Helseopplysninger på tvers - rammer for deling og tilgang

HelsIT

Datatilsynet

15. oktober 2014

Marius Engh Pellerud

Hva er personvern?

Retten til privatliv

Selvbestemmelse

Rett til å vite og forstå

En menneskerettighet

Sentrale personvernprinsipper

Formålsbestemthet
Behandling av personopplysninger skal være saklig begrunnet. Opplysningene skal samles inn til uttrykkelig angitte og legitime formål og brukes i overensstemmelse med disse.

Overskuddsinformasjon og opplysninger som ikke lenger er nødvendige for formålet med registreringen, skal slettes.

Proporsjonalitet
Registrering og bruk av personopplysninger skal ikke innebære en urimelig belastning for den enkeltes selvråderett eller integritet. Man skal alltid velge det minst inngripende alternativet.

Frivillig samtykke
Registrering av personopplysninger skal i størst mulig grad være basert på et frivillig, uttrykkelig og informert samtykke.

Opplysningsplikt
Ved innhenting av personopplysninger har den enkelte uoppfordret rett til å vite om det er frivillig eller obligatorisk å oppgi personopplysningene, hvilket formål de skal brukes til, og om de vil bli utlevert til andre.

Rett til innsyn, retting og sletting
Den behandlingsansvarlige skal bistå den registrerte med å gi innsyn i hvilke opplysninger som er lagret, hva de skal brukes til, og hvor de er hentet fra. Feil opplysninger skal rettes eller slettes.

Informasjonssikkerhet
Personopplysninger skal ikke komme på avveie. Det må etableres en tilfredsstillende informasjonssikkerhet. Det må kunne dokumenteres at rutiner og tiltak som sikrer personopplysninger, blir etterlevd i praksis.

Personvern i helsesektoren

Helseregisterloven § 13

"Bare den databehandlingsansvarlige, databehandlere og den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet, kan gis tilgang til helseopplysninger."

Unntak fra § 13

Virksomhetsovergripende pasientjournal i formalisert arbeidsfellesskap

Virsomhetsovergripende, behandlingsrettede helseregistre

Tilgang på tvers (helseinformasjonssikkerhetsforskriften)

Databehandlere…

Meldingsutveksling…

Helsesektorens behov

- Økt krav til samhandling
- Sammenhengende behandlingsforløp
- Økte krav til spesialiserte helsetjenester i kommunene
- Pasientenes forventninger

Datatilsynet

Nye helseregisterlover

Ny helseregisterlov og pasientjournallov

- Helseregisterloven skal deles i to
- Pasientjournallov
  - Primære formål: Bruk av helseopplysninger til å yte helsehjelp
- Helseregisterlov
  - Sekundære formål: forskning og kvalitetssikring med mer

Ny pasientjournallov

- Forbudet mot å gi andre virksomheter tilgang til opplysninger (gammel helseregisterlov § 13) videreføres ikke…
- Men hvordan opplysninger skal deles skal fortsatt reguleres av forskrift
- Fellesløsninger
  - Nasjonal kjernejournal
  - Reseptformidler
  - En innbygger en journal

Gammel helseregisterlov § 13

"Bare den databehandlingsansvarlige, databehandlere og den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet, kan gis tilgang til helseopplysninger."

Ny pasientjournallov § 19

«Innenfor rammen av taushetsplikten skal den databehandlingsansvarlige sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte.»

Datatilsynet

Taushetspliktsbestemmelsene begrenser hvilke tilganger som kan gis

§ 19

Hvordan avgjøre hvilke opplysninger som er relevante og nødvendige?

«Innenfor rammen av taushetsplikten skal den databehandlingsansvarlige sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte.

Det er altså ikke et krav at tilgangen er nødvendig for å gi helsehjelp.

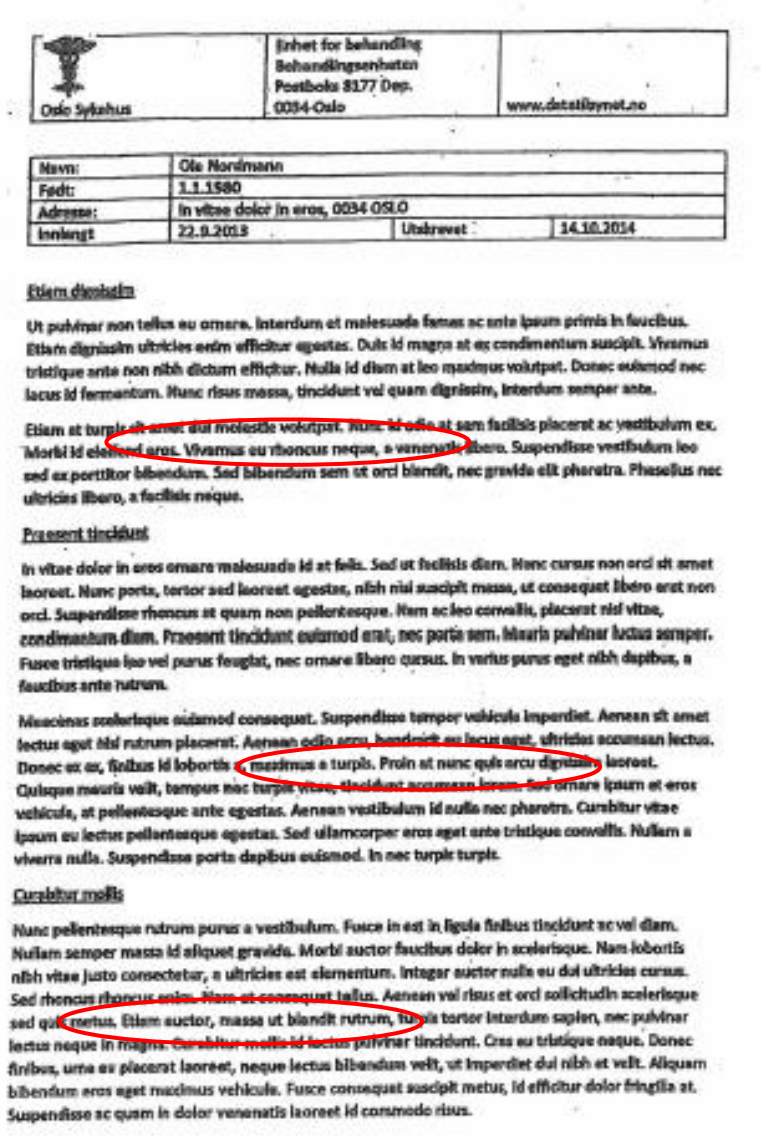
Hvordan styre tilgangen ut fra relevans og nødvendighet?

Forslag til forskrift om tilgang til helseopplysninger mellom virksomheter

1. De informasjonsutvekslende virksomhetene må inngå avtale
   1. Hva slags journalinformasjon skal utveksles
   2. Hvilke risikoelementer ligger til grunn for avtalen
   3. Rutiner og fordeling av oppgaver mellom virksomhetene for ivaretakelse av kravene i lov og forskrift
2. De informasjonsutvekslende virksomhetene må begge ha god informasjonssikkerhet og tilgangsstyring
3. Alle andre krav i pasientjournalloven og personopplysningsloven gjelder

Forutsetninger for å oppnå dette

Fra:



Enhet for behandling
Behandlingsenheten
Postboks 8177 Dep.
0034-Oslo

Oslo Sykehus

www.datatilsynet.no

Navn:	Ola Nordmann		
Født:	1.1.1580		
Adresse:	In vitae dolor in eros, 0034 OSLO		
Innlagt	22.9.2013	Utskrevet	14.10.2014

Etiam dignissim

Ut pulvinar non tellus eu ornare. Interdum et malesuada fames ac ante ipsum primis in faucibus. Etiam dignissim ultricies enim efficitur egestas. Duis id magna at ex condimentum suscipit. Vivamus tristique ante non nibh dictum efficitur. Nulla id diam at leo maximus volutpat. Donec euismod nec lacus id fermentum. Nunc risus massa, tincidunt vel quam dignissim, interdum semper ante.

Etiam at turpis sit amet dui molestie volutpat. Nunc id odio at sem facilisis placerat ac vestibulum ex. Morbi id eleifend eros. Vivamus eu rhoncus neque, a venenatis libero. Suspendisse vestibulum leo sed ex porttitor bibendum. Sed bibendum sem ut orci blandit, nec gravida elit pharetra. Phasellus nec ultricies libero, a facilisis neque.

Praesent tincidunt

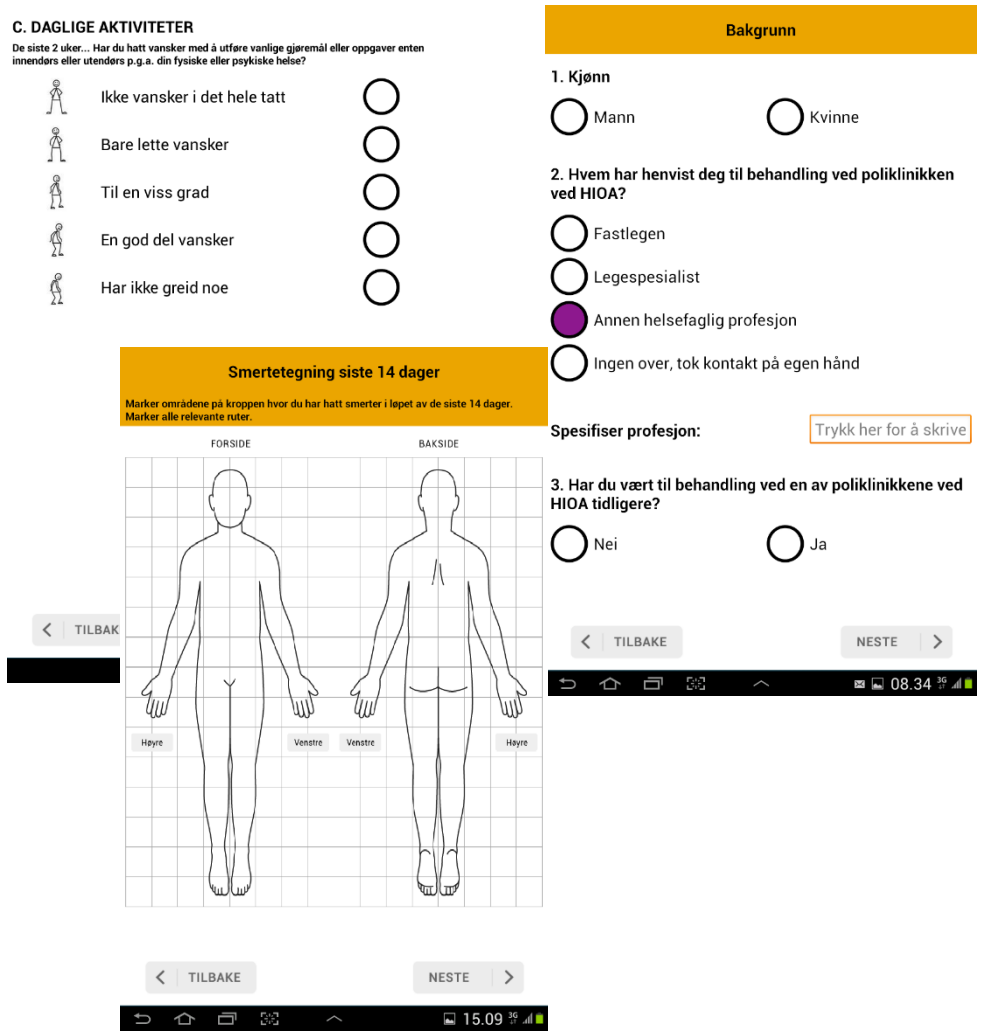
In vitae dolor in eros ornare malesuada id at felis. Sed ut facilisis diam. Nunc cursus non orci sit amet laoreet. Nunc porta, tortor sed laoreet egestas, nibh nisi suscipit massa, ut consequat libero erat non orci. Suspendisse rhoncus at quam non pellentesque. Nam ac leo convallis, placerat nisl vitae, condimentum diam. Praesent tincidunt euismod erat, nec porta sem. Mauris pulvinar luctus semper. Fusce tristique leo vel purus feugiat, nec ornare libero cursus. In varius purus eget nibh dapibus, a faucibus ante rutrum.

Maecenas scelerisque euismod consequat. Suspendisse tempor vehicula imperdiet. Aenean sit amet lectus eget nisl rutrum placerat. Aenean odio arcu, hendrerit eu lacus eget, ultricies accumsan lectus. Donec ex ex, finibus id lobortis a, maximus a turpis. Proin at nunc quis arcu dignissim laoreet. Quisque mauris velit, tempus nec turpis vitae, tincidunt accumsan ipsum. Sed ornare ipsum et eros vehicula, at pellentesque ante egestas. Aenean vestibulum id nulla nec pharetra. Curabitur vitae ipsum eu lectus pellentesque egestas. Sed ullamcorper eros eget ante tristique convallis. Nullam a viverra nulla. Suspendisse porta dapibus euismod. In nec turpis turpis.

Curabitur mollis

Nunc pellentesque rutrum purus a vestibulum. Fusce in est in ligula finibus tincidunt ac vel diam. Nullam semper massa id aliquet gravida. Morbi auctor faucibus dolor in scelerisque. Nam lobortis nibh vitae justo consectetur, a ultricies est elementum. Integer auctor nulla eu dui ultricies cursus. Sed rhoncus rhoncus enim. Nam et consequat tellus. Aenean vel risus et orci sollicitudin scelerisque sed quis metus. Etiam auctor, massa ut blandit rutrum, turpis tortor interdum sapien, nec pulvinar lectus neque in magna. Curabitur mollis id lectus pulvinar tincidunt. Cras eu tristique neque. Donec finibus, urna ac placerat laoreet, neque lectus bibendum velit, ut imperdiet dui nibh et velit. Aliquam bibendum eros eget maximus vehicula. Fusce consequat suscipit metus, id efficitur dolor fringilla at. Suspendisse ac quam in dolor venenatis laoreet id commodo risus.

Til…?



C. DAGLIGE AKTIVITETER

De siste 2 uker... Har du hatt vansker med å utføre vanlige gjøremål eller oppgaver enten innendørs eller utendørs p.g.a. din fysiske eller psykiske helse?

- Ikke vansker i det hele tatt
- Bare lette vansker
- Til en viss grad
- En god del vansker
- Har ikke greid noe

Smertetegning siste 14 dager

Marker områdene på kroppen hvor du har hatt smerter i løpet av de siste 14 dager. Marker alle relevante ruter.

FORSIDE BAKSIDE

Høyre Venstre Venstre Høyre

TILBAKE NESTE

15.09

Bakgrunn

1. Kjønn

Mann Kvinne

2. Hvem har henvist deg til behandling ved poliklinikken ved HIOA?

Fastlegen
Legespesialist
Annen helsefaglig profesjon
Ingen over, tok kontakt på egen hånd

Spesifiser profesjon: Trykk her for å skrive

3. Har du vært til behandling ved en av poliklinikkene ved HIOA tidligere?

Nei Ja

TILBAKE NESTE

08.34

Kilde: Infopad

Tilgangsstyring

- Hvem skal ha tilgang til personopplysninger?
- Hvilken informasjon har man tilgang til?
- I hvilket tidsrom?
- I hvilke situasjoner?
- Hvordan sikre at tilgangen er autorisert og i henhold til regelverket (kontroll)?

Disse faktorene må balanseres. Hva kan vi leve med og hvor bør grensene gå?

Logging

- Autorisert bruk av informasjonssystemet skal registreres
- Forsøk på uautorisert bruk av informasjonssystemet skal registreres
- Ved tilgang på tvers av virksomhetsgrenser skal registreres:
  - Person og organisatorisk tilhørighet
  - Hvor opplysningene er hentet fra
  - Tidspunkt
- Bruk av logg
  - Ved henvendelser fra den registrerte
  - Ved tips om misbruk
  - Stikkprøveanalyse
  - Automatiserte analyser

Datatilsynets kontroller av tilgangsstyring og logging

- Datatilsynet fører tilsyn med helseregisterloven § 13: *"Tilgang kan bare gis i den grad dette er **nødvendig** for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt."*
- Krav til
  - Teknisk løsning for tilgangsstyring
  - Skriftlige vurderinger av nødvendig tilgang
  - Tekniske sperrer for tilgang basert på vurderingene
  - Logging og oppfølging av logger
- Datatilsynet fører ikke tilsyn med om taushetsplikten er ivaretatt

Datatilsynets kontroller av tilgangsstyring i helse

- Helse Stavanger HF (2014)
- Volvat medisinske senter (2014)
- Sykehuset Innlandet (2014)
- Ullevål universitetssykehus (2008)
- St. Olavs Hospital (2008)
- Sykehuset i Vestfold (2007)
- Helse Bergen (2006)
- Ahus (2006)
- UNN (2005)
- Helse Finnmark (2005)
- Helse Bergen (2005)
- Sykehuset Asker og Bærum (2005)

Funn 2005 - 2008

- Sviktende tilgangsstyring
  - Mange i virksomhetene hadde tilgang til helseopplysninger selv om de ikke hadde tjenstlig behov for tilgangene
  - Brudd på § 13 («tilgang på tvers»)
  - Utstrakt bruk av aktualisering (”blålys”)
- Mangelfulle kontrollrutiner for å avdekke snoking
  - En viss vidde er nødvendig – men krever kontroll av tilgangene i ettertid
  - Noen gjør ikke loggkontroller i det hele tatt, noen bare av aktualisering
  - Automatisk logganalyse
- Manglende vurderinger
  - Mange har ikke risikovurdert sitt tilgangsregime
  - Risikovurderinger skjer gjerne kun ved innføring av EPJ

Råd om tilgangsstyring

- Tilstrekkelig styring av tilganger – en samlet vurdering
  - Tilganger
  - Tid
  - Logging
  - Sperring
- Logg som sikkerhetsmekanisme
  - Jo mer man hviler seg på logg – dess strengere krav til oppfølging av logg
- MEN – tilgang til fellesløsninger krever strengere tilgangsstyring
- Risikovurdering og dokumentasjon
  - Nødvendighet må vurderes strengt
- Logisk skille mellom nødrettstilgang (blålys) og annen egenaktualisering

Dette blir ennå viktigere når pasientjournalloven trer i kraft

Innebygd personvern

1. Vær i forkant, forebygg fremfor å reparere
2. Gjør personvern til standardinnstilling
3. Bygg personvern inn i designet
4. Skap full funksjonalitet: Både-og, ikke enten-eller
5. Ivareta informasjonssikkerheten fra start til slutt
6. Vis åpenhet
7. Respekter brukerens personvern

Pasientens rettigheter

- Informasjon til pasienten
- Pasienten har rett til å motsette seg
- Sperring av helseopplysninger

Datatilsynet

Marius Engh Pellerud

rådgiver – helse, forskning, NAV, m.m.

Tlf: 22 39 69 23

marius.engh.pellerud@datatilsynet.no

Følg oss:

www.datatilsynet.no

www.personvernbloggen.no

www.twitter.com/datatilsynet

Datatilsynet – i front for retten til selvbestemmelse, integritet og verdighet