Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Retningslinjer for daglig informasjonssikkerhet (Mal for sikkerhetsinstruks)

Støttedokument
Faktaark nr 27
Versjon: 4.1
Dato: 28.09.2018

Formål	Alle medarbeidere skal opptre på en slik måte i det daglige at de ivaretar god informasjonssikkerhet i virksomheten. Faktaarket kan brukes som mal for virksomhetens brukerinstruks.		
Ansvar	Virksomhetens ledelse er ansvarlig for at alle medarbeidere er kjent med og følger retningslinjer for informasjonssikkerhet. Den enkelte medarbeider har ansvar for å etterleve virksomhetens retningslinjer for informasjonssikkerhet. Virksomhetens ledelse er ansvarlig for at nødvendig opplæring blir gitt		
Gjennomføring	Retningslinjer for daglig informasjonssikkerhet må følges opp kontinuerlig.		
Omfang	Alle virksomheter skal ha retningslinjer for daglig informasjonssikkerhet. Omfanget av retningslinjene må tilpasses virksomhetens type og størrelse.		
Målgruppe Dette faktaarket er spesielt relevant for:	☐ Leverandør ☐ IKT-ansvarlig ☐ Forsker ☐ Prosjektleder	☒ Sikkerhetsleder / sikkerhetskoordinator ☒ Virksomhetens leder/ledelse ☐ Forskningsansvarlig	☒ Medarbeider/ansatt ☒ Databehandler ☐ Personvernombud
Hjemmel	• Personvernforordningen artikkel 32 • Pasientjournalloven § 22 • Helsepersonelloven § 16 • Andre aktuelle bestemmelser finnes i pasient- og brukerrettighetsloven kapitler 3 og 5.		
Referanser	Den Norske Legeforenings "Ti tommelfingerregler" plakat for informasjonssikkerhet på kontoret www.legeforeningen.no https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/normen/mal-for-internkontroll-psykologer-fysioterapeuter-manuellterapeuter-og-kiropraktorer		

Merknad 28.09.2018: 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.

Kjøreregler for informasjonssikkerhet i praksis	Tips og råd
Du skal ikke dele brukernavn og passord med andre	• Ansvar og aktivitet knyttet til journal skal knyttes til enkeltperson • Et passord er lett å huske for meg, men ikke av andre • Du kan bli beskyldt for feil eller aktiviteter som andre som låner passordet ditt har gjort.
Tilgang til og bruk av pasientjournal skal begrunnes ut fra tjenstlige behov, skal kun sendes dit pasienten selv angir, utleveres til pasienten selv eller etter fullmakt. Journal kan også sendes ny fastlege etter ønske fra pasienten	• Journalen eies av pasienten • Pasienten bestemmer – vi forvalter
Man skal alltid logge av PC, lås alltid når du går i fra	• Windows knapp og L • Ctrl+Alt+Delete • Fjerne smartkort
Du skal ikke lagre pasientopplysninger ukryptert på bærbart utstyr som for eksempel minnepinne	• Minnepinne er lett å miste og skal merkes og oppbevares forsvarlig

	• Ta ikke med bærbart utstyr med ukrypterte pasientopplysninger utenfor kontoret/arbeidsplassen • Lagre pasientopplysninger slik arbeidsgiver har bestemt
Du skal ha kontroll på dokumentene dine	• Hente utskrifter med en gang • Skriv ut kun det du må • Ikke legge igjen dokumenter på møterom • Ha gode makuleringsrutiner
Du vet hva du kan og ikke kan lese	• Det er forbudt å lese, søke eller på annen måte tilegne seg eller bruke opplysninger uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift • Ikke lov å åpne i ektefelles, slektningers eller din egen journal, uten grunn.
Du vet hva og med hvem du kan dele pasientinformasjon	• Taushetsplikt gjelder også mellom helsepersonell • Pass på at ikke uvedkommende lytter når du snakker om pasienter med en kollega, i telefon eller på offentlig sted • Pass på at uvedkomne ikke har innsyn • Når du deler pasientopplysninger med andre må du forsikre deg om at vedkommende du kommuniserer med har rett til å få opplysningene. Mottar du f.eks. telefonsamtaler om pasienter, og du er i tvil om identiteten til innringer, kan du be om å få ringe vedkommende tilbake.
Du sender ikke pasientinformasjon på SMS eller på e-post	• Dobbeltsjekk at e post/SMS du sender ikke inneholder pasientinformasjon • Ikke svar pasienter på e post/SMS • Benytt godkjente løsninger
Jeg kommenterer ikke jobb på sosiale medier og er forsiktig når jeg bruker nettsamfunn	• Husk taushetsplikten • Vær forsiktig og ikke røp sensitiv informasjon • Det er ingen angreknapp på internett • Avslå venneforespørsler fra pasienter for å unngå å komme i konflikt med taushetsplikten
Jeg vet hvordan jeg melder avvik	• Bruk avvikssystemet • Se på det som et forbedringstiltak som gjør at man lærer av feil og kan endre rutiner
Vær kritisk til lenker og innhold i e post	• Obs uærlige aktører med baktanker • Du kan få virus og infisere datamaskinen • Ramme arbeidsgiver

Eksempel

Eksempler på regler for bruk av informasjonsteknologi:

a) Privat bruk av informasjonssystemet skal godkjennes
b) Bruk av informasjonssystemet fra hjemmekontor eller på reise skal godkjennes
c) Flytting/kopiering av helse- og personopplysninger (over på minnepinne, CD mv.) skal godkjennes

d) Alle data skal sikkerhetskopieres
e) Utskrifter med helse- og personopplysninger skal oppbevares i låsbart skap og makuleres etter bruk
f) Elektronisk forsendelse av helse- og personopplysninger (e-post, meldingsutveksling mv.) skal krypteres
g) Ved fravær fra arbeidsplass og ved arbeidsdagens slutt skal bruker logge ut av alle systemer
h) Alle brukere skal ha egen brukernavn og passord til alle systemer
i) Oppbevaring, bruk og sikring av passord/PIN-kode/sikkerhetskoder for elektronisk ID skal være iht. fastlagte prosedyrer
j) Brukernavn og passord skal ikke oppgis på telefon eller e-post
k) Forespørsler om pasient via e-post skal ikke besvares
l) Det er ikke tillatt å søke etter informasjon man ikke har behov for eller ikke er autorisert for
m) Kun jobbrelatert informasjon fra Internett kan lastes ned
n) Programvare skal ikke installeres uten godkjennelse
o) E-post og vedlegg til e-post fra mistenkelig ukjent avsender skal ikke åpnes
p) Nødprosedyrer skal etableres
q) Feilsituasjoner skal håndteres iht. fastlagte prosedyrer
r) Avvik skal rapporteres i avvikssystemet
s) Virksomheten kan ha innsynsrett i arbeidstakers e-postkasse som arbeidsgiver har stilt til disposisjon til bruk i arbeidet. Tilsvarende har arbeidsgiver adgang til gjennomsøking av og innsyn i arbeidstakers personlige område i virksomhetens datanettverk og i andre elektroniske kommunikasjonsmedier eller elektronisk utstyr som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet