ENDRINGER FRA FORRIGE VERSJON: Korrigert lenke og henvisning til godkjente tekniske løsninger.

HENSIKT

Hensikten med denne prosedyren er å sikre at utlevering av helse - og personopplysninger, inkludert forskningsopplysninger, skjer med tilfredsstillende informasjonssikkerhet.

MÅLGRUPPE

Alle ansatte ved SSHF.

FREMGANGSMÅTE

Det forutsettes at det foreligger et lovlig grunnlag eller formål for utlevering av helse- og personopplysninger, jf Utlevering av helse- og personopplysninger

Kontroll av sikkerhet ved ekstern utlevering

Ved utlevering av helse- og personopplysninger fra SSHF har både sykehuset og mottakende virksomhet et felles juridisk ansvar for at overleveringen skjer på en måte som ivaretar konfidensialitet, integritet og tilgjengelighet. Når utleveringen skjer til annen juridisk enhet, er det likevel mottakende juridiske enhet som i hovedsak er ansvarlig for at nødvendig sikkerhet er etablert. Ved elektronisk utlevering, vil sykehuset ha et ansvar for at utleveringen gjøres uten at uvedkommende får tilgang til opplysningene. Normalt vil følgende måtte være på plass:

- Kryptering av den elektroniske overføringen, slik at ikke uvedkommende kan avlytte forbindelsen. Slik kryptering kan ivaretas eksempelvis server til server, evt ved at filer/vedlegg krypteres.
- Pålogging med sertifikat for å få tilgang til nettside hvor opplysninger registreres (lastes opp). Herfra er det mottakende juridiske enhet som overtar ansvaret.
- Den ansatte skal føre kontroll med at det ikke ligger igjen usikrede kopier på sykehusets maskin/utstyr som ble brukt for registrering på ekstern nettside.
- Utlevering kan også gjøres med krypterte meldinger.
- Fysisk forsendelse av fysiske lagringsmedier kan benyttes når elektronisk overføring ikke er hensiktsmessig. Dette forutsetter at dataene er kryptert, eller at selve lagringsmediet ivaretar krypteringen.

Kontroll av sikkerhet ved intern utlevering

Kravene til sikkerhet gjelder også ved intern overføring, dvs at overføringen må gjøres på en slik at måte at ikke uautorisert innsyn kan forekomme. Dette innebære i praksis at kravene som nevnt i kulepunktlisten ovenfor også gjelder ved denne type overføring. Samtidig må mottaker påse at det kun benyttes godkjente løsninger for lagring av dekrypterte filere og videre behandling av disse.

Godkjente løsninger for overføring

Se denne siden Intranett - kommunikasjonskanaler for oversikt og IKT-løsninger og hva de kan benyttes til.

Merk at eDialog/eFormidling og Altinn har begrensninger i størrelsen på vedlegg og filer som kan sendes. Alternativt kan tjenesten «Secure Mail» benyttes. Her er maksimum størrelse pr fil som kan sendes 1Gb.

Filer som er større enn dette må deles opp, eksempelvis ved bruk av verktøyet 7-Zip. Se sidene: «Brukerveiledning for SecureMail» og «Bestilling av tilgang til SecureMail»

For bruk av lagringsmedier (USB minnepinner ol), se IKT: Retningslinje for bruk av flyttbare lagringsenheter. Her finnes lenker videre til veiledere for kryptering av dokumenter og filer og bruk av SafeConsole/IronKey.

Godkjente løsninger for lagring

I tillegg til våre fagsystemer lagrer og behandler vi også helse- og personopplysninger utenfor disse fagsystemene. Se Lagring av data utenfor fagsystemer for mer informasjon.

Har du spørsmål til innholdet i dette dokumentet eller til hvordan du ivaretar informasjonssikkerheten ved overføring og utlevering kan du kontakte informasjonssikkerhetsleder i SSHF via epost til informasjonssikkerhet@sshf.no. Se også denne siden: Intranett - temaside Informasjonssikkerhet og personvern.

Kryssreferanser

I.5.9.2-6	IKT: Retningslinje for bruk av flyttbare lagringsenheter
I.5.9.2-9	Lagring av data utenfor fagsystemer
I.5.9.2-11	Utlevering av helse- og personopplysninger

Eksterne referanser

15.34.8 Intranett - kommunikasjonskanaler

15.34.9 Intranett - temaside Informasjonssikkerhet og personvern