Norm for informasjonssikkerhet i helsesektoren

Utgitt med støtte av: Helsedirektoratet

Bruk av e-post ifm helseopplysninger

Støttedokument
Faktaark nr 33
Versjon: 2.0
Dato: 03.12.2009

Målgruppe Dette faktaarket er spesielt relevant for:	☐ Leverandør ☒ IKT-ansvarlig ☐ Forsker ☐ Prosjektleder	☒ Sikkerhetsleder / sikkerhetskoordinator ☐ Virksomhetens leder/ledelse ☐ Forskningsansvarlig	☐ Medarbeider/ansatt ☐ Databehandler ☐ Personvernombud
Ansvar	Sikkerhetsleder / sikkerhetskoordinator skal påse at det finnes retningslinjer for bruk av e-post.		
Gjennomføring	Ved etablering eller endring av e-postløsning.		
Formål	Sikre at e-post benyttes på en forsvarlig måte i virksomheten.		
Omfang	Bruk av e-post ifm helseopplysninger i virksomheten.		
Hjemmel	Personopplysningsforskriften §§ 2 – 11 Sikring av konfidensialitet, 2 – 12 Sikring av tilgjengelighet og 2 – 13 Sikring av integritet		
Referanser	Norm for informasjonssikkerhet i helsesektoren, kapittel 5.7.2 og 5.7.3		

Nr.	Handling/Utførelse
1.	**Bruk av virksomhetens e-postløsninger** - Standard programvare for e-post skal ikke benyttes for utveksling av helse- og personopplysninger. - Virksomheten skal unngå å legge tilrette for at pasienter/klienter kan oversende helse- og personopplysninger pr. e-post. Følgende bør unngås: o Personlige e-postadresser bør ikke legges ut på offentlig tilgjengelig nettsteder o Virksomhetens offentlig tilgjengelig nettsted bør fraråde pasienten å oversende helse- og personopplysninger via e-post, evt. henvise til en sikker tjeneste for slik kommunikasjon o Hvis virksomheten likevel mottar helse- og personopplysninger fra pasienter, bør pasient/bruker oppfordres til å avslutte slik kommunikasjon, og evt. henvises til en sikker tjeneste
2.	**Dedikert løsning med e-postfunksjonalitet for kommunikasjon av helse- og personopplysninger** Benytter virksomheten e-postfunksjonalitet for kommunikasjon av helse- og personopplysninger, f.eks i forbindelse med telemedisin, skal det være et klart skille mellom denne løsningen og generell e-postløsning for virksomheten. 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.
3.	**E-post for administrativ/tjenestelig bruk** Virksomheter som implementerer e-postløsninger for administrative/tjenestelige kommunikasjonsbehov (som ikke omfatter helse- og personopplysninger), må implementere denne løsningen slik at den ikke eksponerer interne systemer og helse-/personopplysninger for risiko. Dette kan innebære: - E-postløsningen nås bare gjennom terminalserverløsning

Nr.	Handling/Utførelse
	- Det benyttes løsninger for å forhindre klipp og lim mellom applikasjoner med helse- og personopplysninger og e-postsystemet - Det benyttes løsninger for virusbeskyttelse og begrensning av uønsket e-post/spam
4.	**Retningslinjer for bruk av e-post** Virksomheten bør etablere retningslinjer for e-post som beskriver hvordan bruker skal/kan benytte e-postløsningen. Retningslinjene bør omfatte: - Hva e-post kan/ikke kan benyttes til - Hvorvidt noen andre enn brukeren selv kan ha tilgang til e-postkontoen - Retningslinjer for vedlegg til e-post - Retningslinjer ift. masseutsending av e-post

Eksempel på retningslinjer for bruk av e-post
- Helse- og personopplysninger skal aldri sendes som vanlig e-post - Dersom du får e-post med helse- og personopplysninger (for eksempel fra en pasient eller kollega) så meld tilbake til vedkommende om at 'blir ikke besvart eller behandlet videre i virksomheten' - Åpne ikke vedlegg i e-post som er mistenkelig eller ukjente avsendere - Kontroller adressen(e) før du sender e-posten - Kontroller at du sender med korrekt vedlegg - Vær forsiktig med å legge igjen din e-postadresse på websider, nyhetsgrupper, chat-kanaler og lignende. Undersøk først betingelser og seriøsitet. Bruk eventuelt en privat e-postadresse på slike tjenester - Ikke spre din personlige e-postadresse ukritisk. 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