WEBINAR:
Bruk av databehandler i helse- og omsorgssektoren

21. april 2021

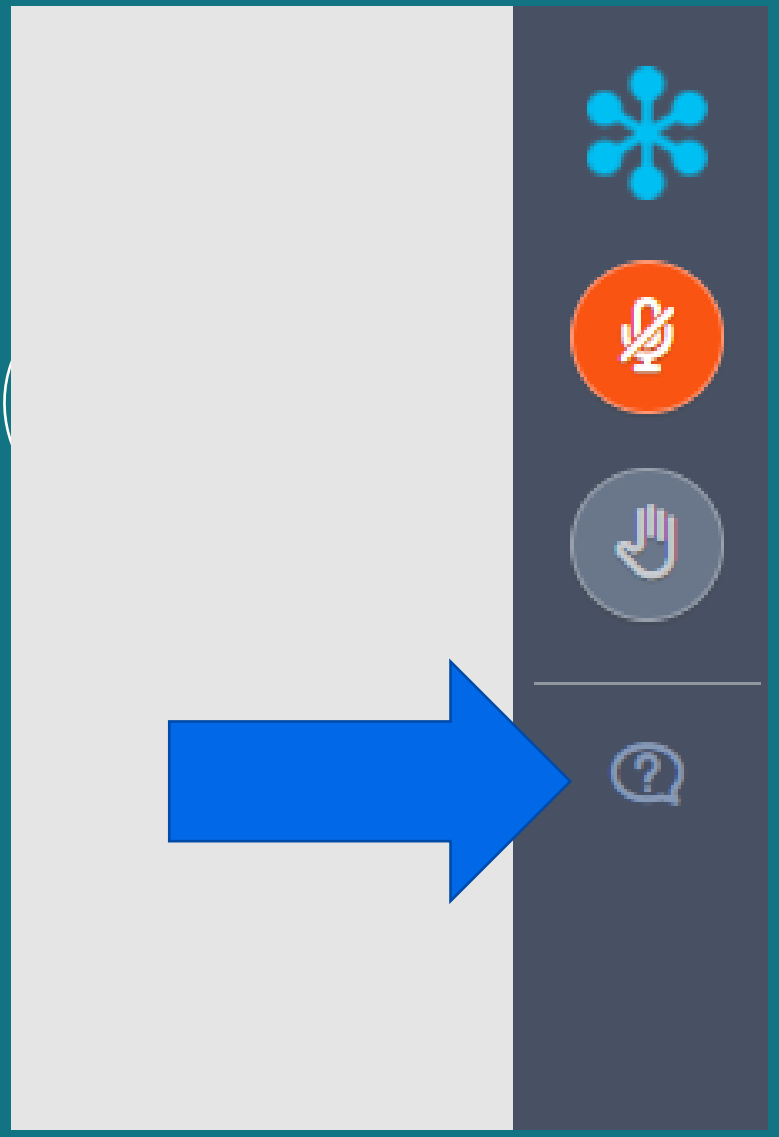
Kjøreregler

- Møteleder styrer ordet
- Deltagernes mikrofoner er mutet som standardinnstilling
- Det foretas opptak av dette webinaret
- Presentasjonene legges ut på kurssiden på normen.no

- Vil du vite mer om hvordan vi jobber med GoToWebinar? Se mer på https://ehelse.no/normen/aktuelt-om-normen/digital-kompetanseheving-med-normen

Spørsmål underveis

- Bruk spørsmålsfunksjonen når som helst under foredragene
- Vi svarer på spørsmål enten i plenum og/eller i chat
- Vi lagrer spørsmålet ditt, men ikke hvem det kommer fra
- Hvis du har spørsmål som ikke blir besvart under kurset, send oss en epost til sikkerhetsnormen@ehelse.no



Agenda

- Innholdet i faktaarket
- Ny mal fra Direktoratet for e-helse
- Noen vanlige problemstillinger
- Spørsmål fra salen

NORMEN

Om faktaarket

- En del av Normens arbeid med oppdatering av veiledningsmateriell
  - Innholdet i dokumentet er gjennomgått og oppdatert ut fra Normen 6.0, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

- Kravene i faktaarket bygger på kravene i Normens hoveddokument, særlig kapittel 5.7.4.

- Dokumentet er ikke bygget opp rundt en mal for databehandleravtale, men følger Normens krav til databehandler(e) og tilhørende krav.

5.7.4 Databehandler

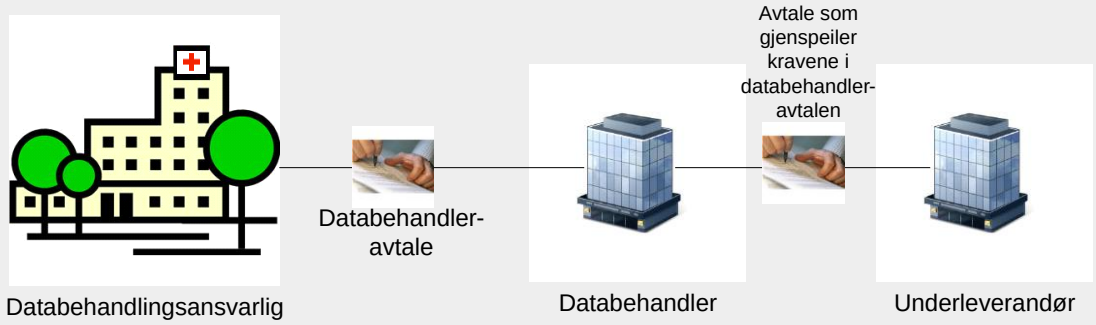
Databehandler skal bare behandle helse- og personopplysninger, samt annen taushetsbelagt informasjon etter instruks fra dataansvarlig. Hvordan databehandler kan behandle data på vegne av dataansvarlig, skal reguleres i avtale.

Den dataansvarlige kan bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personopplysningsloven. Tilstrekkelige garantier betyr at databehandleren oppfyller kravene i lov og forskrift samt de kravene fra Normen som er relevante for det aktuelle avtaleforholdet.

Databehandleren skal ikke engasjere underleverandører uten at det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra den dataansvarlige. Dersom det er innhentet en generell, skriftlig tillatelse, skal databehandleren underrette den dataansvarlige om eventuelle planer for endring av underleverandører. Den dataansvarlige skal kunne motsette seg slike endringer.

De syv fasene

1) Valg av databehandler
2) Beslutning om bruk av ekstern driftsenhet
3) Identifisering av ekstern driftsenhet
4) Utforme databehandleravtale
5) Følge opp en databehandleravtale
6) Krav til tilbakerapportering
7) Avslutning av databehandleravtale



1) Valg av databehandler

- Valg av leverandør av en tjeneste som behandler helse- og personopplysninger på vegne av virksomheten (dataansvarlig).

- Virksomheten kan bare bruke databehandlere som oppfyller kravene i lov og forskrift samt Normens kapittel 3 og 4, og de kravene fra Normen som er relevante for det aktuelle avtaleforhold.

- Databehandleren skal ikke engasjere underleverandører uten at det på forhånd er innhentet skriftlig tillatelse til dette fra virksomheten, med mindre det er innhentet en generell, skriftlig tillatelse eller en slik tillatelse fremgår av databehandleravtalen.

2) Beslutning om bruk av ekstern driftsenhet

- Etter at beslutningen om at IKT-systemer (alle eller noen) skal driftes av en ekstern driftsenhet og før IKT-systemene faktisk settes ut for drifting skal det inngås en databehandleravtale.

3) Identifisering av ekstern driftsenhet

- Etter at beslutningen om at IKT-systemer (alle eller noen) skal driftes av en ekstern driftsenhet og før IKT-systemene faktisk settes ut for drifting skal det inngås en databehandleravtale.
- Skal ha oversikt over alle eksterne driftsenheter.

4) Utforme databehandleravtale

- Databehandler har et selvstendig ansvar for informasjonssikkerheten etter pasientjournalloven § 22, helseregisterloven § 21 og personvernforordningen artikkel 28 og 29, herunder underleverandører.

- Beskrevet en rekke minimumskrav som retter seg mot både innretting og utforming av avtalen, for eksempel beskrivelse av plikter for dataansvarlig og databehandler

5) Følge opp en databehandleravtale

- Dataansvarlig skal ha innsyn i databehandlers prosedyrer og praksis for informasjonssikkerhet for å sikre at denne er tilfredsstillende iht. kravene.

- Det anbefales at det utformes en praktisk måte å håndtere dette på ifm, avtalens utforming, særlig for mindre virksomheter.

- Følgende momenter bør vurderes og beskrives nærmere, avhengig av virksomhetens behov:
  - Databehandler plikter å følge Normen
  - Databehandler plikter å følge virksomhetens akseptkriterier (iht risikovurdering)
  - Databehandler plikter å gjennomføre logging
  - Mulighet for å gjøre endringer i databehandleravtalen (hvis den dataansvarliges sikkerhetsrevisjoner av databehandleren viser at dette er nødvendig)

6) Krav til tilbakerapportering

- Databehandler skal jevnlig rapportere status om resultater fra sine ansvarsområder.

7) Avslutning av databehandleravtale

- Krav til prosedyrer ved avslutning av avtaleforholdet/opphør av databehandleravtalen.
- Tilbakelevering og sletting av opplysninger hos databehandler. Sikre at databehandler fortsatt er bundet av taushetsplikten.

Standard databehandleravtale med veileder

Direktoratet for e-helse har utarbeidet en standard databehandleravtale med veileder for bruk i helse- og omsorgssektoren.

Last ned Standard databehandleravtale og veileder

Overføring av opplysninger til utlandet

Revidering

Standardavtalen skal bidra til å sikre at helse- og personopplysninger blir behandlet i samsvar med regelverket når aktører i sektoren velger å benytte databehandlere.

Direktoratet for e-helse ønsker at virksomheter i helse- og omsorgssektoren benytter denne standardavtalen når de skal inngå databehandleravtale som omfatter helseopplysninger.

Utbredt bruk av en standardisert avtale i sektoren vil forenkle både avtaleinngåelse og senere avtaleforvaltning for både dataansvarlige og databehandlere ettersom avtalestruktur og innhold blir ensartet og kjent.

Last ned Standard databehandleravtale og veileder

Last ned Standard databehandleravtale (Word)

Last ned veileder for databehandleravtalen (PDF)

Bakgrunn

Oppdrag i tildelingsbrev fra HOD:

«Utarbeide en standard databehandleravtale med veileder, som sektoren kan benytte ved inngåelse av slike avtaler»

- ***Større sikkerhet for at nødvendige krav dekkes***
- ***Enklere avtaleinngåelse/avtaleforvaltning***

NORMEN

Standardavtale

- Benyttet tidligere mal som utgangspunkt
  - Kartlegging
- Spisset mot helseopplysninger
  - Vise til Datatilsynet, DigDir for «vanlige» personopplysninger
- «Fast» avtale, endringer i et eget endringsvedlegg
- Kjent vedleggstruktur
  - Vedlegg 1: Behandlingens formål, opplysninger og behandlinger
  - Vedlegg 2: Detaljerte krav til informasjonssikkerhet
  - Vedlegg 3: Administrative opplysninger
  - Vedlegg 4: Underleverandører
  - Vedlegg 5: Endringer i den generelle avtaleteksten ved avtaleinngåelsen
  - Vedlegg 6: Endringer etter avtaleinngåelsen

Innhold

1. OM AVTALEN 3
2. DEFINISJONER 3
3. AVTALENS FORMÅL 4
4. OMFANG 4
5. BEHANDLINGENS FORMÅL, OPPLYSNINGER OG BEHANDLINGER 4
6. RAMMENE FOR BEHANDLING AV HELSE- OG PERSONOPPLYSNINGER 4
7. DATAANSVARLIGES PLIKTER 4
8. DATABEHANDLERS PLIKTER 5
9. BRUK AV UNDERLEVERANDØR 7
10. OVERFØRING AV PERSONOPPLYSNINGER TIL UTLANDET 8
11. TAUSHETSPLIKT 9
12. REVISJON 9
13. VARIGHET OG OPPHØR 10
14. ENDRING AV AVTALE 10
15. LOVVALG, TVISTER OG VERNETING 10

Veileder

Støtte til bruk av standardavtalen

- Informasjon om avtalens oppbygging, forholdet mellom avtaletekst og vedlegg
- Informasjon om avtalens materielle innhold (der nødvendig)
- Veiledning til utfylling av vedleggene

Innspillrunde

Distribusjon:

- Åpent ut på ehelse.no
- Sendt PVO-forum (HODs underliggende etater)
- Sendt kontaktpersoner i HFene
- Sendt NUFA-representantene og PVO i deres virksomheter

Tilbakemeldinger:

- Generelt:
  - De fleste ga klart uttrykk for at det er positivt med en standardavtale for sektoren, både for å forenkle avtaleprosessen for aktørene og for å sikre at personvern og informasjonssikkerhet ivaretas.
  - Det var noe uenighet om avtalens omfang. Enkelte påpekte at avtalen er for omfattende/lang, mens andre ga innspill med til dels betydelig detaljeringsgrad og forslag til ytterligere avtalepunkter.
    - Vi fjernet gjentakelser og slo sammen enkelte punkter. Avtalen ble også strammet opp mht begrepsbruk.
    - Vi så det ikke hensiktsmessig å ta inn i avtalen forslag som er direkte gjengivelse/opplisting av krav fra personvernforordningen.

Tilbakemeldinger forts:

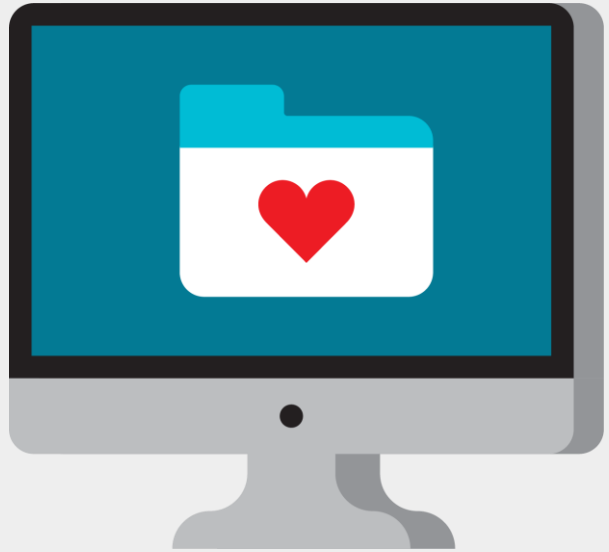
- Konkrete innspill:
  - Punkt 3 og 4 - Avtalens bakgrunn, formål og omfang
    - Flere kommenterte behovet for å presisere/forkorte/omstrukturere disse bestemmelsene noe. Disse innspillene er i all hovedsak fulgt opp.
  - Punkt 7 Dataansvarliges plikter
    - Enkelte virksomheter påpekte at avtalen er ubalansert og at også dataansvarliges plikter bør presiseres nærmere. Innspillene er delvis tatt til følge ved at ordlyden nå er lagt tettere opp til den danske standard databehandleravtalen som er fremlagt for Det europeiske personvernrådet (EDPB).
  - Punkt 8 Databehandlers plikter
    - Det ble gitt mange, til dels omfattende, kommentarer til dette punktet. Vi fulgte ikke opp forslag om vesentlig omstrukturering av punktet, men konkrete endringsforslag er i hovedsak tatt til følge. Enkelte av underpunktene er også slått sammen/forkortet/flyttet i samsvar med mottatte innspill.
  - Punkt 10: Overføring av personopplysninger til utlandet
    - Mange ønsket nærmere veiledning på dette punkter etter Schrems II. Det er som kjent foreløpig uklart hvordan dette følges opp nasjonalt/internasjonalt. Her vil veiledningen oppdateres når nærmere avklaringer kommer.
  - Punkt 12 Revisjon
    - Punktet er strukturelt endret slik at det nå i all hovedsak har lik formulering som tilsvarende bestemmelse i DigDirs databehandleravtalemal. Antatt hensiktsmessig at punktet er likelydende på tvers av sektorer. Innholdsmessig er punktet ikke ment å innebære endringer fra tidligere avtalemal. Ved behov for nærmere presisering av revisjonsrutiner, kan dette gjøres i avtalens vedlegg 3.
  - Vedleggene
    - Det er gjort enkelte mindre endringer i vedleggene i tråd med mottatte innspill.

Problemstillinger og spørsmål fra den digitale salen

Ta gjerne kontakt om du har innspill til Normens veiledningsmateriell!

- Hva trenger du?
- Hva mangler?
- Hva kan oppdatert veiledningsmateriell bidra med?

- Vil du være med i referansegruppe?
  - Internkontroll og risiko
  - Forskning
  - Tilgang



sikkerhetsnormen@ehelse.no

Bli med på våre andre webinarer!

27. april	Adressesperre i helse- og omsorgssektoren
05. mai	TBA
12. mai	Heldagskurs: Intro til Normen
19. mai	Skytjenester og tjenesteutsetting v/Norsk Helsenett

Samtidig legger vi planer for med.tek-kurs, kurs for små virksomheter, innspillswebinarer til Normens veiledningsmateriell og mye mer!

Følg med på normen.no, sosiale medier og Normens nyhetsbrev!

NORMEN