nye *sikkerhetsoppdateringer*.	*Leverandøren* skal ha løsning som hindrer overføring av ondsinnet programvare fra eget nettverk eller utstyr til *virksomhetens* nettverk og utstyr. Løsningen skal kontinuerlig oppdateres med nye *sikkerhetsoppdateringer*.	Faktaark 19 – Tiltak for å hindre ondsinnet programvare

2.7 Adgang til og sikring av utstyr for fjernaksess

I dette avsnittet beskrives krav til sikring av områder slik at uautoriserte ikke får fysisk adgang til ustyr og løsninger med *helse- og personopplysninger*.

2.7.1 Adgangsregulering (Normen kap. 5.8.3)

"Leverandøren kun skal få *adgang* etter særskilt tillatelse fra *virksomheten* i hvert enkelt tilfelle, og kun *adgang* til de enheter hvor det er behov."

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Virksomheten skal etablere prosedyrer for adgangsregulering ved behov.	All *adgang* skal konkret vurderes i hvert enkelt tilfelle og kun gis ved tjenstlig behov	Faktaark –17 - Fysisk sikring av områder og utstyr

2.7.2 Fysiske sikkerhetstiltak (Normen kap. 5.4.2)

"Sikkerhetstiltak skal hindre at personer som ikke er *autoriserte* får *tilgang* til *helse- og personopplysninger* – enten ved adgangsregulert kontroll av lokaler med utstyr, eller ved at utstyret sikres mot misbruk og skjermer, utskrifter mv. skjermes mot uautorisert innsyn."

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Utstyr som er plassert hos *virksomheten* må sikres mot misbruk og uautorisert innsyn.	*Leverandøren* må påse at utstyr som har aktive oppkoblinger til *fagsystemer* blir betryggende sikret slik at uautoriserte ikke får *adgang* til løsningen og derigjennom *tilgang* til *helse- og personopplysninger*. For eksempel låsing av arbeidsstasjon når arbeidsplassen forlates. Dataskjermer må sikres mot innsyn fra uautoriserte. *Leverandøren* må etablere prosedyre for håndtering av eventuelle utskrifter for innsyn fra uautoriserte.	Faktaark 17 - Fysisk sikring av områder og utstyr

2.8 Autorisasjon

I dette avsnittet beskrives krav til autorisasjon av *leverandørens servicemedarbeider som skal ha tilgang*. I avsnittet beskrives også krav til et *autorisasjonsregister*.

2.8.1 Ansvar for å tildele autorisasjon (Normen kap. 5.2.2)

"Databehandlingsansvarlig er ansvarlig for at *autorisasjoner* tildeles, administreres og kontrolleres."

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Ved tildeling av *autorisasjon* skal lovbestemt *taushetsplikt* vurderes og ivaretas. *Servicemedarbeidere* som har ulike roller ifm. *fjernaksess* skal *autoriseres* for hver rolle uavhengig av vedkommendes øvrige roller.	*Leverandøren* kan ikke overstyre *autorisasjoner* gjort av *virksomheten* for eksempel ved å gi seg selv *autorisasjoner* ved bruk av *administratorrettigheter*.	Faktaark 14 - Tilgangsstyring

2.8.2 Prosedyre for tildeling av autorisasjon (Normen kap. 5.2.2)

"Det skal etableres prosedyre for tildeling og administrasjon av tilgangsrettigheter."

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Prosedyren for tildeling av *autorisasjoner* for interne systemer skal ivareta: • Lovbestemt *taushetsplikt* skal vurderes og overholdes • Kun teknisk personell med særskilt behov for *tilgang*, kan *autorisere* for større mengder *helse- og personopplysninger*. Det skal iverksettes tiltak slik at mulig misbruk skal kunne avdekkes	*Leverandøren* skal ha prosedyre for å tildele og trekke tilbake *autorisasjon* for *tilgang* til utstyr og programvare som benyttes til *fjernaksess*. *Autorisasjon* skal kun gis iht. de konkrete oppgaver den enkelte *servicemedarbeider* hos *leverandøren* skal utføre. Det skal kun gis *autorisasjon* til *servicemedarbeider* som har signert taushetserklæring. Det er ikke anledning å tildele felles *autentisering* til en gruppe *servicemedarbeidere*. Alle *servicemedarbeidere* skal ha unik *autentisering* til utstyr som benyttes til *fjernaksess*.	Faktaark 14 - Tilgangsstyring

2.8.3 Autorisasjonsregister (Normen kap. 5.2.2)

"Databehandlingsansvarlig skal sørge for at det oppettes et *autorisasjonsregister* Registeret skal som minimum inneholde:

- informasjon om hvem som er tildelt *autorisasjon*
- til hvilken rolle autorisasjonen er tildelt
- formålet med *autorisasjonen*

- tidspunkt for når *autorisasjonen* ble gitt og eventuelt tilbakekalt
- informasjon om hvilken *virksomhet* den *autoriserte* er knyttet til

Oversikt over tildelte *autorisasjoner* skal lagres i minimum 5 år fra det tidspunkt *autorisasjonen* ble trukket tilbake. ”

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Virksomheten skal føre *autorisasjonsregister* for *virksomhetens* egne systemer iht. kravet.	Det anbefales at *leverandøren* fører *autorisasjonsregister* for *leverandørens* og eventuelt underleverandørens løsning for *fjernaksess*. Oppbevaringskravet på 5 år gjelder også ved opphør av avtalen. Opplysningene i *autorisasjonsregisteret* skal være tilgjengelig for *virksomheten*.	Faktaark 47 - *Autorisasjonsregister*

2.9 Autentisering og tilgang

I dette avsnittet beskrives krav til *autentisering* på *sikkerhetsnivå 4* og generell *autentisering* til *fagsystemer*. Avsnittet dekker også bruk av brukerkontoer, herunder bruk av administratorrettigheter. Det er ikke fastsatt hvor autentisering på sikkerhetsnivå 4 skal utføres.

2.9.1 Autentisering med sikkerhetsnivå 4 (Normen kap. 5.2.1)

”Ved bruk av mobilt utstyr, hjemmekontor og trådløs kommunikasjon skal *autentiseringen* ikke innebære større risiko enn for stasjonært utstyr og *autentisering* på *sikkerhetsnivå 4* må benyttes.”

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Oppkobling med *fjernaksess* til systemer med helse- og personopplysinger vil falle inn under dette kravet. Om *virksomheten* ikke har løsning med bruk av PKI som tilfredsstiller *sikkerhetsnivå 4* skal en slik teknisk løsning etableres og prosedyrer utarbeides.	*Leverandørens servicemedarbeider* med norsk fødselsnummer eller D-nummer må bestille elektronisk identitet fra den *leverandør virksomheten* benytter. Elektronisk ID er personlig og må bestilles for hver av *servicemedarbeiderne* som skal benytte løsningen for *fjernaksess* mot *virksomheten*. *Servicemedarbeidere* uten norsk fødselsnummer eller D-nummer vil ha vanskeligheter med å anskaffe et Norsk deklarert sertifikat. I den sammenheng har Eu-kommisjonen fastsatt at det enkelte EU/EØS-land skal etablere, vedlikeholde og publisere en TL-liste (Trusted List) som inneholder nødvendig informasjon relatert til utstedere av sikkerhetsnivå 4 under tilsyn av det aktuelle landet (jf. lenke til høyre i tabellen)	Faktaark 49 - Krav ved bruk av PKI ved ekstern kommunikasjon http://www.npt.no/portal/page/portal/PG_NPT_NO_NO/PAG_NPT_NO_HOME/PAG_NPT_NO_TEKSTVISNING?p_d_i=-121&p_d_c=&p_d_v=114520

2.9.2 Tilgangstyring (Normen kap. 5.2.3)

”Bare autorisert personell kan få *tilgang* til *helse- og personopplysninger.”*

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Tilgang til *fagsystemer* skal gis på bakgrunn av beslutninger om tjenstlig behov. *Virksomheten* skal sikre at taushetspliktreglene overholdes.	*Tilgang* skal styres slik at taushetspliktreglene ivaretas og at *tilgang* til *helse- og personopplysninger* ikke gis til uautoriserte.	Faktaark 14 – Tilgangsstyring

2.9.3 Bruk av autorisasjon (Normen kap. 5.5.2)

”Tekniske tiltak og organisatoriske tiltak skal iverksettes slik at personer ikke skal kunne få *tilgang* til *helse- og personopplysninger* de ikke er autorisert for.”

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Tilgang basert på *sikkerhetsnivå 4* vil gi tilstrekkelig konfidensialitetsbeskyttelse for *tilgang* til det enkelte system. *Virksomheten* bør ta inn i avtalen for *fjernaksess* at tilganger og autentiseringsmekanismer er personlige og skal ikke lånes ut til andre *servicemedarbeidere*.	*Leverandøren* må lære opp *servicemedarbeiderne* i riktig bruk av autentiseringsmekanismene. *Administratorrettighet* til utstyr i *virksomheten* bør som hovedregel ikke tildeles *servicemedarbeider*. Det kan likevel aksepteres under forutsetning at *virksomheten* har godkjent *servicemedarbeideren* og godkjenner den enkelte oppkobling for *fjernaksess*.	Faktaark 14 - Tilgangsstyring

2.10 Behandling av helse- og personopplysninger hentet fra virksomheten

I dette avsnittet beskrives krav i tilfeller hvor leverandøren skal overføre *helse- og personopplysninger* fra *virksomheten* til *leverandøren*. Avsnittet beskriver også overføring av *helse- og personopplysinger* til utlandet.

2.10.1 Overføring av helse- og personopplysninger til leverandør (Normen kap. 5.8.2)

”Databehandler har et selvstendig ansvar for informasjonssikkerhet etter helseregisterloven § 16 og personopplysningsloven § 13. I avtalen må sikkerhetsforhold reguleres konkret. *Databehandlerens* selvstendige plikt til å etterleve helseregisterloven § 16 og personopplysningsforskriften kap. 2 må presiseres. I tillegg skal det stilles kriterier for akseptabel risiko hos *databehandleren*, samt at *databehandlingsansvarlig* skal sikres innsynsrett for å forsikre seg om at kravene etterleves.”

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Når *leverandøren* laster ned data med helse- og personopplysninger fra *virksomheten* skal det etableres en databehandleravtale med *leverandøren* før overføring finner sted. Under referanse fins det maler og veiledning til databehandleravtale. Faktaark 10 innehar også en mal. Disse malene må tilpasses den aktuelle situasjonen. En databehandleravtale kan gjelde et lengre tidsrom. Formål og hva som kan overføres skal beskrives i avtalen. Databehandleravtalen kan være et vedlegg til avtalen om *fjernaksess*.	Data med helse- og personopplysninger kan ikke behandles på annen måte enn hva databehandleravtalen beskriver. Datafiler som inneholder *helse- og personopplysninger* og som hentes fra *virksomheten* for feilsøking skal kun behandles av autorisert *servicemedarbeider*. Om det er mulig å anonymisere helse- og personopplysningene anbefales dette. Om data blir pseudonymisert gjelder Normen fult ut som for identifiserbare *helse- og personopplysninger*. Datafiler skal kun lagres på utstyr hos *leverandør* som har installert nødvendige *tekniske tiltak* for å hindre at personer uten *autorisasjon* får *tilgang* til *helse- og personopplysninger*. Datafiler skal slettes etter avtale mellom partene når formålet med henting av datafilene er oppfylt. Dette gjelder også eventuelle sikkerhetskopier	Faktaark 10 - Bruk av *databehandler* (ekstern driftsenhet) Maler fra Datatilsynet: http://www.datatilsynet.no/Sikkerhet-internkontroll/Databehandleravtale/ Om anonymisering og pseudonymisering vises det til veileder: Personvern og informasjons-sikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren For sikker sletting av data se: www.nsm.stat.no

2.10.2 Overføring av helse- og personopplysninger til utlandet (Normen kap. 1.0)

”Normen er utviklet med basis i personopplysningslovens regler om bransjevise adferdsnormer (jf. personopplysingsloven § 42 tredje ledd nr. 6). Disse reglene bygger i sin tur på EU-direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med *behandling* av personopplysninger og om fri utveksling av slike opplysninger. Direktivet er implementert i norsk lovgivning med grunnlag i Norges forpliktelser etter EØS-avtalen.”

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Personopplysninger kan overføres til land innen EU og EØS-området, når det er avtalt mellom *virksomhet* og *leverandør*. De kan også overføres til land som Europakommisjonen har godkjent, samt enkeltbedrifter i USA som har sluttet seg til Safe Harbor. En *virksomhet* kan også overføre *helse- og personopplysninger* til andre land dersom Europakommisjonen har funnet at landet har et tilstrekkelig beskyttelsesnivå. Den enkleste måten å overføre *helse- og personopplysninger* til andre land på, er å bruke standardkontraktene EU har laget.	Det er et krav at *leverandøren* bare kan overføre helse- og personopplysinger til en målrettet adresse. Med adresse menes til et spesifisert fysisk sted og til en eller flere spesifiserte fysisk(e) datamaskin(er). *Leverandøren* må kunne dokumentere eierskap til adresse som ligger utenfor EU/EØS- området.	Se Datatilsynets nettsted www.datatilsynet.no for blanketter og prosedyrer

2.10.3 Skille helse- og personopplysninger fra flere virksomheter (Normen kap. 5.8.2)
"Dersom *databehandler* behandler *helse- og personopplysninger* fra flere *virksomheter* skal *databehandler* ved hjelp av *tekniske tiltak* som ikke kan overstyres av brukerne ivareta at: det er etablert skiller mellom *virksomhetene* i henhold til gjennomført risikovurdering."

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Påse at forholdet er ivaretatt gjennom avtalen om *fjernaksess*.	*Leverandøren* skal etablere løsning iht avtale om *fjernaksess*. Kravet er at data med helse- og personopplysinger skal være logisk adskilte fra øvrige kunder og *leverandørens* interne nettverk forøvrig. Det er ikke tilstrekkelig å adskille data ved hjelp av kun autentiseringsløsninger. For eksempel skal ansatte fra en juridisk enhet ikke få *tilgang* til en annen juridisk enhets *helse- og personopplysninger* ved kjennskap til bruker-ID og passord. Risikovurdering skal dokumentere hvilke tiltak som skal benyttes.	

2.11 Fjernadministrasjon

I dette avsnittet beskrives konfigurasjon og bruk av løsning for fjernadministrasjon.

2.11.1 Konfigurasjonskontroll (Normen kap. 5.5.1)
"Konfigurasjonskontroll skal reguleres gjennom avtale ved bruk av fjernaksess for vedlikehold og oppdateringer"

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Bruk av *fjernadministrasjon* skal avtales med *leverandøren*. Avtalen skal beskrive hvordan konfigurasjonskontrollen blir ivaretatt. Verktøyet som benyttes skal ha aktiv konfigurasjonsstyring som ikke kan overstyres av servicemedarbeideren. Ved bruk av verktøy for *fjernadministrasjon* skal *virksomheten* konfigurere løsningen slik at *leverandøren* ikke kan benytte andre funksjoner enn de som er avtalt på forhånd. Oppkobling og bruk av verktøy for *fjernadministrasjon* bør som hovedprinsipp aksepteres fra *virksomheten* som en aktiv handling i det enkelte tilfelle.	*Leverandøren* skal forholde seg til den *konfigurasjonen* som er avtalt og prosedyre for endringshåndtering. *Leverandøren* skal kun benytte løsningen for *fjernaksess* slik det er avtalt på forhånd.	

2.12 Krav til hendelsesregistrering

I dette avsnittet beskrives krav til *hendelsesregistrering* på alle komponenter/løsninger som benyttes ifm. *fjernaksess*.

2.12.1 Hendelsesregistrering (Normen kap. 5.5.2)
"For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres hendelsesregistre over følgende:

- Autorisert bruk av informasjonssystemene skal registreres.
- Sikkerhetsbarrierene skal registrere sikkerhetsrelevante hendelser, bl.a. forsøk på uautorisert bruk av informasjonssystemet
- Nettverksoperativsystemer skal registrere alle forsøk på uautorisert bruk.
- Alle informasjonssystemer skal registrere alle forsøk på uautorisert bruk.
- Bruk av nødrettstilgang til behandlingsrettet helseregister skal registreres.
- Hendelsesregistrene skal sikres mot endring og sletting av uautorisert personell.

Følgende skal som minimum registreres i hendelsesregistre:

- entydig identifikator for den *autoriserte* brukeren
- rollen den *autoriserte* brukeren har ved *tilgangen*
- virksomhetstilhørighet
- organisatorisk tilhørighet til den som er autorisert
- hvilke type opplysninger det er gitt *tilgang* til
- grunnlaget for *tilgangen*
- tidspunkt og varighet for *tilgangen"*

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Det skal iverksettes *hendelsesregistrering*, slik at det er mulig å oppdage og oppklare brudd på sikkerheten. I *virksomhetens* systemer og nettverk skal følgende hendelsesregistreres ved autorisert bruk: • entydig identifikator for den *autoriserte* brukeren • rollen den *autoriserte* brukeren har ved *tilgangen* • virksomhetstilhørighet • organisatorisk tilhørighet til den som er autorisert • hvilke type opplysninger det er gitt *tilgang* til • grunnlaget for *tilgangen* • tidspunkt og varighet for *tilgangen* Ved fjernakses fra *leverandør* skal følgende i tillegg hendelsesregistreres: • Initiert trafikk mot IP-adresser og portnummer • Hvilke data/datafiler som er lastet ned til *leverandøren* (datafiler) eller opp til *virksomheten* (programfiler	Hele eller deler av *hendelsesregistreringen* kan etter avtale ivaretas av *leverandøren*. Hendelsregisteret kan være summen av *leverandørens hendelsesregister* og *virksomhetens hendelsesregister*.	Faktaark 15 – Hendelsesregistrering og oppfølging

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
og patcher) • Entydig identifikator for den hos *leverandør* som har benyttet den aktuelle *fjernaksess* For forsøk på uautorisert bruk skal følgende hendelsesregistreres: • Brukeridentiteten som ble benyttet • Tidspunkt (dato og klokkeslett) • IP-adresse eller annen identifikasjon av PC/arbeidsstasjon som ble benyttet (for eksempel MAC-adresse eller NAT-adresse)		

2.13 Krav til gjennomgang av hendelsesregistre

I dette avsnittet beskrives krav til gjennomgang av og oppbevaringstid for *hendelsesregistre*.

2.13.1 Gjennomgang av hendelsesregistre (Normen kap. 5.2.6)
"All autorisert bruk og forsøk på uautorisert bruk av informasjonssystemene skal registreres og registeret skal lagres i minimum 2 år. *Hendelsesregistrene* skal enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd.

Det skal etableres prosedyrer for å analysere *hendelsesregistrene* slik at hendelser oppdages før de får alvorlige konsekvenser, og fortrinnsvis innen 1 uke."

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Virksomheten må utarbeide skriftlig prosedyre for gjennomgang av de ulike *hendelsesregistre*. Alle hendelsesregistre skal oppbevares i minst 2 år i elektronisk form. Avtalen mellom *virksomhet* og *leverandør* skal ivareta analyse av *hendelsesregistre*. Det er spesielt viktig å sikre hendelsesregistre i *fagsystemene* med hensyn til at *leverandøren* kan ha *tilgang* til disse i forbindelse med annet systemarbeid i *virksomheten*. Om det avdekkes uautoriserte hendelser skal det umiddelbart sendes en avviksmelding til *leverandøren*.	*Leverandøren* må utarbeide skriftlig prosedyre for gjennomgang av de ulike *hendelsesregistrene*. Alle hendelsesregistre skal oppbevares i minst 2 år i elektronisk form. Avtalen mellom *virksomhet* og *leverandør* skal ivareta analyse av *hendelsesregistre*. Om det avdekkes uautoriserte hendelser skal det umiddelbart sendes en avviksmelding til *virksomheten*.	Faktaark 15 – Hendelsesregistrering og oppfølging Faktaark 3 – Oversikt over anbefalte prosedyrer i styringssystemet

2.14 Analyseverktøy

I dette avsnittet beskrives anbefalinger om bruk av dataverktøy for analyse av *hendelsesregistrene*.

2.14.1 Analyse av hendelsesregistre (Normen kap. 5.5.2)
"Alle hendelsesregistre skal kunne analyseres ved hjelp av egnet verktøy og ved behov sammenholdes med *autorisasjonsregister* og tilstedeværelsesregister."

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Virksomheten bør anvende analyseverktøy for gjennomgang av hendelsesregistre.	*Leverandøren* bør anvende analyseverktøy for gjennomgang av hendelsesregistre.	Faktaark 15 – Hendelsesregistrering og oppfølging

2.15 Tilgang til hendelsesregistre hos leverandør

I dette avsnittet beskrives krav til at *virksomheten* skal ha *tilgang* til *leverandørens hendelsesregistre*.

2.15.1 Innsyn i leverandørens hendelsesregistre (Normen kap. 5.3.4)
"Det skal etableres prosedyrer for å sikre at den registrertes rettigheter for innsyn i hendelsesregistre blir ivaretatt."

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Virksomheten skal gjennom avtalen med *leverandøren* ha *tilgang* til hendelsesregistre hos *leverandøren*. Det må i avtalen fremkomme på hvilken måte det skal skje.	*Leverandøren* skal etablere prosedyre for å sikre at *virksomheten* og den registrerte får *tilgang* til hendelsesregistre.	Faktaark 50 – Innsyn i hendelsesregistre Faktaark 3 – Oversikt over anbefalte prosedyrer i styringssystemet

3 TEKNISKE LØSNINGER

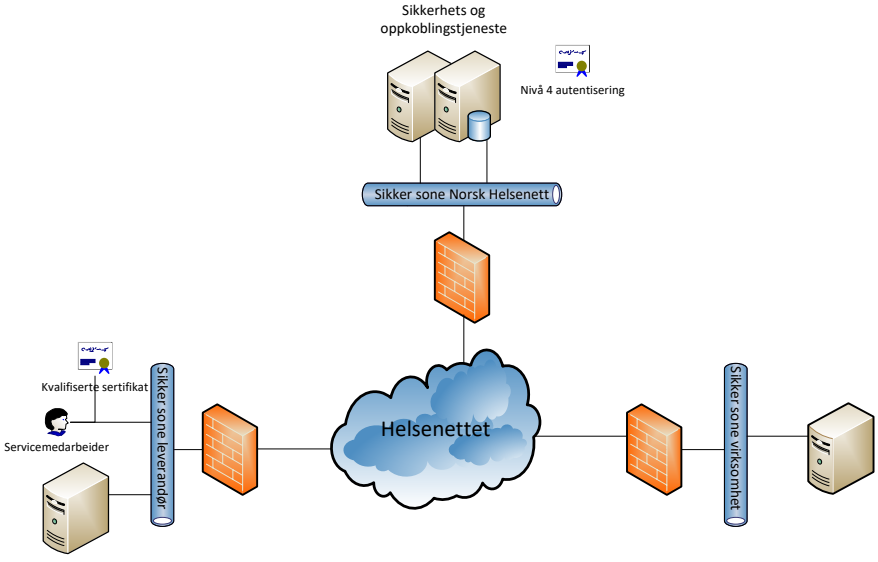
I dette kapitlet beskrives forslag til tekniske løsninger som oppfyller kravene i Normen. Veilederen viser et utvalg løsninger, men det kan være andre løsninger som oppfyller kravene.

Eksemplene nedenfor viser i hovedsak løsninger der *leverandøren* kobler seg opp til *virksomheten* med *fjernaksess*. Det er en rekke løsninger som selv automatisk initierer kontakt med *leverandørens tekniske løsning* (for eksempel for rapportering om status på informasjonssystemer og infrastruktur, oversendelse av feilmeldinger mv.). På bakgrunn av en slik kontakt kan *leverandøren* initiere oppkobling med *fjernaksess*. Selve løsningen for automatisk kontakt beskrives ikke i eksemplene. Slike løsninger bør betraktes som ethvert informasjonssystem i *virksomheten*, som har en forbindelse til eksterne nett.

3.1 Eksempel 1 - løsning levert av Norsk Helsenett

Eksempelet under viser bruk av verktøy for *fjernadministrasjon* levert av *Norsk Helsenett*. Figuren illustrerer at:

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



Tabellen nedfor viser hvem som ivaretar sikkerhetsoppgavene i dette eksempelet (Kap nr og Kapittel tittel er fra dette dokumentet):

Kap nr	Kapittel tittel	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.1.1	Skriftlig avtale med leverandør (Normen kap. 5.8)	☒	☒	☐
2.1.2	Taushetserklæring (Normen kap. 5.8.3)	☒	☐	☐
2.1.3	Sikkerhetsrevisjon og avviksbehandling (Normen kap. 5.8.3, 6.1 og 6.3)	☒	☐	☐
2.1.4	Bevisstgjøring av taushetsplikten (Normen kap. 5.1)	☒	☐	☐
2.2.1	Risikovurdering før tilgang gis (Normen kap. 4.6)	☒	☒	☐
2.2.2	Risikovurdering i driften (Normen kap. 6.2)	☐	☒	☐
2.3.1	Opplæringstiltak (Normen kap. 5.6)	☐	☒	☐
2.4.1	Nettjenesteleverandør (Normen kap. 5.7)	☐	☒	☐
2.4.2	Begrensning av trafikk (Normen kap. 5.7.1)	☐	☒	☐
2.5.1	Krypteringsløsning (Normen kap. 5.4.4)	☐	☒	☐
2.6.1	Løsning for ondsinnet programvare (Normen kap. 5.8.3)	☐	☒	☐
2.7.1	Adgangsregulering (Normen kap. 5.8.3)	☐	☒	☐
2.7.2	Fysiske sikkerhetstiltak (Normen kap. 5.4.2)	☐	☒	☐
2.8.1	Ansvar for å tildele autorisasjon (Normen kap. 5.2.2)	☒	☐	☐
2.8.2	Prosedyre for tildeling av autorisasjon (Normen kap. 5.2.2)	☒	☒	☐
2.8.3	Autorisasjonsregister (Normen kap. 5.2.2)	☒	☐	☐
2.9.1	Autentisering med sikkerhetsnivå 4 (Normen kap. 5.2.1)	☐	☒	☐
2.9.2	Tilgangstyring (Normen kap. 5.2.3)	☒	☒	☐
2.9.3	Bruk av autorisasjon (Normen kap. 5.5.2)	☐	☒	☐
2.10.1	Overføring av helse- og personopplysninger til leverandør (Normen kap. 5.8.2)	☐	☒	☐
2.10.2	Overføring av helse- og personopplysninger til utlandet (Normen kap. 1.0)	☐	☒	☐
2.10.3	Skille helse- og personopplysninger fra flere virksomheter (Normen kap. 5.8.2)	☐	☒	☐
2.11.1	Konfigurasjonskontroll (Normen kap. 5.5.1)	☐	☒	☐
2.12.1	Hendelsesregistrering (Normen kap. 5.5.2)	☐	☒	☐
2.13.1	Gjennomgang av hendelsesregistre (Normen kap. 5.2.6)	☒	☒	☐

Kap nr	Kapittel tittel	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.14.1	Analyse av hendelsesregistre (Normen kap. 5.5.2)	☒	☒	☐
2.15.1	Innsyn i leverandørens hendelsesregistre (Normen kap. 5.3.4)	☒	☐	☐

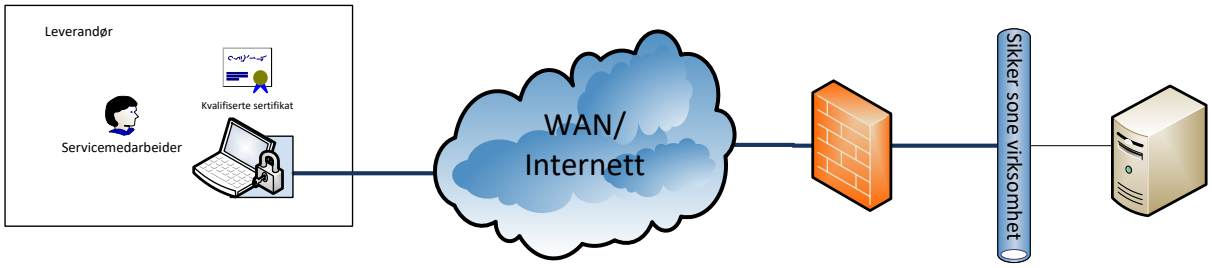
For oppgaver og roller vises det til tjenestebeskrivelsen av fjernaksessløsningen.

3.2 Eksempel på teknisk løsning - 2

Eksempelet under viser oppkobling over Internett der virksomheten har kontroll basert på VPN.

Figuren illustrerer at:

- Leverandøren får en PC av virksomhetene og benytter virksomhetens hjemmekontorløsning
- *Virksomheten* har kontroll på, eller 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 4*



Tabellen nedfor viser hvem som ivaretar sikkerhetsoppgavene i dette eksempelet (Kap nr og Kapittel tittel er fra dette dokumentet):

Kap nr	Kapittel tittel	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.1.1	Skriftlig avtale med leverandør (Normen kap. 5.8)	☒	☐	☐
2.1.2	Taushetserklæring (Normen kap. 5.8.3)	☒	☐	☐
2.1.3	Sikkerhetsrevisjon og avviksbehandling (Normen kap. 5.8.3, 6.1 og 6.3)	☒	☒	☐
2.1.4	Bevisstgjøring av taushetsplikten (Normen kap. 5.1)	☒	☒	☐
2.2.1	Risikovurdering før tilgang gis (Normen kap. 4.6)	☒	☐	☐

Kap nr	Kapittel tittel	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.2.2	Risikovurdering i driften (Normen kap. 6.2)	☒	☐	☐
2.3.1	Opplæringstiltak (Normen kap. 5.6)	☒	☐	☐
2.4.1	Nettjenesteleverandør (Normen kap. 5.7)	☒	☐	☐
2.4.2	Begrensning av trafikk (Normen kap. 5.7.1)	☒	☐	☐
2.5.1	Krypteringsløsning (Normen kap. 5.4.4)	☒	☐	☐
2.6.1	Løsning for ondsinnet programvare (Normen kap. 5.8.3)	☒	☐	☐
2.7.1	Adgangsregulering (Normen kap. 5.8.3)	☒	☐	☐
2.7.2	Fysiske sikkerhetstiltak (Normen kap. 5.4.2)	☐	☒	☐
2.8.1	Ansvar for å tildele autorisasjon (Normen kap. 5.2.2)	☒	☐	☐
2.8.2	Prosedyre for tildeling av autorisasjon (Normen kap. 5.2.2)	☒	☐	☐
2.8.3	Autorisasjonsregister (Normen kap. 5.2.2)	☒	☐	☐
2.9.1	Autentisering med sikkerhetsnivå 4 (Normen kap. 5.2.1)	☒	☐	☐
2.9.2	Tilgangstyring (Normen kap. 5.2.3)	☒	☐	☐
2.9.3	Bruk av autorisasjon (Normen kap. 5.5.2)	☒	☐	☐
2.10.1	Overføring av helse- og personopplysninger til leverandør (Normen kap. 5.8.2)	☒	☒	☐
2.10.2	Overføring av helse- og personopplysninger til utlandet (Normen kap. 1.0)	☒	☒	☐
2.10.3	Skille helse- og personopplysninger fra flere virksomheter (Normen kap. 5.8.2)	☒	☒	☐
2.11.1	Konfigurasjonskontroll (Normen kap. 5.5.1)	☒	☐	☐
2.12.1	Hendelsesregistrering (Normen kap. 5.5.2)	☒	☒	☐
2.13.1	Gjennomgang av hendelsesregistre (Normen kap. 5.2.6)	☒	☐	☐
2.14.1	Analyse av hendelsesregistre (Normen kap. 5.5.2)	☒	☐	☐
2.15.1	Innsyn i leverandørens hendelsesregistre (Normen kap. 5.3.4)	☒	☒	☐

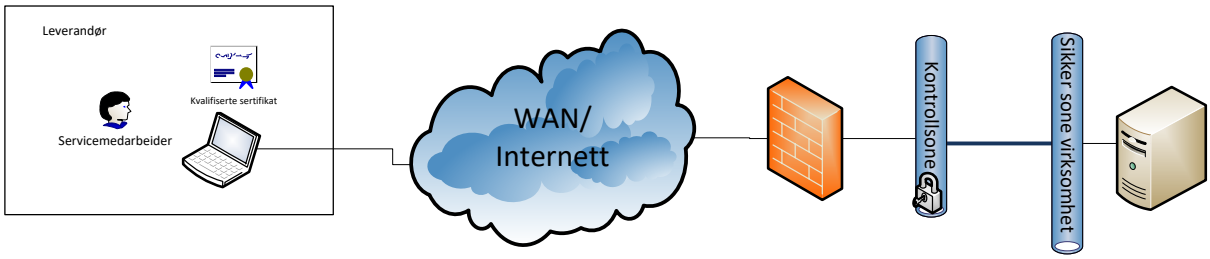
3.3 Eksempel på teknisk løsning - 3

Eksempelet under viser oppkobling over Internett basert på å håndtere sikkerhet i en kontrollsone, i virksomheten.

Figuren illustrerer at:

- Foretaket har ingen kontroll med leverandørens brukerutstyr

- All kommunikasjon foregår kryptert
- Foretaket har en kontrollsone som innehar nødvendige sikkerhetsmekanismer, og forhindrer direkte kommunikasjon fra leverandørens brukerutstyr til foretakets systemer. Eks. VDI/TS
- Tilgang til pasientdata krever at bruker identifiserer seg med sikkerhetsnivå 4



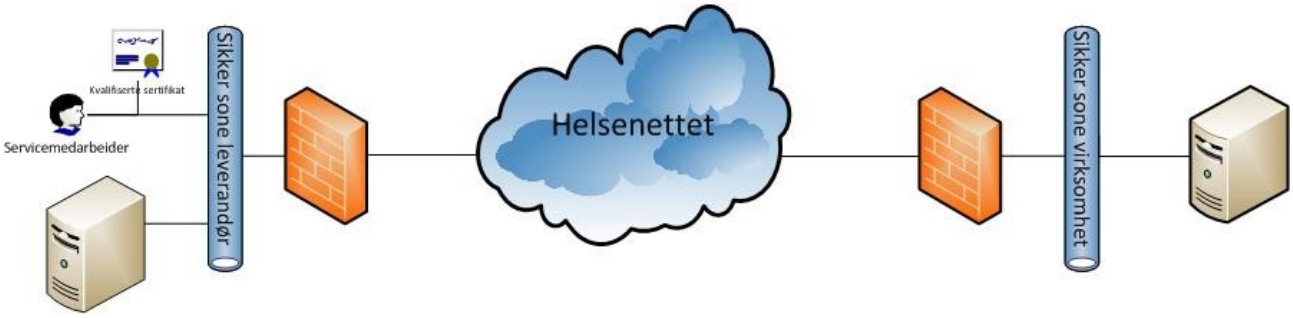
Tabellen nedfor viser hvem som ivaretar sikkerhetsoppgavene i dette eksempelet (Kap nr og Kapittel tittel er fra dette dokumentet):

Kap nr	Kapittel tittel	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.1.1	Skriftlig avtale med leverandør (Normen kap. 5.8)	☒	☐	☐
2.1.2	Taushetserklæring (Normen kap. 5.8.3)	☒	☐	☐
2.1.3	Sikkerhetsrevisjon og avviksbehandling (Normen kap. 5.8.3, 6.1 og 6.3)	☒	☒	☐
2.1.4	Bevisstgjøring av taushetsplikten (Normen kap. 5.1)	☒	☒	☐
2.2.1	Risikovurdering før tilgang gis (Normen kap. 4.6)	☒	☐	☐
2.2.2	Risikovurdering i driften (Normen kap. 6.2)	☒	☐	☐
2.3.1	Opplæringstiltak (Normen kap. 5.6)	☒	☐	☐
2.4.1	Nettjenesteleverandør (Normen kap. 5.7)	☒	☐	☐
2.4.2	Begrensning av trafikk (Normen kap. 5.7.1)	☒	☐	☐
2.5.1	Krypteringsløsning (Normen kap. 5.4.4)	☒	☐	☐
2.6.1	Løsning for ondsinnet programvare (Normen kap. 5.8.3)	☒	☐	☐
2.7.1	Adgangsregulering (Normen kap. 5.8.3)	☒	☐	☐
2.7.2	Fysiske sikkerhetstiltak (Normen kap. 5.4.2)	☐	☒	☐
2.8.1	Ansvar for å tildele autorisasjon (Normen kap. 5.2.2)	☒	☐	☐
2.8.2	Prosedyre for tildeling av autorisasjon (Normen kap. 5.2.2)	☒	☐	☐
2.8.3	Autorisasjonsregister (Normen kap. 5.2.2)	☒	☐	☐
2.9.1	Autentisering med sikkerhetsnivå 4 (Normen kap. 5.2.1)	☒	☐	☐
2.9.2	Tilgangstyring (Normen kap. 5.2.3)	☒	☐	☐

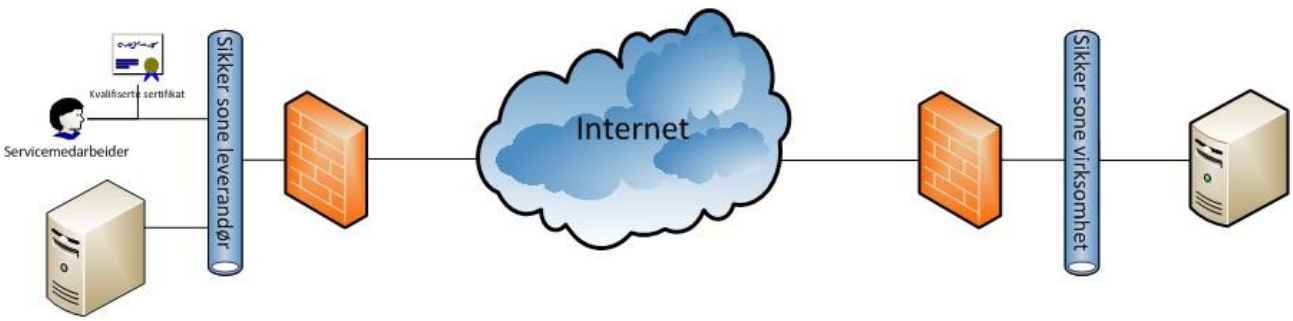
Kap nr	Kapittel tittel	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.9.3	Bruk av autorisasjon (Normen kap. 5.5.2)	☒	☐	☐
2.10.1	Overføring av helse- og personopplysninger til leverandør (Normen kap. 5.8.2)	☒	☒	☐
2.10.2	Overføring av helse- og personopplysninger til utlandet (Normen kap. 1.0)	☒	☒	☐
2.10.3	Skille helse- og personopplysninger fra flere virksomheter (Normen kap. 5.8.2)	☒	☒	☐
2.11.1	Konfigurasjonskontroll (Normen kap. 5.5.1)	☒	☐	☐
2.12.1	Hendelsesregistrering (Normen kap. 5.5.2)	☒	☒	☐
2.13.1	Gjennomgang av hendelsesregistre (Normen kap. 5.2.6)	☒	☐	☐
2.14.1	Analyse av hendelsesregistre (Normen kap. 5.5.2)	☒	☐	☐
2.15.1	Innsyn i leverandørens hendelsesregistre (Normen kap. 5.3.4)	☒	☒	☐

3.4 Eksempel på teknisk løsning - 4

Site-to-Site VPN løsning via Norsk Helsenett



Site-to-Site VPN løsning via Internet



Kommunikasjon mellom Leverandør og kunde skjer på en IPsec-sikret VPN forbindelse.

Kommunikasjonen kan gå enten via Norsk Helsenett eller via Internet.

Autentisering av Servicemedarbeider skjer med sikkerhetsnivå 4 hos leverandøren. F.eks PKI pålogging.

Eksempel på bruk:

1. Kunde melder feil på et system til en leverandør
Servicemedarbeider hos leverandør logger på systemet via leverandørens fjerndiagnosesystem. Denne påloggingen gir en begrenset tilgang til systemet. Ved hjelp av verktøy på systemet kan Servicemedarbeider så analysere feillogger. Etter noe analyse avdekkes at det må utføres en jobb på systemet. Kunde åpner så opp for utvidet tilgang slik at Servicemedarbeider 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 Servicemedarbeider 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 kundens systemet automatisk tilbake til Leverandørens fjerndiagnosesystem at oppdateringen er utført.

3. Proaktiv overvåking av viktige parametre
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 nedfor viser hvem som ivaretar sikkerhetsoppgavene i dette eksempelet (Kap nr og Kapittel tittel er fra dette dokumentet):

Kap nr	Kapittel tittel	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.1.1	Skriftlig avtale med leverandør (Normen kap. 5.8)	☐	☒	☐
2.1.2	Taushetserklæring (Normen kap. 5.8.3)	☐	☒	☐
2.1.3	Sikkerhetsrevisjon og avviksbehandling (Normen kap. 5.8.3, 6.1 og 6.3)	☒	☒	☐
2.1.4	Bevisstgjøring av taushetsplikten (Normen kap. 5.1)	☐	☒	☐
2.2.1	Risikovurdering før tilgang gis (Normen kap. 4.6)	☒	☒	☐
2.2.2	Risikovurdering i driften (Normen kap. 6.2)	☒	☒	☐
2.3.1	Opplæringstiltak (Normen kap. 5.6)	☐	☒	☐
2.4.1	Nettjenesteleverandør (Normen kap. 5.7)	☒	☐	☐
2.4.2	Begrensning av trafikk (Normen kap. 5.7.1)	☒	☒	☐
2.5.1	Krypteringsløsning (Normen kap. 5.4.4)	☐	☒	☐

Kap nr	Kapittel tittel	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.6.1	Løsning for ondsinnet programvare (Normen kap. 5.8.3)	☐	☒	☐
2.7.1	Adgangsregulering (Normen kap. 5.8.3)	☐	☒	☐
2.7.2	Fysiske sikkerhetstiltak (Normen kap. 5.4.2)	☐	☒	☐
2.8.1	Ansvar for å tildele autorisasjon (Normen kap. 5.2.2)	☐	☒	☐
2.8.2	Prosedyre for tildeling av autorisasjon (Normen kap. 5.2.2)	☐	☒	☐
2.8.3	Autorisasjonsregister (Normen kap. 5.2.2)	☐	☒	☐
2.9.1	Autentisering med sikkerhetsnivå 4 (Normen kap. 5.2.1)	☐	☒	☐
2.9.2	Tilgangstyring (Normen kap. 5.2.3)	☐	☒	☐
2.9.3	Bruk av autorisasjon (Normen kap. 5.5.2)	☐	☒	☐
2.10.1	Overføring av helse- og personopplysninger til leverandør (Normen kap. 5.8.2)	☒	☒	☐
2.10.2	Overføring av helse- og personopplysninger til utlandet (Normen kap. 1.0)	☒	☒	☐
2.10.3	Skille helse- og personopplysninger fra flere virksomheter (Normen kap. 5.8.2)	☐	☒	☐
2.11.1	Konfigurasjonskontroll (Normen kap. 5.5.1)	☐	☒	☐
2.12.1	Hendelsesregistrering (Normen kap. 5.5.2)	☐	☒	☐
2.13.1	Gjennomgang av hendelsesregistre (Normen kap. 5.2.6)	☒	☒	☐
2.14.1	Analyse av hendelsesregistre (Normen kap. 5.5.2)	☒	☒	☐
2.15.1	Innsyn i leverandørens hendelsesregistre (Normen kap. 5.3.4)	☒	☒	☐

4 AVTALER OG PROSEDYRER

4.1 Generelt om avtaler og prosedyrer

Det skal inngås skriftlig avtale mellom *virksomhet* og *leverandør*. Avtalene skal inkludere forpliktelser om at partene skal oppfylle de krav og tiltak som følger av den til enhver tid gjeldende Norm for informasjonssikkerhet, samt regulering av sanksjoner ved brudd på Normen og avtalen for øvrig.

Enkeltoppgaver skal dokumenteres i prosedyrer (se pkt 4.3 for hvilke prosedyrer som skal etableres).

4.2 Avtaler

Når *virksomheten* inngår avtale med *leverandøren* om vedlikehold og oppdateringer må det benyttes en avtaletype som har korrekt juridisk avtaletekst. I slike avtaler er det viktig at *virksomheten* påser at Normens krav ivaretas.

Anbefalte elementer i avtalen:

Nr	Element	Innarbeidet
1.	Hvem avtalepartene er	☐ Ja ☐ Nei
2.	Formålet med avtalen eller særavtalen	☐ Ja ☐ Nei
3.	Ansvarlige personer/roller	☐ Ja ☐ Nei
4.	*Virksomheten* skal ha tilgang til *leverandørens* dokumentasjon av sikkerhetsmål og strategi	☐ Ja ☐ Nei
5.	*Virksomheten* skal ha innsynsrett i *leverandørens* løsning for ivaretakelse av Normen	☐ Ja ☐ Nei
6.	*Virksomheten* skal ha rett til innsyn i *leverandørens* hendelsesregistre	☐ Ja ☐ Nei
7.	*Taushetsplikt* for *leverandørens* personale	☐ Ja ☐ Nei
8.	Hvilke prosedyrer som gjelder for *fjernaksess*løsningen	☐ Ja ☐ Nei
9.	Prosedyre for *avvik*sbehandling	☐ Ja ☐ Nei
10.	Konsekvenser ved brudd på avtalen	☐ Ja ☐ Nei
11.	Oversikt over hvilke systemer det gis *fjernaksess* til	☐ Ja ☐ Nei
12.	Beskrivelse av utstyr *leverandøren* kan benytte til *fjernaksess* og eierforholdet til utstyret	☐ Ja ☐ Nei
13.	Konsekvensutredning ved tilsiktet brudd under bruk av fjerntilkoblingen	☐ Ja ☐ Nei

4.3 Prosedyrer

Både *leverandør* og *virksomhet* skal etablere prosedyrer før *fjernaksess* opprettes. Prosedyrene skal være tilgjengelig for begge parter.

Relevante prosedyrer:

Nr	Element	Faktaark	Innarbeidet	Ansvar
1.	Signering av taushetserklæring og bekreftelse på at sikkerhetsinstruks er lest og akseptert		☐ Ja ☐ Nei	
2.	Opplæring av *servicemedarbeider*		☐ Ja ☐ Nei	
3.	Administrasjon av *autorisasjon* til utstyr som benyttes til *fjernaksess*	14	☐ Ja ☐ Nei	
4.	Bruk av løsning for sterk *autentisering*	24	☐ Ja ☐ Nei	
5.	Avviksbehandling ifm *fjernaksess*	8	☐ Ja ☐ Nei	
6.	*Hendelsesregistrering* og oppfølging av hendelsesregistre	15	☐ Ja ☐ Nei	
7.	Sletting av datafiler hentet fra *virksomheten*	34	☐ Ja ☐ Nei	
8.	Destruksjon av lagringsmedia ved utrangering	34	☐ Ja ☐ Nei	
9.	Oppgaver som kan utføres ved oppkobling /etablering av *fjernaksess* (se sjekkliste i pkt 5 Vedlegg)		☐ Ja ☐ Nei	
10.	Tildele *autorisasjon* til nettverk, utstyr og systemer		☐ Ja ☐ Nei	
11.	*Autentisering* av *servicemedarbeider* hos *leverandør*	14	☐ Ja ☐ Nei	
12.	Kontroll av tildelte *autorisasjoner*		☐ Ja ☐ Nei	
13.	Oppgaver som skal utføres ved oppkobling /etablering av *fjernaksess* (se sjekkliste i pkt 5 Vedlegg)		☐ Ja ☐ Nei	

Ifm opplæring kan følgende prosedyrer være relevante:

Nr	Prosedyre
1.	Konfigurasjonskontroll
2.	Bestilling, endring og sletting av brukerkontoer
3.	Oppretting og vedlikehold av *autorisasjonsregister*
4.	Hindre ødeleggende dataprogram
5.	*Hendelsesregistrering*
6.	Sletting av *helse- og personopplysninger*
7.	Bruk av bærbart datautstyr
8.	Krav til IKT-leverandører ifm *fjernaksess*
9.	Håndtering av flyttbare datalagringsmedier (internt hos *leverandør*)
10.	Bruk av trådløs teknologi
11.	Tilknytning av *leverandører* for *fjernaksess*
12.	Taushetserklæring og skjema for *autorisasjon* av *servicemedarbeider* til *fjernaksess*
13.	Avviksbehandling

5 VEDLEGG

5.1 Sjekkliste for etablering av oppkobling

Kap nr	Kapittel tittel	Utført	Kommentar
2.1.1	Skriftlig avtale med leverandør (Normen kap. 5.8)	☐ Ja ☐ Nei	
2.1.2	Taushetserklæring (Normen kap. 5.8.3)	☐ Ja ☐ Nei	
2.1.3	Sikkerhetsrevisjon og avviksbehandling (Normen kap. 5.8.3, 6.1 og 6.3)	☐ Ja ☐ Nei	
2.1.4	Bevisstgjøring av taushetsplikten (Normen kap. 5.1)	☐ Ja ☐ Nei	
2.2.1	Risikovurdering før tilgang gis (Normen kap. 4.6)	☐ Ja ☐ Nei	
2.2.2	Risikovurdering i driften (Normen kap. 6.2)	☐ Ja ☐ Nei	
2.3.1	Opplæringstiltak (Normen kap. 5.6)	☐ Ja ☐ Nei	
2.4.1	Nettjenesteleverandør (Normen kap. 5.7)	☐ Ja ☐ Nei	
2.4.2	Begrensning av trafikk (Normen kap. 5.7.1)	☐ Ja ☐ Nei	
2.5.1	Krypteringsløsning (Normen kap. 5.4.4)	☐ Ja ☐ Nei	
2.6.1	Løsning for ondsinnet programvare (Normen kap. 5.8.3)	☐ Ja ☐ Nei	
2.7.1	Adgangsregulering (Normen kap. 5.8.3)	☐ Ja ☐ Nei	
2.7.2	Fysiske sikkerhetstiltak (Normen kap. 5.4.2)	☐ Ja ☐ Nei	
2.8.1	Ansvar for å tildele autorisasjon (Normen kap. 5.2.2)	☐ Ja ☐ Nei	
2.8.2	Prosedyre for tildeling av autorisasjon (Normen kap. 5.2.2)	☐ Ja ☐ Nei	
2.8.3	Autorisasjonsregister (Normen kap. 5.2.2)	☐ Ja ☐ Nei	
2.9.1	Autentisering med sikkerhetsnivå 4 (Normen kap. 5.2.1)	☐ Ja ☐ Nei	
2.9.2	Tilgangstyring (Normen kap. 5.2.3)	☐ Ja ☐ Nei	
2.9.3	Bruk av autorisasjon (Normen kap. 5.5.2)	☐ Ja ☐ Nei	
2.10.1	Overføring av helse- og personopplysninger til leverandør (Normen kap. 5.8.2)	☐ Ja ☐ Nei	
2.10.2	Overføring av helse- og personopplysninger til utlandet (Normen kap. 1.0)	☐ Ja ☐ Nei	
2.10.3	Skille helse- og personopplysninger fra flere virksomheter (Normen kap. 5.8.2)	☐ Ja ☐ Nei	
2.11.1	Konfigurasjonskontroll (Normen kap. 5.5.1)	☐ Ja ☐ Nei	
2.12.1	Hendelsesregistrering (Normen kap. 5.5.2)	☐ Ja ☐ Nei	
2.13.1	Gjennomgang av hendelsesregistre (Normen kap. 5.2.6)	☐ Ja ☐ Nei	
2.14.1	Analyse av hendelsesregistre (Normen kap. 5.5.2)	☐ Ja ☐ Nei	
2.15.1	Innsyn i leverandørens hendelsesregistre (Normen kap. 5.3.4)	☐ Ja ☐ Nei	

5.2 Eksempel på risikovurdering for virksomheten

I eksemplet er de generelle akseptkriteriene i tabell 1 i "Faktaark 5 - Fastsette akseptkriterier for tilgjengelighet, konfidensialitet, integritet og kvalitet" lagt til grunn.

RISIKOVURDERING

Virksomhet: Helsevirksomheten AS	
Vurdert av: IKT-leder	**Dato:** 31.mai 2012
Formålet med risikovurderingen:	Etablering av løsning for fjernaksess

	Forhold som er vurdert (uønsket hendelse / senario)	**Sannsynlighet**				**Konsekvens**				**Risikonivå**	**Tiltak Alltid Ja på Høy**
		1 = Usannsynlig	2 = Mindre Sannsynlig	3 = Mulig	4 = Sannsynlig	1 = Ubetydelig	2 = Moderat	3 = Alvorlig	4 = Kritisk		
1.	Uautorisert *tilgang* til *virksomhetens* nettverk pga manglende autentisering med *sikkerhetsnivå 4* (kun brukt nivå 2)	☐ 1	☐ 2	☐ 3	☒ 4	☐ 1	☐ 2	☒ 3	☐ 4	☐Lavt ☐Middels ☒Høy	☒Ja ☐Nei
2.	Manglende eller for svak kryptering av datakommunikasjon	☐ 1	☐ 2	☒ 3	☐ 4	☐ 1	☐ 2	☒ 3	☐ 4	☐Lavt ☐Middels ☒Høy	☒Ja ☐Nei
3.	Manglende eller mangelfull *hendelsesregistrering* på brannmuren	☐ 1	☒ 2	☐ 3	☐ 4	☐ 1	☒ 2	☐ 3	☐ 4	☒Lavt ☐Middels ☐Høy	☐Ja ☒Nei
4.	Manglende endingsstyring/konfigurasjonsstyring med konsekvens for utilsiktet nedetid	☐ 1	☐ 2	☒ 3	☐ 4	☐ 1	☐ 2	☒ 3	☐ 4	☐Lavt ☐Middels ☒Høy	☒Ja ☐Nei

	Beskrivelse av tiltak *(Nr 1 har høyest prioritet)*	**Betydning/ Kommentar**	**Ref linje nr over**
1.	Etablerer løsning for autentisering på sikkerhetsnivå 4	Utrede teknisk løsning Installere og sette i verk prosedyrer Påse at leverandørene bestiller sikkerhetsnivå 4	1
2.	Etablere obligatorisk kryptering fra brannmur mottakk	Slå på godkjent kryptering	2
3.	Etablere prosedyre for endringshåndtering og dokumentasjon av feil	Ny prosedyrer i kvalitetssystemet. Opplæring av medarbeidere og servicemedarbeidere	4

5.3 Eksempel på risikovurdering for leverandøren

I eksemplet er de generelle akseptkriteriene i tabell 1 i "Faktaark 5 - Fastsette akseptkriterier for tilgjengelighet, konfidensialitet, integritet og kvalitet" lagt til grunn.

RISIKOVURDERING

Virksomhet: Fagsystemleverandøren AS	
Vurdert av: Fjernaksess ansvarlig	**Dato: 3**1.mai 2012
Formålet med risikovurderingen:	Oppkobling av fjernaksess til Helsevirksomheten AS

	Forhold som er vurdert (uønsket hendelse / senario)	**Sannsynlighet**				**Konsekvens**				**Risikonivå**	**Tiltak Alltid Ja på Høy**
		1 = Usannsynlig	2 = Mindre Sannsynlig	3 = Mulig	4 = Sannsynlig	1 = Ubetydelig	2 = Moderat	3 = Alvorlig	4 = Kritisk		
1.	Uautorisert utlevering av *helse- og personopplysninger* med konsekvens for konfidensialitet	☐ 1	☐ 2	☒ 3	☐ 4	☐ 1	☐ 2	☒ 3	☐ 4	☐Lavt ☐Middels ☒Høy	☒Ja ☐Nei
2.	Overføring av ondsinnet programvare fra *leverandør* til *virksomheten*	☐ 1	☒ 2	☐ 3	☐ 4	☐ 1	☒ 2	☐ 3	☐ 4	☒Lavt ☐Middels ☐Høy	☐Ja ☒Nei
3.	Manglende eller for svak kryptering av datakommunikasjon med konsekvens av at autentiseringsdata og helse- og personopplysinger kan komme på avveie	☐ 1	☐ 2	☒ 3	☐ 4	☐ 1	☐ 2	☒ 3	☐ 4	☐Lavt ☐Middels ☒Høy	☒Ja ☐Nei
4.	Manglende eller mangelfull *hendelsesregistrering*	☒ 1	☐ 2	☐ 3	☐ 4	☐ 1	☐ 2	☐ 3	☐ 4	☒Lavt ☐Middels ☐Høy	☐Ja ☐Nei
5.	Behandling av *helse- og personopplysninger* hentet fra *virksomheten* blir gjennomført på åpent nettverk hos leverandøren pga manglende logisk adskillelse i *leverandørens* nett	☐ 1	☒ 2	☐ 3	☐ 4	☐ 1	☐ 2	☒ 3	☐ 4	☐Lavt ☒Middels ☐Høy	☒Ja ☐Nei

	Beskrivelse av tiltak *(Nr 1 har høyest prioritet)*	**Betydning/ Kommentar**	**Ref linje nr over**
1.	Utarbeide prosedyrer for bruk av fjernaksess samt gjennomføre opplæring	Involvere alle relevante servicemedarbeidere	1
2.	Etablere godkjent kryptering	Iverksette kryptering i VPN	3
3.	Etablere logisk adskillelse i nettverket / fjernaksessløsningen mellom de ulike kundene og mellom leverandørens egen virksomhet.	Utrede teknologi. Anskaffe og installere løsning Iversette prosedyrer og opplæring	5

5.4 Forslag til tekst i vedlikeholdsavtale

Forslaget kan benyttes som bilag til statens standardavtaler (se http://www.difi.no/statens-standardavtaler-ssa).

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 "Norm for informasjonssikkerhet" (Normen) av 2. juni 2010 legges til grunn.

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

Kunden skal ha full innsynsrett i *leverandørens*:

- Sikkerhetsmål og -strategi
- Tekniske og organisatoriske løsninger for *fjernaksessen*
- Prosedyrer som gjelder for *fjernaksessen*
- Resultat av risikovurdering og sikkerhetsrevisjoner
- Hendelsesregistre

Krav i Normen som skal ivaretas av *leverandøren* (Jf. kap 5.8.3 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.

Følgende elementer er innarbeidet i avtale:

Nr	Element	Innarbeidet
1.	Hvem avtalepartene er	☐ Ja ☐ Nei
2.	Formålet med avtalen eller særavtalen	☐ Ja ☐ Nei
3.	Ansvarlige personer/roller	☐ Ja ☐ Nei
4.	*Virksomheten* skal ha tilgang til *leverandørens* dokumentasjon av sikkerhetsmål og strategi	☐ Ja ☐ Nei
5.	*Virksomheten* skal ha innsynsrett i *leverandørens* løsning for ivaretakelse av Normen	☐ Ja ☐ Nei
6.	*Virksomheten* skal ha rett til innsyn i *leverandørens* hendelsesregistre	☐ Ja ☐ Nei
7.	*Taushetsplikt* for *leverandørens* personale	☐ Ja ☐ Nei
8.	Hvilke prosedyrer som gjelder for *fjernaksess*løsningen	☐ Ja ☐ Nei

Nr	Element	Innarbeidet
9.	Prosedyre for *avvik*sbehandling	☐ Ja ☐ Nei
10.	Konsekvenser ved brudd på avtalen	☐ Ja ☐ Nei
11.	Oversikt over hvilke systemer det gis *fjernaksess* til	☐ Ja ☐ Nei
12.	Beskrivelse av utstyr *leverandøren* kan benytte til *fjernaksess* og eierforholdet til utstyret	☐ Ja ☐ Nei
13.	Konsekvensutredning ved tilsiktet brudd under bruk av fjerntilkoblingen	☐ Ja ☐ Nei

Følgende prosedyrer er innarbeidet:

Nr	Element	Innarbeidet	Ansvar
1.	Signering av taushetserklæring og bekreftelse på at sikkerhetsinstruks er lest og akseptert	☐ Ja ☐ Nei	
2.	Opplæring av *servicemedarbeider*	☐ Ja ☐ Nei	
3.	Administrasjon av *autorisasjon* til utstyr som benyttes til *fjernaksess*	☐ Ja ☐ Nei	
4.	Bruk av løsning for sterk *autentisering*	☐ Ja ☐ Nei	
5.	Avviksbehandling ifm *fjernaksess*	☐ Ja ☐ Nei	
6.	*Hendelsesregistrering* og oppfølging av hendelsesregistre	☐ Ja ☐ Nei	
7.	Sletting av datafiler hentet fra *virksomheten*	☐ Ja ☐ Nei	
8.	Destruksjon av lagringsmedia ved utrangering	☐ Ja ☐ Nei	
9.	Oppgaver som kan utføres ved oppkobling /etablering av *fjernaksess* (se sjekkliste i pkt 5 Vedlegg)	☐ Ja ☐ Nei	
10.	Tildele *autorisasjon* til nettverk, utstyr og systemer	☐ Ja ☐ Nei	
11.	*Autentisering* av *servicemedarbeider* hos *leverandør*	☐ Ja ☐ Nei	
12.	Kontroll av tildelte *autorisasjoner*	☐ Ja ☐ Nei	
13.	Oppgaver som skal utføres ved oppkobling /etablering av *fjernaksess* (se sjekkliste i pkt 5 Vedlegg)	☐ Ja ☐ Nei	

5.5 Eksempel på momenter i en sikkerhetsinstruks

Sikkerhetsinstruks

(Eksempelet gjelder for den enkelte servicemedarbeider)

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 servicemedarbeider plikter å forhindre at uautoriserte får tilgang til løsninger som kan benyttes mot <virksomheten>
- 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 brukenavn, 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 servicemedarbeideres 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 personopplysingene du håndterer. Ikke la helse- og personopplysinger flyte rundt, men sikre dem etter gjeldene prosedyre

Feil sletting av informasjon

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

Hendelsesregistrering

- <virksomheten> har plikt til å hendelsesregistre 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 personopplysinger 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 hvilke prosedyrer som gjelder for avvikshåndtering

5.6 Deltagere i referansegruppen

Følgende har deltatt i referansegruppen:

Navn	E-post	Rolle/stilling	Virksomhet
Andre Meldal	andre.meldal@nhn.no	Sikkerhetsingeniør	Norsk Helsenett SF
Frode Olsen	frode.olsen@farmait.no	IT konsulent	FarmaIT
Geir Hovind	geihov@sykehuspartner.no	Seksjonsleder - risikostyring, sikkerhet og compliance	Sykehuspartner
Hallgeir Nisja	hallgeir.nisja@hemit.no	Rådgiver IT sikkerhet/ Personverneombud	Hemit - Helse Midt-Norge IT
Hanne Kolflaath	hanne@acos.no	Forretningsansvarlig Levekår	Acos
Jan Gunnar Broch	jangunnar.broch@helsedir.no	Seniorrådgiver	Helsedirektoratet
Kjell Inge Hestad	Kjell.Inge.Hestad@visma.no	IT manager	Visma
Ole Erik Dammen	ole.erik.dammen@ compugroupmedical.no	Leveranseansvarlig	CompuGroup Medical
Sven Egil Hauan	sven.e.hauan@siemens.com	SRS Manager	Siemens
Sverre Biseth	sverre.biseth@med.ge.com	IT konsulent	GE Healtcare
Nils Jensson	nils.jensson@helse-vest-ikt.no	IT konsulent	Helse Vest IKT