Prinsipper for informasjonsbehandling HNT

Dokumentadministrator: Heidi Værdal | Gyldig fra: 07.01.2019 | Revisjon: 4.1
Godkjent av: Hilde Fossland | Revisjonsfrist: 01.01.2020 | ID: 643

Innledning

Helse Nord-Trøndelag HF (HNT) behandler informasjon, herunder sensitive personopplysninger, elektronisk. Dette innebærer bl.a at det settes strenge krav til tekniske løsninger og til den enkelte medarbeiders ansvarsbevissthet og kompetanse vedrørende informasjonssikkerhet.

De tekniske løsninger internt i helseforetaket, hos leverandør av IT-tjenester (HEMIT) samt underleverandører, skal bl.a. sammen med **ansvarsbevissthet, holdninger og kultur** i virksomheten, bidra til sikker informasjonsbehandling.

Aktuelt lovverk er sammen med helselovgivningen Helseregisterloven og Personopplysningsloven med forskrift. (Se også lenke til lovdata under "Relatert")

Sentrale begreper

Sensitive personopplysninger (særlige kategorier):

1. opplysninger om rasemessig eller etnisk opprinnelse
2. opplysninger om politisk oppfatning
3. opplysninger om religion
4. opplysninger om filosofisk overbevisning
5. opplysninger om fagforeningsmedlemskap
6. genetiske opplysninger
7. biometriske opplysninger med det formål å entydig identifisere noen
8. helseopplysninger
9. opplysninger om seksuelle forhold
10. opplysninger om seksuell legning
11. opplysninger om straffedommer
12. opplysninger om lovovertredelser

Sikker informasjonsbehandling innebærer at relevant informasjon skal være lett tilgjengelig for den som har tjenstlig behov for den. Når det gjelder opplysninger om pasienter, vil dette som hovedregel si den som deltar i utredning, behandling og pleie av pasienten

Tilgjengelighet: Informasjonen er lett å finne for autorisert person

Konfidensialitet: Informasjonen skal være utilgjengelig for den som ikke er autorisert for innsyn.

Integritet: Informasjonen skal ikke endres eller slettes på en uautorisert måte, den skal være riktig og oppdatert

Autorisert bruker: Har kunnskap og holdninger som medfører at en er i stand til å bruke IT-verktøyet på en lovlig og etisk riktig måte, samt at en har bruk for de aktuelle opplysninger i behandlings- eller

forskningsøyemed på det gitte tidspunkt.

Organisering og ansvar

- Administrerende direktør er databehandleransvarlig
- Informasjonssikkerhetsrådgiver og IT-leder har ansvar for tilrettelegging på foretaksnivå.
- Klinikk-/avdelingsleder har ansvar for å legge til rette for sikker informasjonsbehandling i egen klinikk/avdeling. Dette innebærer blant annet at den enkelte nettbruker har tilgang til nødvendig informasjon om emnet til enhver tid.
- Den enkelte nettbruker har ansvar for å sikre konfidensialitet, integritet og tilgjengelighet for de opplysninger han/hun håndterer av sensitiv art. Signering av databrukerkontrakt innebærer en aksept for helseforetakets rutiner i denne sammenhengen.

Relevante rutiner ligger hovedsakelig i EQS, i kategoriene "Informasjonssikkerhet".

Sentrale infosikkerhetselementer

Taushetsplikt: innebærer i denne sammenhengen ikke bare at opplysningene er konfidensielle, men også at man kun skal innhente personopplysninger på det tidspunkt man har bruk for dem i behandlings- eller forskningsøyemed. Taushetsplikten innebærer også at andre personer kun skal gjøres kjent med pasientopplysninger i det de deltar i utredning, behandling eller pleie av pasienten. Andre personer er i denne sammenhengen uautoriserte. Pasienten kan gi fritak fra taushetsplikten.

Passord: Hver bruker har eget brukernavn og nettverkspassord (se relatert dokument: "Passordrutiner - nettverkspassord"). Passord skal ikke oppgis til andre. Dette bl.a fordi om en person logger seg på med en annens brukernavn og passord, er det sistnevnte bruker det registreres aktivitet på, og som vil kunne stilles til ansvar for denne aktiviteten. Nettbruker skal logge ut av arbeidsstasjonen når denne forlates. Dette skal også bidra til at opplysningenes konfidensialitet sikres.

Logging: All bruk av eksternt og internt nettverk logges, dvs. at det registreres elektronisk hvilken bruker som er inne i nettverkene, på hvilket tidspunkt og fra hvilken arbeidsstasjon. (Se relatert dokument "Loggrutiner"). Logg fra aktivitet i programmer som tilhører elektronisk pasientjournal skal etter lovverket sjekkes ved hjelp av stikkprøver ift. nettbruker eller pasient. Slik sjekk varsles ikke. Pasienten kan på forespørsel få innsyn i hvilket helsepersonell som har hatt innsyn i vedkommendes journal, og når .

Elektronisk lagring av sensitive personopplysninger: Gjelder ikke EPJ (Doculive og PACS/RIS), PAS samt lokale systemer som håndterer lagring av sensitive personopplysninger i systemet. Sensitive personopplysninger skal lagres på helseforetakets interne nettverk, på en slik måte at ingen andre enn autoriserte personer kan ha tilgang til dem, samt at opplysningene er tilgjengelig for de som har bruk for dem når de har bruk for dem. I tillegg skal journalen fremstå som helhetlig og ajour fortløpende. Det vil si i en katalog med begrenset tilgang.

Det er ikke tillatt å lagre på lokal harddisk, bærbar PC, minnebrikke, CD eller diskett. Det er ikke tillatt å ta sensitive personopplysninger med ut av helseforetaket.

Hjemmekontor og tilgang til kliniske applikasjoner eller andre applikasjoner som inneholder sensitive personopplysninger

De som de sensitive opplysningene omfatter, skal oppleve at sikkerheten omkring disse opplysningene, ved bruk av hjemmekontorløsning, er de samme om den ansatte har tilgang til opplysningene på sitt arbeidssted i helseforetaket.

Krav til bruk av hjemmekontor

- Foretakets prosedyrer for bruk av Internett og e-post skal følges i forbindelse med hjemmekontor
- Sensitive personopplysninger skal ikke lagres lokalt på PC
- Ingen andre enn den som er autorisert til å bruke virksomhetens PC skal benytte denne
- Utskrifter som inneholder helse- og personopplysninger skal oppbevares sikkert og/eller umiddelbart makuleres etter bruk. Under bruk skal innsyn fra uautoriserte ikke forekomme
- PC skal låses av bruker ved fravær
- Privat bruk av hjemmekontor-PC følger de samme reglene som for privat bruk av PC på

arbeidsplassen
- Ved arbeid med helse- og personopplysninger skal det iverksettes tiltak for å hindre innsyn fra eksterne (f.eks. familiemedlemmer og andre)
- Programvaren skal til enhver tid være oppdatert iht. gjeldende standarder og krav i virksomheten

Det er brukeren av hjemmekontorløsningen som er ansvarlig for at informasjonssikkerheten ivaretas ved bruk av hjemmekontorløsning.

Utlevering av pasientopplysninger: Kan bare skje til samarbeidende personell dersom pasienten ikke motsetter seg dette (se Helsepersonelloven § 45). Pasienten kan bestemme at andre skal få tilgang til opplysninger. Pasientopplysninger kan ikke sendes som E-post uten godkjent kryptering.

Underskrift: Signering av databrukerkontrakt og mottak av autorisasjon innebærer at en forplikter seg til å følge gjeldende lover og forskrifter, samt helseforetakets interne krav.

Endring av tilgang: Ved endret behov for tilgangsrettigheter skal dette meldes HEMIT ved å fylle ut skjemaet "Valg av elektronisk programtilgang" (se relatert dokument).

Etablering av personregistre: Et personregister er etablert dersom det ved hjelp av registeret er mulig å identifisere enkeltpersoner (mer personidentifikasjon enn alder og kjønn). Nye personregistre skal meldes inn til kvalitetsrådgiver i HNT før de etableres. Det er den som oppretter eller er ansvarlig bruker for registeret som skal melde dette inn. (Se relatert dokument "Personregistre - prosedyre for opprettelse, bruk og sletting").

For etablering av forskningsregistre, se dokumentet "Behandling av personopplysninger i forbindelse med forskning i HNT"

E-post: Det er ikke tillatt å klippe/lime fra programmer som behandler pasientopplysninger inn i E-post. E-postadresse ved HNT skal brukes i tjenestlig behov, og brukeren skal vise nødvendig aktsomhet i det vedkommende representerer HNT. (Se relatert dokument "Rutiner for bruk av E-post")

Internett: Internettbruk ved HNT skal være ut ifra tjenestlig behov, og brukeren skal vise nødvendig aktsomhet i det vedkommende representerer HNT. Helseforetakets regler for akseptabel atferd og gjeldende lovverk skal oppfylles i bruk av internett fra foretakets nettverk. Det er f.eks ikke tillatt å søke etter eller formidle pornografi eller taushetsbelagte opplysninger.

Oppsett av datamaskiner: Nettbruker skal ikke innstallere nytt datautstyr eller programvare på HNTs utstyr uten at dette er godkjent av IT-leder. Endring i oppsett av datamaskinen skal ikke gjøres av andre enn HEMIT.

Innstallering av modem eller annet kommunikasjonsutstyr er ikke tillatt opp mot nettverksoppkoblet utstyr. Forsøk på å omgå logiske eller tekniske sikringstiltak anses som brudd på sikkerhetsrutinene, og vil oppfattes som avvik.

Ved utskrift til skriver er bruker ansvarlig for å vite hvilken skriver utskriften kommer på. Utskrift skal ikke være tilgjengelig for uautoriserte personer.

Det gjelder spesielle sikkerhetsregler for bruk av bærbart IKT-utstyr i HNT. Se relatert dokument "Bærbart IKT-utstyr". Her heter det blant annet at det ikke er tillatt å koble utstyret til eksternt nettverk (f.eks internett) utenom hjemmekontorløsningen eller bruk av IR-kommunikasjon mot annet utstyr, for deretter å koble utstyret opp i helseforetakets nettverk.

Avvik: Brudd på prinsipper for informasjonssikkerhet skal meldes som avvik i tråd med gjeldende avviksprosedyrer (se relatert dokument: "Avviksbehandling") I enkelte tilfeller kan det av faglige eller andre hensyn være nødvendig å omgå prinsippene. Dette skal meldes til informasjonssikkerhetsansvarlig på forhånd.

Konsekvenser ved brudd på prinsipper for informasjonssikkerhet i HNT: Det vil kunne ha konsekvenser for den enkelte bruker å bryte disse prinsippene. Dette vil kunne variere fra muntlig advarsel, via tap av nettverkstilgang og betydning for ansettelsesforhold, til politianmeldelse.

Bruk av sosiale medier:

Sosiale medier:
Arbeidstakers bruk av sosiale medier kan skape en del problemstillinger og grensespørsmål i forhold til lojalitetsplikten. Det gjelder kanskje spesielt når arbeidstaker som privatperson bruker sosiale medier. Lojalitetsplikten gjelder også når arbeidstaker bruker sosiale medier som privatperson. Det vil si at det kan få konsekvenser for arbeidsforholdet dersom arbeidstaker omtaler arbeidsgiver på en illojal måte på sosiale medier.

Det er viktig å være klar over at ytringer i lukkede grupper som når mer enn 20 - 30 personer, er å betrakte som offentlig ytring, jfr (Kilder: Lovdata, Straffeloven§ 135 a, Ot.prp. nr. 90 (2003-2004) punkt 12.2.2 side 163

Tilbake til søk

Relaterte dokumenter
- Databrukerkontrakt
- Loggbehandling
- Passordrutiner - nettverkspassord
- Personregistre - prosedyre for opprettelse, bruk og sletting
- Rutiner for bruk av E-post

Relaterte lenker
- Forskrift til lov om personopplysninger
- Helsepersonelloven
- Helseregisterloven
- Lov om behandling av personopplysninger

Vedlegg
- Sjekkliste ved behov for nettverkstilgang Sykehuset Levanger
- Sjekkliste ved behov for nettverkstilgang Sykehuset Namsos