Norm for informasjonssikkerhet i helsesektoren

Utgitt med støtte av: Direktoratet for e-helse

# Fjernaksess mellom leverandør og virksomhet

**Støttedokument**
**Faktaark nr 36**
Versjon: 3.2
Dato: 01.10.2018

| | | | |
|---|---|---|---|
| **Formål** | Hindre uautorisert bruk og ivareta integritet og konfidensialitet for helse- og personopplysninger ifm. fjernaksess. Sørge for tilstrekkelig sikkerhet ved tilkobling og overføring av helse- og personopplysninger. | | |
| **Ansvar** | Virksomhetens ledelse har ansvaret for å forsikre seg om at bruk av fjernaksess fra leverandører ivaretar kravene til konfidensialitet, integritet, tilgjengelighet og kvalitet. | | |
| **Gjennomføring** | Gjennomføres før oppkobling av fjernaksess og som en løpende aktivitet ved bruk av fjernaksess. | | |
| **Omfang** | Ved etablering og bruk av fjernaksess. | | |
| **Målgruppe**<br><br>Dette faktaarket er spesielt relevant for: | ☒ Leverandør<br>☒ IKT-ansvarlig<br>☐ Forsker<br>☐ Prosjektleder | ☒ Sikkerhetsleder / sikkerhetskoordinator<br>☒ Virksomhetens leder/ledelse<br>☐ Forskningsansvarlig | ☐ Medarbeider/ansatt<br>☒ Databehandler<br>☐ Personvernombud |
| **Hjemmel** | • Personvernforordningen artikkel 32<br>• Pasientjournalloven § 22<br>• Helseregisterloven § 21<br>• Helsepersonelloven § 25 | | |
| **Referanser** | • Norm for informasjonssikkerhet i helsesektoren<br>• Veileder for fjernaksess mellom leverandør og virksomhet<br>• Faktaark 15 – Hendelsesregistrering (logging) og oppfølging<br>• Faktaark 7 – Risikovurderinger<br>• Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, april 2008 http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf | | |

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

| Nr. | Aktivitet/Beskrivelse |
|---|---|
| 1. | **Prinsipper for fjernaksess**<br>a) Prinsipper for fjernaksess må være forankret i virksomhetens styringssystem for informasjonssikkerhet<br>b) Virksomheten bør etablere en enhetlig løsning for fjernaksess ifm helse- og personopplysninger og ikke mange fragmenterte løsninger for enkelte leverandører<br>c) All tilgang til virksomhetens systemer ved bruk av fjernakses<br>d) 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 mellom leverandør og helsevirksomhet)<br>e) Alle aktiviteter skal hendelsesregistreres. Leverandør skal dokumentere hva som er utført i virksomheten. Hendelsesregistre kan være både elektroniske og manuelle |

| Nr. | Aktivitet/Beskrivelse |
|---|---|
| 2. | **Før fjernaksess etableres**<br>a) Det skal gjennomføres en behovskartlegging for hvert nytt eller endret leverandørforhold med mål å fastsette:<br>- Det faglige formålet med oppkoblingen og viktigheten for organisasjonen<br>- Hvilke system eller registre det skal gis tilgang til<br>- Hvilken teknisk løsning oppkoblingen baseres på: terminalserver, klient, databaseverktøy, WEB, osv<br>- TCP/IP nettadresser og port numre som skal anvendes<br>- Behov for tilgang for å lese, skrive og opp/nedlastning av helse- og personopplysninger, og hvordan dette skal administreres og dokumenteres<br>- Tilgang med administratorrettigheter på operativsystem, database eller fagapplikasjon<br>- Bruk av fjernadministrasjon (ta over skjerm, tastatur og datamus) som skal initieres fra virksomheten<br>b) Det skal gjennomføres en risikovurdering med basis i virksomhetens nivå for akseptabel risiko<br>c) Ut fra risikovurderingen må virksomheten fastsette følgende:<br>- Om fjernaksess skal benyttes og om den skal benyttes på den aktuelle løsningen<br>- Hvilket nivå tilgangen skal skje på i forhold til operativsystem, database med mer<br>- Bruk av predefinert utstyr for aksess til fjernaksessløsningen<br>- Tilgang til deler av registre med helse- og personopplysninger og typen av tilgang i forhold til: lese, skrive, opp- og nedlastning<br>- Bruk av opp- og nedlasting av tekniske rettinger i programmer og konfigurasjonsparametere<br>- Krav til leverandørens nettverk og utstyr<br>- Oppkobling og bruk av verktøy for fjernadministrasjon skal i hovedsak initieres fra virksomheten som en aktiv handling<br>- Behov for koordinering mellom flere leverandører før løsningen etableres<br>- Hvilke prosedyrer og avtaler som må være på plass ut fra øvrige krav i virksomhetens styringssystem for informasjonssikkerhet |
| 3. | **Avtaler**<br>a) Det skal inngås skriftlig avtale som minimum skal inneholde:<br>- Hvem avtalepartene er<br>- Formålet med avtalen eller særavtalen<br>- Ansvarlige personer/roller<br>- Virksomheten skal ha tilgang til leverandørens dokumentasjon av sikkerhetsmål og strategi<br>- Virksomheten skal ha innsynsrett i leverandørens løsning for ivaretakelse av Normen<br>- Virksomheten skal ha rett til innsyn i leverandørens relevante hendelsesregistre<br>- Taushetsplikt for leverandørens personale<br>- Hvilke prosedyrer som gjelder for fjernaksessløsningen<br>- Prosedyre for avviksbehandling<br>- Konsekvenser ved brudd på avtalen<br>- Oversikt over hvilke systemer det gis fjernaksess til<br>- Beskrivelse av utstyr leverandøren kan benytte til fjernaksess og eierforholdet til utstyret<br>- Konsekvensutredning ved tilsiktet brudd under bruk av fjerntilkoblingen |
| 4. | **Dokumentasjon**<br>a) Følgende dokumentasjon skal være på plass før tilgang til fjernaksess gis:<br>- Signert taushetserklæring med henblikk på tilgang til helse- og personopplysninger. Leverandøren oppbevarer disse for eget personell. Se Normen vedrørende taushetsplikt for ansatte<br>- Lest og akseptert sikkerhetsinstruks |

| Nr. | Aktivitet/Beskrivelse |
|---|---|
| | - Prosedyre for<br>▪ Signering av taushetserklæring og bekreftelse på at sikkerhetsinstruks er lest og akseptert<br>▪ Opplæring av servicemedarbeider<br>▪ Administrasjon av autorisasjon til utstyr som benyttes til fjernaksess<br>▪ Bruk av løsning for sterk autentisering<br>▪ Avviksbehandling ifm fjernaksess<br>▪ Hendelsesregistrering og oppfølging av hendelsesregistre<br>▪ Sletting av datafiler hentet fra virksomheten<br>▪ Destruksjon av lagringsmedia ved utrangering<br>▪ Oppgaver som kan utføres ved oppkobling /etablering av fjernaksess Tildele autorisasjon til nettverk, utstyr og systemer<br>▪ Autentisering av servicemedarbeider hos leverandør<br>▪ Kontroll av tildelte autorisasjoner<br>▪ Oppgaver som skal utføres ved oppkobling /etablering av fjernaksess<br>▪ Andre tekniske og administrative prosedyrer som styringssystemet krever eller som risikovurderingen påpeker |
| 5. | **Valg og etablering av teknisk løsning**<br>a) Den tekniske løsningen bør inneholde følgende elementer:<br>- Den ytre termineringen bør skje gjennom en brannmur og i en egen DMZ-sone for fjernaksess<br>- Kun forhåndsgodkjent og eksplisitt definert trafikk tillates<br>- Autentisering skal være med sikkerhetsnivå 4<br>- Om det foreligger et faglig behov for at leverandøren flytter helse- og personopplysninger til leverandørens sikre nettverksområder skal det utføres iht en databehandleravtale<br>- All ekstern kommunikasjon med helse- og personopplysninger skal krypteres med minimum krypteringsstyrke som tilsvarer bruk av PKI eller virksomhetssertifikat iht gjeldende "Kravspesifikasjon for PKI i offentlig sektor" er tilfredsstillende. [1]<br>- Det skal være løsninger for å hindre ondsinnet programvare hos leverandøren og virksomheten<br>- Det skal sikres med tekniske tiltak at leverandørens arbeidsstasjon ikke er tilkoblet andre nettverk når det gjennomføres tilkobling til virksomhetens nettverk<br><br>Eksempler på tekniske løsninger finnes i "Veileder for fjernaksess mellom leverandør og virksomhet" |
| 6. | **Hendelsesregistrering**<br>a) 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:<br>- entydig identifikator for den autoriserte brukeren<br>- rollen den autoriserte brukeren har ved tilgangen<br>- virksomhetstilhørighet<br>- organisatorisk tilhørighet til den som er autorisert<br>- hvilke type opplysninger det er gitt tilgang til<br>- grunnlaget for tilgangen<br>- tidspunkt og varighet for *tilgangen*<br>b) Ved fjernakses fra *leverandør* skal følgende i tillegg hendelsesregistreres:<br>- Initiert trafikk mot IP-adresser og portnummer |

[1] http://www.difi.no/artikkel/2010/04/kravspesifikasjon-for-pki

| Nr. | Aktivitet/Beskrivelse |
|---|---|
| | - Hvilke data/datafiler som er lastet ned til leverandøren (datafiler) eller opp til virksomheten (programfiler og patcher)<br>- Entydig identifikator for den hos *leverandør* som har benyttet den aktuelle *fjernaksess*<br>c) For forsøk på uautorisert bruk skal følgende hendelsesregistreres:<br>- Brukeridentiteten som ble benyttet<br>- Tidspunkt (dato og klokkeslett)<br>- IP-adresse eller annen identifikasjon av PC/arbeidsstasjon som ble benyttet (for eksempel MAC-adresse eller NAT-adresse)<br>d) Hendelsesregistre skal oppbevares i minimum 2 år. |