

| | |
|---|--|
|  <p>Norm for informasjonssikkerhet i helsesektoren</p> | Utgitt med støtte av:  |
| <h2>Fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet</h2> | Støttedokument Faktaark nr 36 Versjon: 2.0 Dato: 03.12.2009 |

| | | | |
|--|---|--|--|
| Målgruppe Dette faktaarket er spesielt relevant for: | <input checked="" type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input type="checkbox"/> Prosjektleder | <input checked="" type="checkbox"/> Sikkerhetsleder / sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig | <input type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud |
| Ansvar | Virksomhetens ledelse har ansvaret for å forsikre seg om at oppkobling av fjernaksess fra leverandører ivaretar konfidensialitet, integritet, tilgjengelighet og kvalitet. | | |
| Gjennomføring | Gjennomføres før oppkobling av fjernaksess og som en løpende aktivitet ved bruk av fjernaksess. | | |
| Formål | Hindre uautorisert bruk og ivareta integritet og konfidensialitet for helse- og personopplysninger ifm. fjernaksess. Sørge for å ha tilstrekkelig skille mellom leverandørens supportnettverk og øvrige tekniske løsninger, og sikre tilstrekkelig sikkerhet ved tilkobling og overføring. | | |
| Omfang | Alltid når fjernaksess skal etableres og under bruk. | | |
| Hjemmel | <ul style="list-style-type: none"> • Personopplysningsforskriften § 2-10 Fysisk sikring, § 2-11 Sikring av konfidensialitet, § 2-12 Sikring av tilgjengelighet, § 2-13 Sikring av integritet • Helseregisterloven § 16 Sikring av konfidensialitet, integritet, kvalitet og tilgjengelighet • Helsepersonelloven § 25, opplysninger til samarbeidende personell. | | |
| Referanser | <ul style="list-style-type: none"> • Norm for informasjonssikkerhet i helsesektoren, pkt. 4.4, 5.2 og 5.8.3 • Veileder for fjernaksess for vedlikehold og oppdateringer fra leverandør til helsevirksomhet • Faktaark 15 – Hendelsesregistrering (logging) og oppfølging • Faktaark 7 – Risikovurderinger • Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, april 2008 | | |

Definisjon

Med ”fjernaksess” menes i dette dokumentet ekstern tilgang fra leverandør til helsevirksomhet via kommunikasjonslinje for å utføre vedlikehold og oppdateringer av IKT-løsninger.

| Nr. | Aktivitet/Beskrivelse |
|-----|---|
| 1. | Prinsipper for fjernaksess <ul style="list-style-type: none"> - Prinsipper for fjernaksess må være forankret i virksomhetens styringssystem for informasjonssikkerhet - Virksomheten bør etablere en enhetlig løsning for fjernaksess ifm sensitive personopplysninger og ikke mange fragmenterte for enkelte leverandører - Leverandør kan inngå avtale med Norsk Helsenett for fjernaksess til virksomheten. Alle som benytter helsenettet må avklare løsningen med Norsk Helsenett - Det skal i størst mulig grad benyttes tekniske tiltak som utstyr og programvare. Det er ikke tilstrekkelig med bare skriftlige rutiner som viser ansvar og arbeidsoppgaver - På forhånd skal det gjennomføres en risikovurdering av de løsninger som skal etableres - All tilgang til virksomhetens systemer gjennom fjernaksess, skal kun skje etter en særskilt tillatelse, fra leverandørens adskilte supportnettverk og med individuell pålogging for leverandørens personell - Etter en risikovurdering, og hvis det er i samsvar med formålet med fjernaksess, kan det unntaksvis legges opp til løsninger som ikke krever manuelle operasjoner for å åpne opp tilgangen til fjernaksess (se Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet) - Alle aktiviteter skal hendelsesregistreres. Leverandør skal dokumentere hva som er utført i |

| Nr. | Aktivitet/Beskrivelse |
|-----|--|
| | virksomheten. Hendelsesregistre kan være både elektroniske og manuelle |
| 2. | <p>Før fjernaksess etableres</p> <ul style="list-style-type: none"> - Det skal gjennomføres en behovskartlegging for hvert nytt eller endret leverandørforhold med mål å fastsette: <ul style="list-style-type: none"> a) Det faglige formålet med oppkoblingen og viktigheten for organisasjonen b) Hvilke system eller registre det skal gis tilgang til c) Hvilken teknisk løsning oppkoblingen baseres på: terminalserver, klient, databaseverktøy, WEB, osv d) TCP/IP nettadresser og port numre som skal anvendes e) Behov for tilgang for å lese, skrive og opp/nedlastning av helse- og personopplysninger, og hvordan dette skal administreres og dokumenteres f) Tilgang med administratorrettigheter på operativsystem, database eller fagapplikasjon g) Skille mellom leverandørens supportnettverk og utstyr i forhold til leverandørens øvrige tekniske løsning, personell og Internett-tilganger og -tjenester h) Bruk av fjernkontroll (ta over skjerm, tastatur og datamus) som skal initieres fra virksomheten - Det skal gjennomføres en risikovurdering med basis i virksomhetens nivå for akseptabel risiko - Ut fra risikovurderingen må virksomheten fastsette følgende: <ul style="list-style-type: none"> a) Om fjernaksess skal benyttes og om den skal benyttes på den aktuelle løsningen b) Hvilket nivå tilgangen skal skje på i forhold til operativsystem, database med mer c) Bruk av predefinert utstyr for aksess til fjernaksesløsningen d) Tilgang til deler av registre med helse- og personopplysninger og typen av tilgang i forhold til: lese, skrive, opp- og nedlastning e) Bruk av opp- og nedlastning av tekniske rettinger i programmer og konfigurasjonsparametere f) Krav til leverandørens nettverk og utstyr g) Oppkobling og bruk av verktøy for fjernadministrasjon skal i hovedsak initieres fra virksomheten som en aktiv handling h) Krav til separasjon mellom leverandørens nettverk- og utstyr og øvrig personell som ikke har noe med supporten å gjøre samt leverandørens tilgang til Internett-tjenester i) Behov for koordinering mellom flere leverandører før løsningen etableres j) Hvilke rutiner og avtaler som må være på plass ut fra øvrige krav i virksomhetens styringssystem for informasjonssikkerhet |
| 3. | <p>Valg og etablering av teknisk løsning</p> <p>Den tekniske løsningen skal inneholde følgende elementer:</p> <ul style="list-style-type: none"> - Den ytre termineringen bør skje gjennom en brannmur og i en egen DMZ-sone for fjernaksess - Kun forhåndsgodkjent og eksplisitt definert trafikk, som reguleres av brannmuren, tillates - For tilkoblingssikkerhet skal det benyttes Nivå 4 for autentisering med bruk av engangspassord eller tilsvarende og i tillegg individuell pålogging - Om det foreligger et faglig behov for at leverandøren flytter helse- og personopplysninger til leverandørens sikre nettverksområder skal det føres kontroll med hva som overføres og sikring hos leverandør. Kontrollen kan gjøres dels ved hendelsesregistrering og dels ved skriftlige rutiner og rapportering - All ekstern kommunikasjon med helse- og personopplysninger skal krypteres iht gjeldende krav - Det skal være løsninger for å hindre ondsinnet programvare hos leverandøren - Følgende skal hendelsesregistreres: <ul style="list-style-type: none"> a) Aksepterte og forkastede oppkoblinger til den ytre termineringen (brannmur og DMZ) b) Den aktuelle autentisering c) Pålogging på servere, databaser og ulike fagsystemer d) Flytting av helse- og personopplysninger til leverandørens sikre nettverksområder e) Tilgang til helse- og personopplysninger (se Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet) - Det skal sikres med tekniske tiltak at leverandørens arbeidsstasjon ikke er tilkoblet andre nettverk når det gjennomføres tilkobling til virksomhetens nettverk |

| Nr. | Aktivitet/Beskrivelse |
|-----|---|
| 4. | <p>Avtale Følgende dokumentasjon skal være på plass før tilgang til fjernaksess gis:</p> <ul style="list-style-type: none"> - Signert taushetserklæring med henblikk på tilgang til helse- og personopplysninger. Leverandøren oppbevarer disse for eget personell. Se Normen vedrørende taushetsplikt for ansatte - Lest og akseptert sikkerhetsinstruks - Tilknytningsavtale i hvert enkelt tilfelle med varighet. I avtalen skal det være en passus med konsekvenser og sanksjoner ved mislighold og leverandørens plikt til å etterleve Normen - Rutine for tilkobling, herunder tildeling av engangspassord og overvåking - Rutine for gjennomgang av hendelsesregistre - Rutiner for fjerning av tilgang når avtalen opphører - Rutine for behandling og sletting av helse- og personopplysninger som er flyttet til leverandørens sikre nettverksområder - Andre tekniske og administrative rutiner som styringssystemet krever eller som risikovurderingen påpeker |
| 5. | <p>Oppfølging av leverandør</p> <ul style="list-style-type: none"> - Avviksbehandling skal skje fortløpende. Avvik som har betydning for virksomheten skal rapporteres fortløpende - Leverandøren skal minimum årlig rapportere bruk og hendelser samt dokumentere at leverandørens plikt til å informere/lære opp egne medarbeidere blir ivaretatt - Virksomheten skal følge opp leverandørens hendelsesregistre. Dette kan gjøres ved at leverandøren innarbeider hendelsesregistre som er fortolket i sin rapportering til virksomheten - Leverandør skal dokumentere hva som er utført hos virksomheten |

Eksempel på fjernaksesløsninger:

Eksempelet under viser bruk av terminalserver og engangspassord. Figuren illustrerer at:

- Virksomhet drifter og administrerer server for engangspassord
- Virksomhet drifter terminalserver
- Leverandør har atskilt nettverk for vedlikehold og oppdateringer (atskilt supportnettverk)
- Servicemedarbeider hos leverandør har fått utlevert engangspassordgenerator (Token) fra virksomhet
- Helsenettet benyttes for kommunikasjon

For små virksomheter kan deler av den tekniske løsningen i virksomheten leveres av en leverandør. For eksempel server for engangspassord og terminalserver for tilgang til journalsystem.

