

» Informasjonssikkerhet

KITH

INFORMASJONSTEKNOLOGI
FOR HELSE OG VELFERD

Epost – sikker kommunikasjon?

Avdelingssjef Bjarte Aksnes, KITH

Tema

- Hvilket ansvar har virksomheten
- Hvilket ansvar har vi som mottakere og avsendere av epost
- Prinsipper for epost
- Retningslinjer for epost
- Pasient- og klientkommunikasjon

Min påstand: Den største trusselen er ikke at andre "snapper opp" informasjonen underveis, men manglende rutiner og systemer for å håndtere og videreformidle informasjonen internt

Virksomhetens ansvar

- Offentlighetsloven
- Personopplysningsloven og Helseregisterloven
 - Skal etablere tilfredsstillende informasjonssikkerhet
 - Elektronisk behandling av personopplysninger skal tilfredsstille sikkerhetskravene i personopplysningsloven § 13 og forskriften kapittel 2
 - Virksomheten skal videre blant annet utarbeide sikkerhetsmål og strategi, lage rutiner samt sørge for at ansatte har nødvendig kompetanse. Prosedyrer og rutiner skal dokumenteres skriftlig.
 - Ved ekstern overføring av sensitive personopplysninger stilles det i tillegg krav om kryptering eller sikring på annen måte.
- eForvaltningsforskriften

Personlig- eller virksomhetsrelatert-epost

- **Virksomhetsrelatert epost**

E-postadresser av typen postkasse@helseforetaket.no eller hjerteavdelingen@helseforetaket.no fremstår som klart virksomhetsrelatert. Verken avsender eller mottaker av e-posten vil ha en berettiget forventning om at e-post som sendes til slike adresser skal behandles som privat post.

- **Personlig e-postadresse**

De fleste virksomheter benytter e-postadresser som angir den ansattes navn, initialer eller lignende i adressen og deretter virksomhetens navn, slik som ola.nordmann@helseforetaket.no eller on@hf.no

Sensitive personopplysninger

- Sensitive personopplysninger er opplysninger om helseforhold, rase, politisk eller religiøs oppfatning og medlemskap i fagforeninger. Det er også opplysninger som angir om en person har vært mistenkt, tiltalt eller dømt for straffbart forhold. (Se personopplysningsloven § 2 nr. 8)
- Konesesjonsplikt er hovedregelen etter personopplysningsloven ved behandling av sensitive opplysninger. Det er imidlertid et unntak for behandling av sensitive personopplysninger som er avgitt uoppfordret. (Personopplysningsloven § 33.)
- Unntak for behandling av helseopplysninger

Norm for informasjonssikkerhet

- Felles krav til informasjonssikkerhet, spesielt med henblikk på elektronisk behandling av helse- og personopplysninger
- Norm for informasjonssikkerhet i helsesektoren (se www.kith.no)
- Faktaark 32: elektronisk pasient- og klientkommunikasjon
- Faktaark 33: Bruk av e-post

Fra faktaark for epost –

1. tradisjonell epostløsninger

- Standard programvare for e-post skal ikke benyttes for utveksling av helse- og personopplysninger.
- Virksomhetens fagsystemer skal benyttes for elektronisk kommunikasjon av helse- og personopplysninger. Dette for å sikre at blant annet journalverdig informasjon journalføres, at informasjonen knyttes til riktig pasient og sikres ved hjelp av virksomhetens løsninger for tilgangsstyring.
- Kommunikasjon av helse- og personopplysninger bør gjøres ved å implementere strukturerte meldinger for pasientkommunikasjon (som epikrisemelding, henvisningsmelding osv.) i virksomhetens fagsystem. Dette gjelder også ved telemedisinske løsninger som overfører helse- og personopplysninger.

2. Bruk av virksomhetens e-post-løsninger

- Virksomheten skal unngå å legge til rette for at pasienter/klienter kan oversende helseopplysninger pr. e-post. Følgende bør unngås:
 - Personlige e-postadresser bør ikke legges ut på offentlig tilgjengelig nettsted
 - Virksomhetens offentlig tilgjengelige nettsted bør fraråde pasienten å oversende helse- og personopplysninger via e-post, evt. henwise til en sikker tjeneste for slik kommunikasjon
 - Hvis virksomheten likevel mottar helse- og personopplysninger fra pasienter, bør pasient/klient oppfordres til å avslutte slik kommunikasjon, og evt. henvises til en sikker tjeneste

3. Dedikert løsning med e-postfunksjonalitet for kommunikasjon av helse- og personopplysninger

- Generelt bør det benyttes fagsystemer for elektronisk kommunikasjon av helse- og personopplysninger.
- E-postløsningen som benyttes for helse- og personopplysninger må:
 - sikre at **alle** oversendinger blir kryptert
 - sikre at kun forhåndsdefinerte mottakere (f.eks. mottakere i virksomhetens katalogtjeneste) kan motta e-post fra løsningen
 - ha tilstrekkelig virusbeskyttelse og beskyttelse mot uønsket e-post/spam
 - Avsender må være sikker på at mottaker også har slike tiltak implementert. Virksomheten må også ha rutiner som sørger for at journalverdig informasjon fra dette systemet blir riktig journalført.

4. E-post for administrativ/tjenstlig bruk

- Virksomheter som implementerer e-postløsninger for administrative/tjenstlige kommunikasjonsbehov (som ikke omfatter helse- og personopplysninger), må implementere denne løsningen slik at den ikke eksponerer interne systemer og helse- og personopplysninger for risiko. Dette kan innebære:
 - E-postløsningen nås bare gjennom terminalserverløsning
 - Det benyttes løsninger for å forhindre klipp-og-lim mellom applikasjoner med helse- og personopplysninger og e-postsystemet
 - Det benyttes løsninger for virusbeskyttelse og begrenning av uønsket e-post/spam.

5. Retningslinjer for bruk av e-post

- Virksomheten bør etablere retningslinjer for e-post som beskriver hvordan sluttbruker skal/kan benytte e-postløsningen. Retningslinjene bør omfatte:
 - Hva e-post kan/ikke kan benyttes for
 - Hvorvidt noen andre enn brukeren selv kan ha tilgang til e-postkontoen
 - Retningslinjer for vedlegg til e-post
 - Retningslinjer knyttet til masseutsending av e-post
- Eksempel

Eksempel på retningslinjer for epost

- Helse- og personopplysninger skal aldri sendes via vår vanlige e-postløsning.
- Dersom du får e-post med helse- og personopplysninger (for eksempel fra en pasient eller kollega) så meld tilbake til vedkommende om at dette frarådes, og evt. henvis til sikker tjeneste.
- Åpne ikke e-post fra ukjente avsendere.
- Åpne ikke vedlegg i en mistenkelig e-post (for eksempel dersom du uventet får en e-post på engelsk).
- Kontroller adressen(e) en ekstra gang før du sender e-post.

Retningslinjer forts.

- Kontroller at du sender med korrekt vedlegg.
- Vær forsiktig med å legge igjen din e-postadresse på websider, nyhetsgrupper, chatte-kanaler og lignende. Undersøk først betingelser og seriøsitet. Bruk eventuelt en privat e-postadresse på slike tjenester.
- Ikke spre jobb-e-postadressen din ukritisk til mange. Bruk flere e-postadresser, for eksempel én i jobbsammenheng, en annen i kontakt med venner og en tredje for kontakt med ukjente personer, innlegg på diskusjonsforum osv.
- Ikke bruk automatisk svar i e-postprogrammet. Ved bruk av automatisk svar forstår spammere at e-postadressen er i bruk.
- Ikke videresend kjedebrev.

Hva bør gjøres når sensitiv informasjon mottas uoppfordret?

- Gi standard svar tilbake med opplysninger om hvilke muligheter man har for å komme i kontakt (telefon, brev, ev. egen IT-løsning)
- Husk: man kan ikke være sikker på om avsenderen er den vedkommende gir seg ut for å være
- Derfor gis aldri personlige opplysninger eller svar på spørsmål om personlige forhold tilbake i epost
- Vis til en egen nettside der man gir utfyllende opplysninger ift personvern og sikkerhet
- Dersom informasjonen vurderes som kritisk ift. liv og helse viderefremmes snarest til aktuell avdeling eller person på en hensiktsmessig måte (telefon, papir). Den som mottar informasjonen bør forsøke å komme i kontakt med vedkommende på telefon el. for å få bekreftet opplysningene. Dette må dokumenteres i EPJ.
- Sørg for å slette korrespondansen fra arkivsystemet

§ 5. *Formidling av taushetsbelagte opplysninger og personopplysninger til forvaltningen*

- (1) Når et forvaltningsorgan legger til rette for bruk av elektronisk kommunikasjon for mottak av opplysninger som på forvaltningens hånd kan være underlagt taushetsplikt, eller som kan være underlagt krav til sikring etter reglene om behandling av personopplysninger eller tilsvarende regler, skal risiko for uberettiget innsyn i opplysningene være forebygget på tilfredsstillende måte.
- (2) Forvaltningsorgan som legger til rette for å motta opplysninger som nevnt i nr. (1), skal på hensiktsmessig måte informere om eventuelle risikoer ved elektronisk overføring av slike opplysninger og om hva som er rette elektroniske adresse.
- (3) Forvaltningsorganet skal opplyse generelt om hvordan taushetsbelagte opplysninger og personopplysninger sikres under behandling i forvaltningsorganet.

eForvaltningsforskriften

§ 6. *Bekreftelse på at en henvendelse er mottatt*

- (1) Et forvaltningsorgan som mottar henvendelser i elektronisk form skal gi bekreftelse til avsender om at en henvendelse er mottatt.
- (2) Bekreftelse bør gis straks henvendelsen er mottatt. Den bør inneholde et referansenummer eller lignende og angi på hvilket tidspunkt henvendelsen ble mottatt.
- (3) Forvaltningsorganet kan unnlate å sende bekreftelse, hvis henvendelsen er av en slik art at den ikke utløser saksbehandling, eller mottaket fremgår på annen betryggende måte, og ved bruk av automatiserte systemer der henvendelsen straks blir besvart. Forvaltningsorganet kan også inngå avtale med næringsdrivende og med andre forvaltningsorganer om ikke å sende egen bekreftelse etter denne bestemmelsen i forbindelse med rutinemessig eller periodisk rapportering.

eForvaltningsforskriften

§ 7. *Henvendelser som ikke tilfredsstiller aktuelle krav*

- (1) Henvender noen seg til urette myndighet eller benytter uriktig elektronisk adresse ved en henvendelse til et forvaltningsorgan, skal det forvaltningsorgan som mottar henvendelsen, gi avsender beskjed om feilen og om mulig vise vedkommende til rett organ og rett elektronisk adresse, jf. forvaltningslovens § 11.
- (2) Er en henvendelse avgitt i en annen form eller på en annen måte enn det som er angitt i eller i medhold av forskriften her, skal organet gi avsenderen beskjed om dette dersom feilen har betydning for behandling av saken eller det av andre grunner finnes nødvendig. Organet bør samtidig gi frist til å rette opp feilen og gi veiledning om hvordan dette kan gjøres.
- (3) Forvaltningsorganet skal registrere tidspunkt for når det er sendt varsel etter nr. (1) og (2) ovenfor, og til hvem varselet ble sendt. Dersom feilen er av en slik art at det ikke er mulig å identifisere avsender, og varsel ikke kan sendes, skal det registreres opplysning om dette.

Sikker epost?

- Teknologisk er dette mulig (PKI)! MEN...
- Krever at man har identifisert og godkjent brukeren på forhånd (autorisering)
- Krever at brukeren har en teknologisk løsning for sterkt autentisering (smartkort, kodekort, mobil e)
- Krever et mottakssystem for utpakking, verifisering, logging, arkivering og videreformidling
- Generelt: frarådes det å bruke "sikker epost"
- Derimot kan man lage egne løsninger for pasient-klientkommunikasjon (web-baserte)

Fra normen: Kommunikasjon med pasienter/brukere

Virksomheten er ansvarlig for at

- Samtykke fra pasienten/brukeren er innhentet til å formidle *helse- og personopplysninger* elektronisk. Samtykke skal innhentes i tråd med alminnelige regler for samtykke. Samtykke fra pasienten er etter denne *normen* det eneste grunnlaget for datakommunikasjon med pasienter/brukere.
- Pasienten/brukeren entydig identifiseres.
- *Tekniske tiltak* iverksettes slik at all kommunikasjon krypteres.
- Det ikke skal kunne kommuniseres samtidig med andre parter enn den angitte pasient/bruker.
- *Helse- og personopplysninger* skal ikke stilles til rådighet på en slik måte at pasient/bruker er avhengig av å lagre opplysningene på eget utstyr for å gjøre seg kjent med informasjonen.

Fra faktaark: Elektronisk pasient-klientkommunikasjon

- Tradisjonelle e-postløsninger skal ikke benyttes for kommunikasjon av helse- og personopplysninger med pasienter/klienter. Vanlig e-post eller SMS skal aldri brukes til å bære slik sensitiv informasjon.
- For pasient-/klientkommunikasjon skal det benyttes tjenester som er spesielt tilrettelagt for slik kommunikasjon..
- Alle helse- og personopplysninger skal være kryptert under overføringen over åpne nettverk som internett eller Norsk helsenett
- For å sikre at kun riktig personer får tilgang til informasjon i løsningen må brukerne autentiseres.
- Journalverdig informasjon fra pasient-/klientkommunikasjonen skal journalføres. Det bør være mulig å overføre informasjon fra kommunikasjonen til et system der dette kan journalføres (for eksempel til virksomhetens EPJ-system).

Hovedprinsipper for løsninger med pasient- og klientkommunikasjon

- Pasienten/klienten bør kunne bruke "standard" programvare for tilgang til den elektroniske løsningen (for eksempel standard nettlesere)
- Løsningen må vanskeliggjøre lokal lagring av helse- og personopplysninger ute hos brukeren. Løsningen skal ikke presentere informasjon slik at det er nødvendig for pasient/klient å lagre informasjonen lokalt på egen PC for å gjøre seg kjent med informasjonen
- Data skal ikke lagres i løsningen lenger enn nødvendig
- Det må kreves samme sikkerhetsnivå ved tilgang til slike tjenester som ved tilgang til andre systemer med helse- og personopplysninger

Helsevirksomhet



- Mottar og behandler forespørsler fra pasient/klient
- Kan kommunisere og/eller utlevere informasjon til pasient/klient

Norsk Helsenett

Løsning for pasient-/klientkommunikasjon



- Gir pasient/klient tilgang til utlevert informasjon fra legekantoret
- Ivaretar sikkerhet både i forhold til helsevirksomhet og pasient/klient. Dette gjelder blant annet overføringssikkerhet og autentisering av pasient/klient

Internett

Pasient/klient



- Bør kunne bruke standard programvare (for eksempel nettleser) for å kommunisere med helsepersonell
- Får tilgang til utleverte helse- og personopplysninger fra legekantoret gjennom dedikert løsning for dette, for eksempel et nettsted

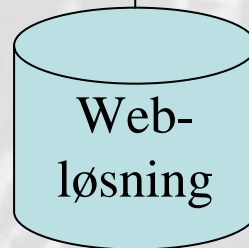
Løsning for mottak av korrespondanse

Avsender

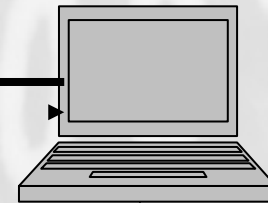
Sender informasjon



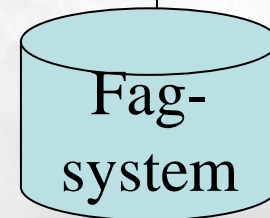
Web-skjema for innsending



Helseforetak



Mottak, Registrering



Spørsmål?

www.kith.no

Bjarte.Aksnes@kith.no