



WEBINAR:

Lansering av veileder om rettigheter ved behandling av helse- og personopplysninger

17. mars 2021

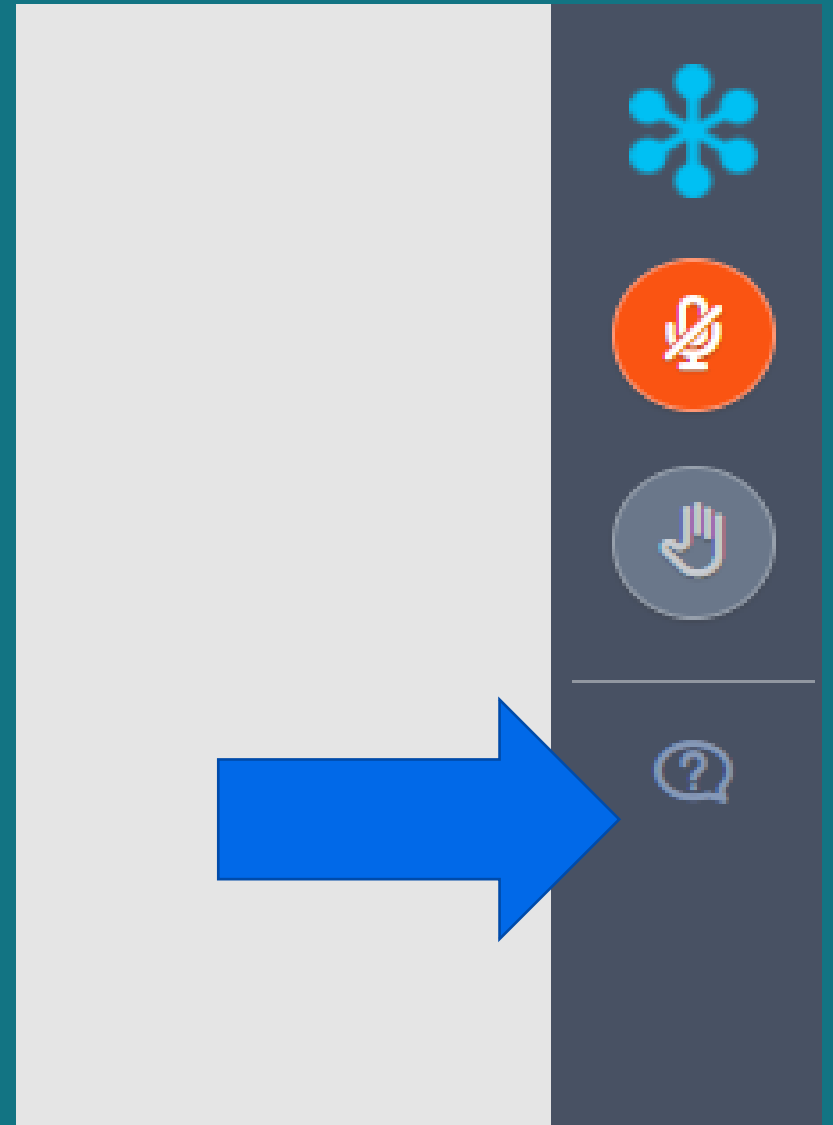
Kjøreregler

- Møteleder styrer ordet
- Deltagernes mikrofoner er mutet som standardinnstilling
- Det foretas opptak av dette webinarret
- Presentasjonene legges ut på kurs- og webinarsiden 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 webinarret, send oss en epost til sikkerhetsnormen@ehelse.no



Agenda

- Om veilederen og rettighetene
- Leseveiledning
- Særlig om retten til informasjon om behandling av personopplysninger
- Et eksempel fra virkeligheten
- Veien videre



Overordnet om veilederen

- Veilederen er omfattende, men ikke uttømmende
- Mer oppslagsverk enn lese veilederen A-Å
- Handler i all hovedsak om rettigheter tilknyttet **hvordan** virksomheten behandler helse- og personopplysningene, ikke innholdet i dem
- Versjon 1.0

Vi minner om:

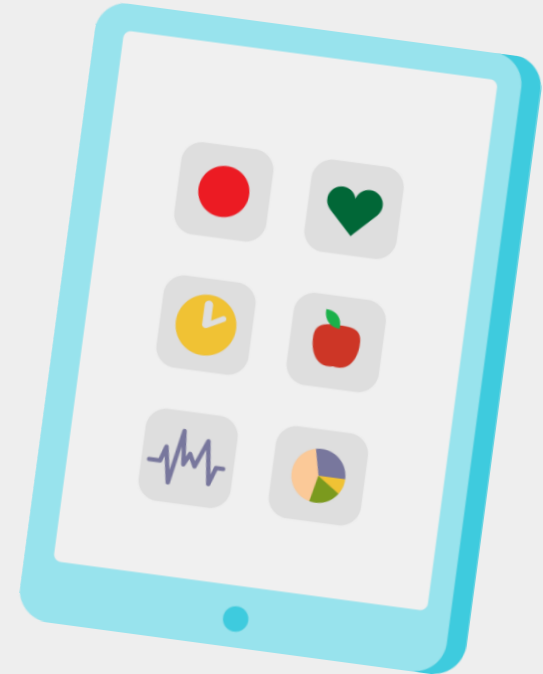
Behandling av personopplysninger

Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke.

For eksempel innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, tilgjengeliggjøring ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

Innholdet i veilederen

- Innledning samt kapittel om hvordan rettigheter ivaretas
 - Ansvar, frister og plikter
- Utgangspunkt i personvernrettighetene
 - Informasjon
 - Innsyn
 - Retting
 - Sletting
 - Begrensning
 - Dataportabilitet
 - Protestere mot behandling
 - Motsette seg behandling (pasientrettighet)
 - Automatiserte avgjørelser
 - Innebygget personvern
- Pasientrettigheter som rett til helsehjelp og lignende beskrives ikke i denne veilederen

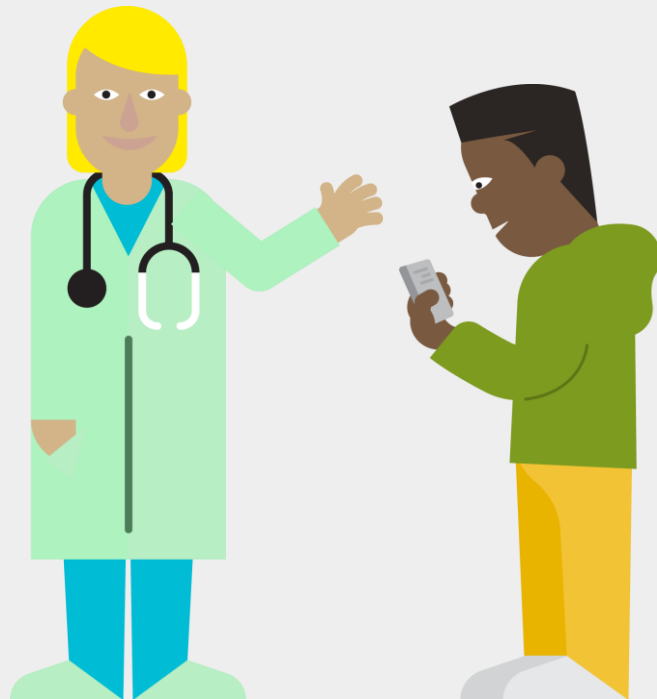


Personvernprinsippene

- Lovlig, rettferdig og åpen behandling
 - Formålsbegrensning
 - Dataminimering
 - Riktighet
 - Lagringsbegrensning
 - Integritet og konfidensialitet
 - Ansvarlighet
-
- Var lenge en del av veilederen, men vil komme i eget produkt



Slik ser veilederen ut



Innhold

| | |
|--|----|
| 1 Om veilederen | 7 |
| 1.1 Hvorfor er rettigheter viktige? | 7 |
| 1.2 Om veilederen..... | 7 |
| 1.2.1 Hvem kan ha nytte av veilederen? | 7 |
| 1.2.2 Hvordan skal jeg lese veilederen? | 8 |
| 1.3 Rettigheter i personvern- og helselovgivning | 8 |
| 1.4 Arkivlovgivningens begrensninger | 9 |
| 2 Ivaretagelse av rettigheter | 10 |
| 2.1 Ansvar for at rettigheter blir oppfylt..... | 10 |
| 2.2 Frister for å svare på og oppfylle registrertes rettigheter | 11 |
| 2.3 Plikter ved avslag på registrertes forespørsler | 11 |
| 3 Retten til informasjon om behandling av personopplysninger | 12 |
| 3.1 Innledning | 12 |
| 3.2 Retten til informasjon etter helselovgivning..... | 12 |
| 3.2.1 Helselovgivningens ulike informasjonsplikter | 12 |
| 3.2.2 Informasjonsplikt om pasientens rett til å motsette seg deling av opplysninger i behandlingsrettet helseregister | 13 |
| 3.2.3 Informasjonsplikt ved tilgjengeliggjøring av taushetsbelagte opplysninger på grunn av opplysningsplikt | 13 |
| 3.3 Retten til informasjon etter personvernlovgivingen | 14 |
| 3.3.1 Når skal informasjon gis? | 14 |
| 3.3.2 Hvordan skal informasjon gis?..... | 15 |
| 3.3.3 Hva skal det gis informasjon om?..... | 17 |
| 3.3.4 Generelle unntak fra plikten til å gi informasjon om behandling av helse- og personopplysninger | 19 |
| 3.3.5 Unntak fra plikten til å gi informasjon når personopplysningene er samlet inn fra andre enn den registrerte selv..... | 20 |
| 3.4 Informasjon ved brudd på personopplysningssikkerheten | 21 |
| 4 Retten til innsyn | 23 |
| 4.1 Innledning | 23 |
| 4.2 Retten til innsyn i behandlingsrettede helseregistre (journalinnsyn)..... | 23 |
| 4.2.1 Hvilke opplysninger skal det gis innsyn i? | 23 |
| 4.2.2 Pårørende og foreldres rett til innsyn..... | 24 |
| 4.2.3 Hvilke opplysninger kan pasienten nektes innsyn i? | 25 |



| | | |
|-------|---|-----------|
| 4.2.4 | Hvordan skal innsyn gis?..... | 26 |
| 4.3 | Retten til innsyn i forskriftsregulerte helseregistre og i forskningsprosjekter | 27 |
| 4.3.1 | Kort om retten til innsyn i forskriftsregulerte helseregistre..... | 28 |
| 4.3.2 | Kort om retten til innsyn i helserelaterte forskningsprosjekter | 28 |
| 4.4 | Retten til innsyn etter personvernlovgivningen | 28 |
| 4.4.1 | Hvilke opplysninger skal den registrerte få innsyn i? | 28 |
| 4.4.2 | Virksomhetens plikt til å gi informasjon i forbindelse med innsyn..... | 29 |
| 4.4.3 | Hvilke opplysninger kan den registrerte nektes innsyn i?..... | 29 |
| 4.4.4 | Hvordan skal innsyn gis?..... | 32 |
| 5 | Retten til retting | 33 |
| 5.1 | Innledning | 33 |
| 5.2 | Retten til retting i behandlingsrettede helseregistre | 33 |
| 5.2.1 | Hvilke opplysninger skal rettes i behandlingsrettet helseregister? | 33 |
| 5.2.2 | Hvordan skal retting skje i behandlingsrettet helseregister? | 34 |
| 5.3 | Retten til retting i forskriftsregulerte helseregistre og forskningsprosjekter | 34 |
| 5.3.1 | Kort om retten til retting i forskriftsregulerte helseregistre | 35 |
| 5.3.2 | Kort om retten til retting i helserelaterte forskningsprosjekter..... | 35 |
| 5.4 | Retten til retting etter personvernlovgivningen..... | 35 |
| 5.4.1 | Hvilke personopplysninger skal rettes? | 35 |
| 5.4.2 | Unntak fra plikten til å rette uriktige eller ufullstendige personopplysninger..... | 36 |
| 5.4.3 | Hvordan skal retting av personopplysninger skje?..... | 36 |
| 5.4.4 | Plikt til å varsle mottakere når opplysninger rettes..... | 36 |
| 6 | Retten til sletting | 37 |
| 6.1 | Innledning | 37 |
| 6.2 | Retten til sletting i behandlingsrettede helseregistre..... | 37 |
| 6.2.1 | Vilkår for sletting av helse- og personopplysninger i behandlingsrettede helseregistre..... | 38 |
| 6.2.2 | Journal ført på feil person..... | 39 |
| 6.3 | Retten til sletting i forskriftsregulerte helseregistre og forskningsprosjekter | 40 |
| 6.3.1 | Kort om retten til sletting i forskriftsregulerte helseregistre..... | 40 |
| 6.3.2 | Kort om retten til sletting i helserelaterte forskningsprosjekter | 40 |
| 6.4 | Retten til sletting etter personvernlovgivningen | 40 |
| 6.4.1 | Hvilke personopplysninger skal slettes? | 41 |
| 6.4.2 | Hvilke personopplysninger er unntatt fra sletteplikten?..... | 41 |
| 6.4.3 | Hvordan skal sletting av personopplysninger skje? | 42 |
| 6.4.4 | Plikt til å varsle mottakere når opplysninger slettes | 43 |
| 7 | Retten til å kreve begrensning av behandling av personopplysninger | 43 |

Slik ser veilederen ut

| | | |
|--------|--|-----------|
| 7.1 | Innledning | 43 |
| 7.2 | I hvilke tilfeller skal behandlingen av personopplysninger begrenses? | 44 |
| 8 | Retten til dataportabilitet..... | 45 |
| 9 | Retten til å protestere mot behandling av personopplysninger | 46 |
| 10 | Retten til å motsette seg behandling av helseopplysninger i behandlingsrettet helseregister ("Sperring av journal") | 47 |
| 10.1 | Innledning | 47 |
| 10.2 | Hva slags behandling kan pasienten motsette seg? | 48 |
| 10.2.1 | Tilgjengeliggjøring av helseopplysninger | 48 |
| 10.2.2 | Automatisk registrering av egenandeler | 49 |
| 10.2.3 | Behandling av helseopplysninger i Nasjonal kjernedokument | 49 |
| 11 | Rettigheter ved automatiserte avgjørelser | 49 |
| 11.1 | Innledning | 49 |
| 11.2 | Forbud mot automatiserte avgjørelser..... | 50 |
| 11.3 | Unntak fra forbudet om automatiserte avgjørelser | 50 |
| 11.3.1 | Generelle unntak | 50 |
| 11.3.2 | Tilleggskrav ved behandling av særlige kategorier av personopplysninger..... | 51 |
| 12 | Innebygget personvern | 51 |

Hvordan skal jeg lese veilederen?

Jeg er fastlege og lurer på hvordan jeg skal gi god informasjon til mine pasienter.

- Les veilederens kapittel 3 om informasjon, spesielt innledningen i kapitlet for å få oversikt. Kapittel 3.3.2 sier hvordan informasjon skal gis.

Jeg jobber på legevakten og har fått en forespørsel om innsyn i journal. + sletting

- Les veilederens kapittel 4.2 og kapittel 6

Jeg er pasient og vil gjerne vite hvordan jeg kan få innsyn i min journal

- Les veilederens kap 4, særlig kap 4.2.

Jeg er leverandør og har fått et krav om å ivareta innebygget personvern og særlig rettigheten om dataportabilitet.

- Les veilederens kap 8 og 12.

Jeg er personvernombud og trenger en grundig innføring i hva de registrertes rettigheter er i helse- og omsorgssektoren.

- Les hele veilederen.

Jeg er leder og trenger en kort innføring i hva de registrertes rettigheter er.

- Les veilederens kapittel 1.1, 1.3 og innledningene til resten av kapitlene. Så kan du lese grundig om hver rettighet når du trenger veiledning på den konkrete rettigheten.

Hvor finner fastlegen svar?

3 Retten til informasjon om behandling av personopplysninger

3.1 Innledning

For å sikre åpenhet, rettferdighet og tillit rundt behandlingen av personopplysninger, skal virksomheten gi den registrerte informasjon om hvordan den behandler personopplysninger. Denne plikten er en viktig forutsetning for flere av de andre rettighetene den registrerte har, både personvernrettighetene og pasient- og brukerrettighetene. Det vil være vanskelig for den registrerte å be om innsyn, retting eller sletting, hvis ikke hun vet at personopplysningene hennes blir behandlet.

Regler om informasjonsplikt ved behandling av personopplysninger finnes i både helselovgivningen og personvernlovgivningen. Plikten til å gi informasjon om behandling av helse- og personopplysninger skiller seg fra helselovgivningens plikt til å gi informasjon om pasientens helsetilstand og innholdet i helsehjelpen. Denne veilederen tar bare for seg virksomhetens plikt til å gi informasjon om behandling av helse- og personopplysninger.

Helselovgivningen har i liten grad egne regler om virksomhetens plikt til å gi informasjon om behandlingen av helse- og personopplysninger, men henviser i stedet til reglene i personvernlovgivningen.¹⁵ Dette kapittelet gir først en kort beskrivelse av helselovgivningens regler om informasjon. Deretter gis det en beskrivelse av reglene om informasjon i personvernlovgivningen. Til slutt gis det også en beskrivelse av personvernlovgivningens regler om informasjon ved brudd på personopplysningssikkerheten som også gjelder ved behandling av helseopplysninger.

3.3.2 Hvordan skal informasjon gis?

Virksomheten må gi informasjon om behandling av personopplysninger, men virksomheten har ingen plikt til å sikre at den registrerte har tilegnet seg informasjonen.

Hensikten med informasjonsplikten er å sette den registrerte i stand til å forstå behandlingen av personopplysninger om seg selv. Hvordan informasjonen skal gis og på hvilket nivå vil derfor kunne variere.

Virksomheten må selv vurdere hvordan informasjonen skal gis til den registrerte. Personvernforordningen sier lite om hvilke metoder virksomheten bør eller kan benytte, men den gir noen føringer som virksomheten må følge.

Informasjonen bør være skriftlig

Informasjonen bør i utgangspunktet gis skriftlig, men den kan også gis på andre måter.³² Virksomheten kan for eksempel bruke hjemmesider, videoer, skjemaer og illustrasjoner, men informasjonen bør også være tilgjengelig skriftlig.³³

Hvis den registrerte spør om det, kan informasjonen også gis muntlig.³⁴ Det vil si at hvis helsepersonell får spørsmål om behandlingen av personopplysninger, så kan spørsmålet besvares muntlig der og da. Helsepersonellet bør dokumentere at informasjon ble gitt, og hva som ble sagt.³⁵

Hvor finner fastlegen svar?

3.3.3 Hva skal det gis informasjon om?

Personvernlovgivingens regler om informasjonsplikt skiller mellom tilfeller der personopplysningene er samlet inn fra den registrerte selv, og der personopplysningene er samlet inn fra noen andre. I begge tilfellene har den registrerte rett på mye av den samme informasjonen, men det er også noen ulikheter. I dette delkapittelet behandles de to tilfellene sammen. Der det er forskjeller, slik at et krav bare gjelder det ene tilfellet, er dette presisert.

Ved behandling av personopplysninger i behandlingsrettede helseregistre, er virksomheten kun pålagt å gi informasjon hvis opplysningene er samlet inn fra den registrerte selv.⁴⁷ Dette er nærmere beskrevet senere i kapittelet.

Informasjon om virksomheten

Den registrerte skal få informasjon om virksomheten som er ansvarlig for behandlingen av personopplysningene. Det skal gis informasjon om virksomhetens identitet og kontaktinformasjon. Virksomheten må også oppgi personvernombudets kontaktinformasjon, hvis virksomheten har et personvernombud.⁴⁸

Informasjon om behandlingen av personopplysninger

Den registrerte skal få informasjon om selve behandlingen av personopplysninger, herunder hvilke formål personopplysningene behandles for, og hvilket rettslig behandlingsgrunnlag

⁴⁷ Pasientjournalloven § 18 jf. Prp.56 LS (2017-2018) s. 188

⁴⁸ Personvernforordningen artikkel 13 (1)(b) og artikkel 14 (1)(b)

3.3.4 Generelle unntak fra plikten til å gi informasjon om behandling av helse- og personopplysninger

Det finnes flere unntak fra plikten til å gi informasjon om behandling av personopplysninger. Den registrertes rett til informasjon er nært tilknyttet den registrertes rett til innsyn i egne personopplysninger, og det finnes flere unntak som gjelder begge rettighetene. Det kan være

3.3.5 Unntak fra plikten til å gi informasjon når personopplysningene er samlet inn fra andre enn den registrerte selv

Noen unntak gjelder bare når personopplysningene er samlet inn fra noen andre enn den registrerte selv. Disse unntakene er snevre, og det skal mye til for at virksomheten kan bruke dem. De mest aktuelle unntakene for helse- og omsorgssektoren er:

Behandlingen av personopplysninger pålagt i lov eller forskrift

Informasjonsplikten gjelder ikke alltid når personopplysninger behandles for å ivareta en rettslig plikt. Det gjøres unntak fra informasjonsplikten når behandlingen har en tydelig hjemmel i lov eller forskrift, og loven eller forskriften inneholder regler som ivaretar den registrertes interesser.

Hvor finner fastlegen svar?

3.4 Informasjon ved brudd på personopplysningssikkerheten

Ved hendelser som innebærer brudd på personopplysningssikkerheten⁷¹, er det egne regler om oppfølgingen.⁷² Disse reglene inneholder blant annet regler om at det skal gis informasjon til berørte registrerte når det er høy risiko for deres rettigheter og friheter.

Virksomheten skal som hovedregel gi berørte registrerte følgende informasjon:

- Kontaktopplysningene til virksomhetens personvernombud eller annen kontaktperson
- De sannsynlige konsekvensene av bruddet på personopplysningssikkerheten
- En beskrivelse av tiltakene som virksomheten har iverksatt eller planlegger å iverksette for å redusere konsekvensene av bruddet

Et brudd på personopplysningssikkerheten kan føles sterkt belastende for den registrerte. Det kan derfor være nødvendig å gi den registrerte mer informasjon enn det virksomheten er pliktig til å utlevere for å ivareta den registrertes interesser. Virksomheten kan likevel ikke gi informasjon som vil medføre brudd på helsepersonellens taushetsplikt⁷³ eller som kan gå på bekostning av andre registrertes personvern.

Informasjonen skal gis på en hensiktsmessig måte. Dette kan f.eks. skje per telefon eller per brev.

Selv om virksomheten ikke er pålagt å varsle de berørte kan det være gode grunner til å informere om avviket. Dette sikrer åpenhet, og kan bidra til at saken blir bedre håndtert f.eks. ved at feilsende opplysninger slettes og den berørte kan treffe egne sikkerhetstiltak.

Eksempel

Pasient NN er 16 år og er innlagt på Nørmland sykehus. I forbindelse med en oppdatering av sykdomsbildet, skal sykehuset sende informasjon til de pårørende. Pasienten har samtykket til at denne informasjonen gis. Ved en feil sendes denne informasjonen til en rekke andre pårørende i tillegg til rett mottaker. Pårørende til NN får vite dette via andre som har mottatt informasjonen, da lokalsamfunnet er lite, og alle kjenner alle.

Pårørende til NN blir svært opprørte, og kontakter sykehuset for å få informasjon om det som har skjedd. Sykehuset har ikke oppdaget feilen, men tar affære og melder avviket til Datatilsynet. De vurderer avviket til å ikke være så alvorlig at det er nødvendig å varsle de registrerte.

De pårørende kontakter sykehusets personvernombud for å få bistand. De mener at de har rett på mer informasjon om det som har skjedd, og synes det er svært ubehagelig at andre i lokalsamfunnet har fått sensitiv informasjon om sønnen deres. De vil derfor, i tillegg til informasjon om avviket, ha kontaktinformasjon til de andre mottakerne.

Personvernombudet kontakter egen virksomhet og argumenterer for at de pårørende bør få varsel etter artikkel 34, da de allerede er kjent med at avviket har skjedd og hva slags informasjon som er på avveie. Videre er det et viktig å demonstrere at man tar hendelsen på alvor og at man gjør det man kan for å ivareta pasienten og de pårørende. I en ubehagelig situasjon som denne er det avgjørende at pårørende og NN føler at de blir sett og at deres ubehag ikke bagatelliseres. Personvernombudet anbefaler at virksomheten tar hensyn til dette i sin kontakt med NN og de pårørende. Ombudet mener likevel at man ikke kan gi ut informasjon om andre mottakere, da disse har en selvstendig rett til å få sitt personvern ivaretatt.

Hendelsen resulterer i at sykehuset gjør endringer i sine informasjonsrutiner, og heretter sender informasjon via andre kanaler der risikoen for feilsending vurderes å være mye lavere. Sykehuset følger opp NN og hans pårørende ved å kontakte de direkte og informere om rutineendringen, for å gjøre de trygge på at dette ikke vil skje igjen.

Hvordan skal jeg lese veilederen?

Jeg er fastlege og lurer på hvordan jeg skal gi god informasjon til mine pasienter.

- Les veilederens kapittel 3 om informasjon, spesielt innledningen i kapitlet for å få oversikt. Kapittel 3.3.2 sier hvordan informasjon skal gis.

Jeg jobber på legevakten og har fått en forespørsel om innsyn i journal. + sletting

- Les veilederens kapittel 4.2 og kapittel 6

Jeg er pasient og vil gjerne vite hvordan jeg kan få innsyn i min journal

- Les veilederens kap 4, særlig kap 4.2.

Jeg er leverandør og har fått et krav om å ivareta innebygget personvern og særlig rettigheten om dataportabilitet.

- Les veilederens kap 8 og 12.

Jeg er personvernombud og trenger en grundig innføring i hva de registrertes rettigheter er i helse- og omsorgssektoren.

- Les hele veilederen.

Jeg er leder og trenger en kort innføring i hva de registrertes rettigheter er.

- Les veilederens kapittel 1.1, 1.3 og innledningene til resten av kapitlene. Så kan du lese grundig om hver rettighet når du trenger veiledning på den konkrete rettigheten.

Hvor finner legevakten svar?

4.2 Retten til innsyn i behandlingsrettede helseregistre (journalinnsyn)

Pasienten har rett til innsyn i helse- og personopplysninger som nedtegnes i behandlingsrettede helseregistre i forbindelse med helsehjelp.⁷⁵ Dette delkapittelet gir en beskrivelse av hva virksomheter og helsepersonell må tenke på når en pasient ber om innsyn i slike opplysninger.

Personvernlovgivingens regler om innsyn gjelder for behandlingsrettede helseregistre.

Personvernlovgivingens regler inneholder noen tilleggskrav og unntak som gjelder i tillegg til reglene i helselovgivingen. Disse er nevnt underveis i delkapittelet, og nærmere beskrevet i veilederens kapittel Retten til innsyn etter personvernlovgivingen.

4.2.1 Hvilke opplysninger skal det gis innsyn i?

6 Retten til sletting

6.1 Innledning

Sletting av helse- og personopplysninger er et endelig tiltak som ikke kan omgjøres. Den registrertes ønske om sletting må derfor veies opp mot behovet for å bevare dokumentasjonen. Bevaring kan være nødvendig for kvalitetssikring og forbedring av helsetjenester, for å dokumentere et krav i en tvist eller for senere forskning.

Virksomheter kan i noen tilfeller ha en plikt til å slette helse- og personopplysninger både etter eget initiativ, eller etter forespørsel fra den registrerte. Denne veilederen dekker kun situasjoner der den registrerte har bedt om sletting.

Virksomhetens plikt til å slette opplysninger, og unntakene fra plikten, er grundig regulert i både helselovgivingen og personvernlovgivingen. Sletteplikten i personvernlovgivingen gjelder ved behandling av helse- og personopplysninger til statistikk, helseanalyser, forskning, kvalitetsforbedring, planlegging, styring og beredskap i helse- og omsorgsforvaltningen og helse- og omsorgstjeneste.¹³¹ Personvernlovgivingens regler om sletting gjelder også for annen behandling av personopplysninger, som for eksempel behandling av ansattes personopplysninger.

Sletteplikten gjelder ikke for helse- og personopplysninger som er nedtegnet i behandlingsrettede helseregistre i forbindelse med helsehjelp.¹³² For sletting av personopplysninger i behandlingsrettede helseregistre, er det gitt egne regler i helselovgivingen.

Hvis opplysninger ikke kan slettes, vil virksomheten kunne rette opplysninger ved å supplere dem etter reglene om retting. Reglene om retting og sletting må derfor ses i sammenheng.

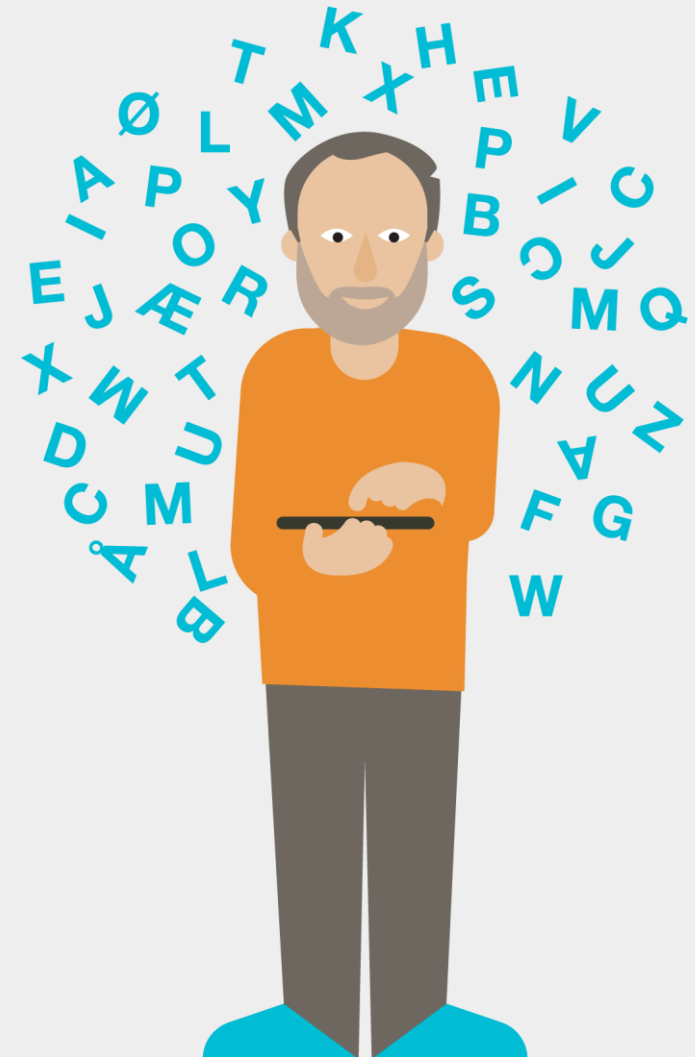
Dette kapittelet gir først en beskrivelse av reglene om sletting i behandlingsrettede helseregistre. Deretter gis det en kort beskrivelse av reglene om sletting i forskriftsregulerte helseregistre og forskningsprosjekter. Til slutt beskrives reglene om sletting i personvernlovgivingen.

6.2 Retten til sletting i behandlingsrettede helseregistre

Pasienten har i noen tilfeller rett til å få slettet helse- og personopplysninger i behandlingsrettede helseregistre.¹³³ Denne rettigheten er imidlertid svært snever.

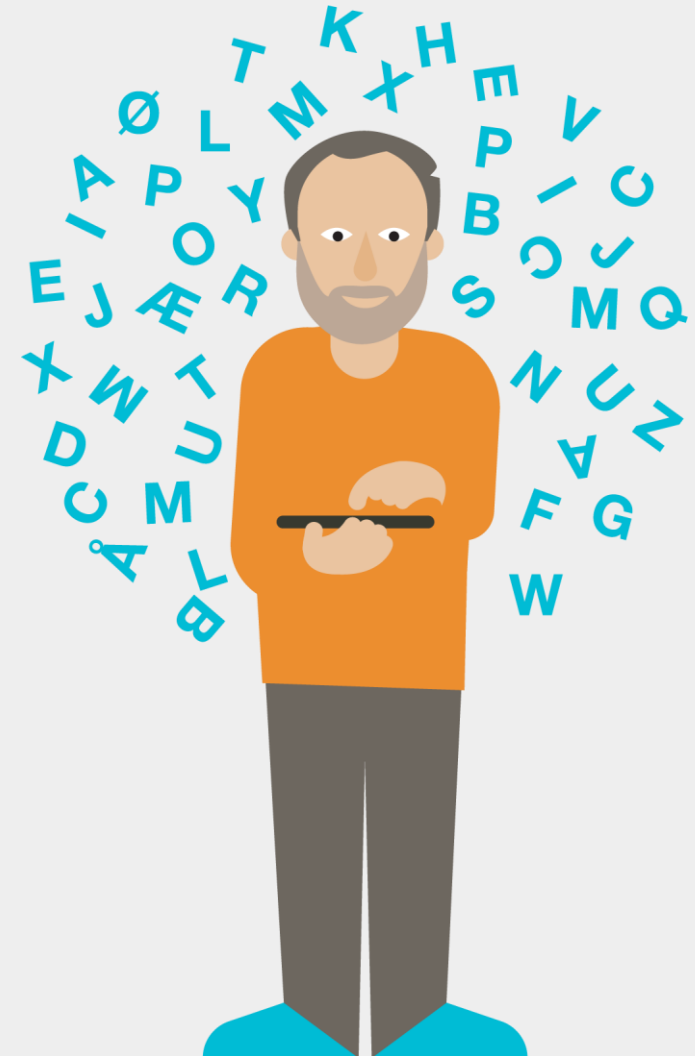
Vi går litt nærmere inn i én av rettighetene:

- Informasjon
- Innsyn
- Retting
- Sletting
- Begrensning
- Dataportabilitet
- Protestere mot behandling
- Motsette seg behandling (pasientrettighet)
- Automatiserte avgjørelser
- Innebygget personvern

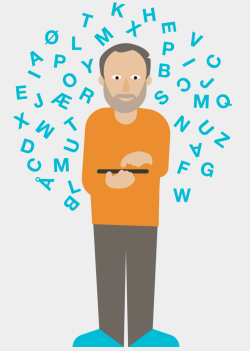


Vi går litt nærmere inn i én av rettighetene:

- **Informasjon**
- Innsyn
- Retting
- Sletting
- Begrensning
- Dataportabilitet
- Protestere mot behandling
- Motsette seg behandling (pasientrettighet)
- Automatiserte avgjørelser
- Innebygget personvern



Retten til informasjon om behandling av personopplysninger



- Handler ikke om retten til å få informasjon om helsehjelpen din, men informasjon om behandling av personopplysningene dine
- For å sikre åpenhet, rettferdighet og tillit rundt behandlingen
- Viktig forutsetning for flere av de andre rettighetene
 - Vanskelig å be om innsyn, retting eller sletting om du ikke vet at personopplysningene behandles
- Krevende kapittel – omfattende rettighet og flere rettigheter i helselovgivningen
- Rettigheter om informasjon i helselovgivningen nevnes først i kapittelet
- Informasjon ved brudd på personopplysningssikkerheten
 - Ikke på samme sted i forordningen, men er tatt med her fordi det også gir en rett til informasjon

Et eksempel fra virkeligheten – informasjon til de registrerte ved brudd på informasjonssikkerheten



Pasient NN er 16 år og er innlagt på Normland sykehus. I forbindelse med en oppdatering av sykdomsbildet, skal sykehuset sende informasjon til de pårørende. Pasienten har samtykket til at denne informasjonen gis. Ved en feil sendes denne informasjonen til en rekke andre pårørende i tillegg til rett mottaker. Pårørende til NN får vite dette via andre som har mottatt informasjonen, da lokalsamfunnet er lite, og alle kjenner alle.

Et eksempel fra virkeligheten – informasjon til de registrerte ved brudd på informasjonssikkerheten



Pårørende til NN kontakter sykehuset for å få informasjon om det som har skjedd.

Sykehuset har ikke oppdaget feilen, men melder avviket til Datatilsynet.

Sykehuset vurderer avviket til å ikke være så alvorlig at det er nødvendig å varsle de registrerte.

De pårørende kontakter sykehusets personvernombud for å få bistand. De mener at de har rett på mer informasjon. Vil i tillegg til informasjon om avviket, ha kontaktinformasjon til de andre mottakerne.

Et eksempel fra virkeligheten – informasjon til de registrerte ved brudd på informasjonssikkerheten



Personvernombudet mener de pårørende bør få varsel etter artikkel 34, da de allerede er kjent med at avviket har skjedd og hva slags informasjon som er på avveie.

Videre er det et viktig å demonstrere at man tar hendelsen på alvor og at man gjør det man kan for å ivareta pasienten og de pårørende.

Personvernombudet anbefaler at virksomheten tar hensyn til dette i sin kontakt med NN og de pårørende.

Et eksempel fra virkeligheten – informasjon til de registrerte ved brudd på informasjonssikkerheten



Ombudet mener likevel at man ikke kan gi ut informasjon om andre mottakere, da disse har en selvstendig rett til å få sitt personvern ivaretatt.

Hendelsen resulterer i at sykehuset gjør endringer i sine informasjonsrutiner, og heretter sender informasjon via andre kanaler der risikoen for feilsending vurderes å være mye lavere. Sykehuset følger opp NN og hans pårørende ved å kontakte de direkte og informere om rutineendringen, for å gjøre de trygge på at dette ikke vil skje igjen.

Hva kan man lære av denne hendelsen?

Hvor går veien videre?

Basert på denne veilederen:

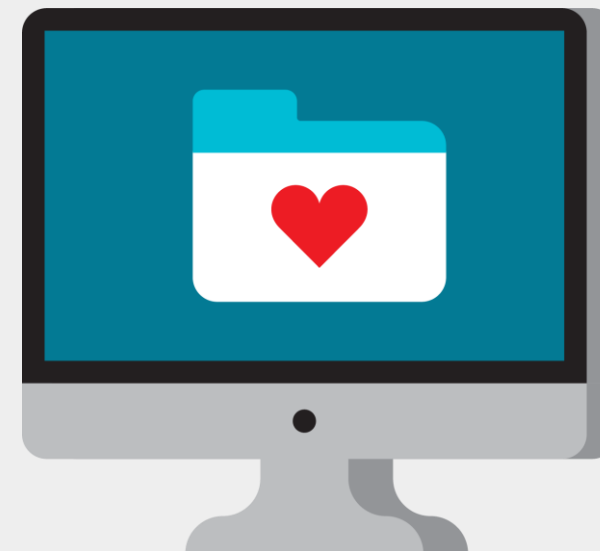
- Innspill til forbedringer av veilederen til neste versjon?
- Temaer for fremtidige webinarer?
 - Mer om spesifikke rettigheter?
 - Praktiske caser?
 - Helt andre ting?



Ta gjerne kontakt om du har innspill til Normens veiledningsmaterieill!

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

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



sikkerhetsnormen@ehelse.no

Bli med på våre andre webinarer og kurs!

| | |
|-----------|---|
| 24. mars | IKT-tilsyn med Helsetilsynet |
| 31. mars | PÅSKEFERIE |
| 7. april | Medisinsk utstyr og informasjonssikkerhet |
| 14. april | TBD |

Vi legger blant annet planer for med.tek-kurs, webinar om databehandleravtale, kurs for små virksomheter, webinar om adressesperre (kode 6 og 7) og nye heldagskurs med intro til Normen.

Oppdatert plan legges ut snart –

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