Tidsskriftet Tidsskrift for Den norske legeforening

Helseopplysninger i private digitale kanaler

DEBATT

KJERSTI WILSON

kjersti.wilson@konsilito.no
Kjersti Wilson har master i rettsvitenskap og er personvernrådgiver hos Konsilito.
Forfatteren har fylt ut ICMJE-skjemaet og oppgir ingen interessekonflikter.

IDA THORSRUD

Ida Thorsrud har master i rettsvitenskap og er personvernrådgiver.
Forfatteren har fylt ut ICMJE-skjemaet og oppgir ingen interessekonflikter.

KARIANN KROHNE

Kariann Krohne er sosialantropolog, førsteamanuensis ved Institutt for folkehelsevitenskap, Norges miljø- og biovitenskapelige universitet og seniorforsker ved Nasjonalt senter for aldring og helse.
Forfatteren har fylt ut ICMJE-skjemaet og oppgir ingen interessekonflikter.

ANNE-LENE ARNESEN

Anne-Lene Arnesen er jurist og pasient- og brukerombud i Buskerud.
Forfatteren har fylt ut ICMJE-skjemaet og oppgir ingen interessekonflikter.

Kommuniserer du digitalt med og om dine pasienter i private kanaler? Det kan være i strid med helse- og personvernlovgivningen.

Noen virksomheter som tilbyr helsetjenester, oppgir e-postadresse eller mobilnummer på sine hjemmesider. Ofte informerer de samtidig om at helseopplysninger ikke skal gis på e-post eller SMS. Her er et eksempel fra en privat legepraksis:

«Utover telefontiden vår kan du sende SMS eller epost med kort beskrivelse av problemstillingen. Ikke oppgi helseinformasjon».

En oppfordring om å *ikke* gi helseinformasjon er ingen garanti for at pasientene lar være å gi helseopplysninger. Som helsepersonell må du alltid ta høyde for at de *kan* gjøre det – og du må ha en plan for hvordan du skal håndtere slike opplysninger.

Når du åpner for digital kommunikasjon i private kanaler som e-post, SMS, Messenger, WhatsApp eller Snapchat, er du ansvarlig for at taushetsplikten (1) og journalføringsplikten (2) overholdes. I tillegg må du sørge for at kommunikasjonskanalene er sikret i tråd med kravene til informasjonssikkerhet som følger av helselovgivningen (3) og personvernlovgivningen (4).

> ***«Kravene til informasjonssikkerhet er de samme, uavhengig av om helsepersonellet kommuniserer med pasienter gjennom virksomhetens digitale kanaler eller i private digitale kanaler»***

Vurder informasjonssikkerheten først

Helselovgivningen (3) og personvernforordningen (4) stiller krav til informasjonssikkerhet når kommunikasjon foregår i digitale kanaler. Kravene til informasjonssikkerhet er de samme, uavhengig av om helsepersonellet kommuniserer med pasienter gjennom virksomhetens digitale kanaler eller i private digitale kanaler.

Informasjonssikkerhet innebærer å beskytte konfidensialitet, integritet og tilgjengelighet av personopplysninger mot uautorisert tilgang, endringer eller ødeleggelser. Helseopplysninger er sensitive personopplysninger, og håndtering av disse har et iboende høyt risikonivå (5, 6). Den som behandler personopplysninger, må innføre passende tekniske og organisatoriske tiltak for å sikre dem (7).

Tekniske tiltak kan inkludere tilgangsstyring, passordbeskyttelse og logging (hvem bruker systemet, når og hvorfor). Organisatoriske tiltak kan være interne rutiner som angir hvilke systemer ansatte skal bruke i kommunikasjonen med pasienter.

Det er aldri tilstrekkelig å bare innføre tekniske og organisatoriske tiltak. Disse må også dokumenteres og etterleves i form av «tilgangsstyring, logging og etterfølgende kontroll» (8). For eksempel må nødvendige sikkerhetsoppdateringer utføres for å beskytte personopplysningene. Store helsevirksomheter har fagpersoner som ivaretar informasjonssikkerheten og

gjør slike sikkerhetsoppdateringer, men ved bruk av private kanaler er det du selv som er ansvarlig for å dokumentere informasjonssikkerheten og gjennomføre oppdateringer.

Husk at helseopplysninger som deles i private digitale kanaler, kan komme på avveie på grunn av menneskelig feil. Du kan ved et uhell sende en SMS eller e-post med helseopplysninger til feil person, eller låne bort mobiltelefonen til et familiemedlem som ser det som er sendt eller mottatt i Messenger eller som SMS. Det siste skjedde med den syv år gamle pasienten Truls. Han var hos fastlegen fordi han var hoven i ansiktet etter et vepsestikk. Fastlegen tok et bilde av Truls' ansikt med sin mobiltelefon for å konferere med en sykehuslege. Senere samme dag lånte fastlegen bort mobilen til sin datter som ville spille et spill. Datteren så da bildet av klassekameraten Truls med hovent ansikt – og fortalte dette til alle på skolen neste dag. Du må også være oppmerksom på at helseopplysninger kan komme på avveie hvis du ikke har gjennomført sikkerhetsoppdateringer på din private telefon eller pc, noe som gjør at enheten er mer sårbar for dataangrep. Blir helseopplysninger kompromittert gjennom et dataangrep, vil dette være brudd på både informasjonssikkerheten og den lovpålagte taushetsplikten.

Alltid ditt ansvar

Taushetsplikten gjelder uavhengig av kommunikasjonsform (1). Vær klar over at dersom du blir kontaktet i private digitale kanaler av pasienter eller pårørende, så er det ikke alltid nok å la være å svare dem. Det anbefales å slette opplysningene umiddelbart for å unngå å bryte taushetsplikten dersom andre får tilgang til telefonen, pc-en eller nettbrettet. Videre har private kanaler ingen automatisk funksjon for journalføring som den man for eksempel finner i Helsenorge-appen. For å ivareta journalføringsplikten, må du selv sørge for å dokumentere kommunikasjonen i pasientens journal. Manglende journalføring utgjør en pasientsikkerhetsrisiko (2, 9).

I Veileder for digital pasientkommunikasjon for helse- og omsorgssektoren (10) gis det gode eksempler på hvilke typer informasjon som kan gis i ulike digitale kanaler. Veilederen er et godt verktøy for deg som ønsker å lære hvordan du best mulig kan ivareta informasjonssikkerheten, taushetsplikten og journalføringsplikten.

REFERENCES

1. LOV-1999-07-02-64. Lov om helsepersonell m.v. (helsepersonelloven) § 21. https://lovdata.no/dokument/NL/lov/1999-07-02-64/KAPITTEL_5#KAPITTEL_5 Lest 7.3.2024.

2. LOV-1999-07-02-64. Lov om helsepersonell m.v. (helsepersonelloven) § 39. https://lovdata.no/dokument/NL/lov/1999-07-02-64/KAPITTEL_8#KAPITTEL_8 Lest 7.3.2024.

3. LOV-2014-06-20-42. Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) § 22 https://lovdata.no/dokument/NL/lov/2014-06-20-42/KAPITTEL_4#KAPITTEL_4 Lest 3.3.2024.

4. LOV-2018-06-15-38. Lov om behandling av personopplysninger (personopplysningsloven), artikkel 32. https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr-4-2#KAPITTEL_gdpr-4-2 Lest 3.3.2024.

5. LOV-2018-06-15-38. Lov om behandling av personopplysninger (personopplysningsloven), artikkel 9. https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr-2#KAPITTEL_gdpr-2 Lest 7.3.2024.

6. Normen. Veileder om risikostyring i informasjonssikkerhet og personvern. https://www.ehelse.no/normen/normen-dokumenter/Veileder-om-risikostyring-i-informasjonssikkerhet%20og%20personvern#2.3.6-nbsp-risiko Lest 12.4.2024.

7. LOV-2018-06-15-38. Lov om behandling av personopplysninger (personopplysningsloven), artikkel 24. https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr-4#KAPITTEL_gdpr-4 Lest 7.3.2024.

8. LOV-2018-06-15-38. Lov om behandling av personopplysninger (personopplysningsloven), artikkel 5. https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr-2#KAPITTEL_gdpr-2 Lest 7.3.2024

9. LOV-1999-07-02-64. Lov om helsepersonell m.v. (helsepersonelloven) § 40. https://lovdata.no/dokument/NL/lov/1999-07-02-64/KAPITTEL_8#KAPITTEL_8 Lest 28.4.2024.

10. Normen. Veileder i digital pasientkommunikasjon for helse- og omsorgssektoren. https://www.ehelse.no/normen/normen-dokumenter/Veileder%20i%20digital%20pasientkommunikasjon/_/attachment/inline/8ab10456-9856-4b6c-bf29-ef57c74db8db:581884ccb8adbf06f7eccc03e014c3eafa5d209c/Veileder%20digital%20pasientkommunikasjon.pdf Lest 29.2.2024.

Publisert: 23. mai 2024. Tidsskr Nor Legeforen. DOI: 10.4045/tidsskr.24.0155
Mottatt 15.3.2024, første revisjon innsendt 16.4.2024, godkjent 19.4.2024.