”Sviktende tilgangsstyring i elektroniske pasientjournaler?”

Datatilsynet

Ragnhild Castberg, seniorådgiver

Norsk Arkivråds arkivseminar ,18.september 2012

Om Datatilsynet

- Et forvaltningsorgan med stor grad av faglig uavhengighet
- Målgruppen består av offentlig og privat sektor
- Informasjon – Veiledning - Tilsyn – Regulering

Ca 40 medarbeidere

- 4 Avdelinger
  - Juridisk
  - Tilsyns- og sikkerhet
  - Informasjon
  - Administrasjon

Hva er egentlig personvern?

”Den enkeltes *rett til å ha kontroll med egne personopplysninger*”

Selvbestemmelse – rett til selv å bestemme hvilke opplysninger som skal brukes, av hvem, til hvilke formål osv

Informasjon – hvis man ikke har rett til å samtykke, har man i det minste rett til å vite hvilke opplysninger som brukes, av hvem, til hvilke formål osv

Personvern er noe mer enn informasjonssikkerhet. Informasjonssikkerheten er bare en nødvendig *forutsetning* for å kunne ivareta personvernet

Fokusområder for Datatilsynet på helseområdet

- Helseregistre
- Helseforskning
- NAV
- Bioteknologi
- Tilgangsstyring
- Tilgang på tvers
- Kjernejournal
- Velferdsteknologi

- Strategi: **Bedre personvern i helsesektoren**

Godt personvern - bedre helse…..

Godt personvern sikrer befolkningens tillit til helsepersonell

Tillit mellom pasienter og helsepersonell er en nødvendig forutsetning for god medisinsk behandling

Dersom pasienten ikke har tillit til at sensitiv informasjon, som gis i fortrolighet, blir ivaretatt på en god måte svekkes også tilliten til helsetjenestene og helsepersonell

Dersom tilliten svikter kan resultatet bli at pasientene ikke vil gi nødvendig informasjon til helsepersonellet.

Sviktende tilgangsstyring?

”I en tilsynsrapport ser Datatilsynet på hvordan sikkerheten er ivaretatt i elektroniske pasientjournaler og konkluderer med at man ennå er langt unna en løsning på problemene med tilgangsstyring”

Norge er ikke alene om dette problemet……..

William Behringer testet HIV-positiv på et ”medical center” i New Jersey, der han selv jobbet som kirurg.

Kort tid etter at testresultatene var ferdig ringte kollegaer og andre ved virksomheten for å uttrykke sin empati og medlidenhet.

Få dager senere mistet han jobben.

Principles of Biomedical Ethics

James F. Childress –Tom Beauchamp

Tilgangsstyring
Hva er viktig?

- At journalen behandles med respekt
  ⇒TAUSHETSPLIKTEN

- At journalen er tilgjengelig ved behov
  ⇒Tilgjengelighet
- At journalen ikke er tilgjengelig utover behov
  ⇒konfidensialitet
- At journalen er til å stole på
  ⇒Kvalitet & Integritet

Hovedmomenter fra et ”tilsyn” med et helseforetak

Tilsynsfokus: Sikring av konfidensialitet gjennom tilgangsstyring og logging

Gjennomgang av EPJ, PAS, IS og PACS:

- Tildeling av lesetilgang i journal for de store gruppene av helsepersonell:

  - Journalinndeling: domener: psykiatri/ somatikk
  - ”Normal tilgang”: tilgang til pasienter ved egen avdeling/ enhet
  - ”aktualisering” : tilgang til hele domenet
  - ”blålystilgang” : tilgang til alle domener

”Normal tilgang” og ”aktualiseringstilgang”

Utgangspunkt for tildeling av tilgang til pasientjournaler:

- den avdeling legen er tilknyttet
- den enhet sykepleier er tilknyttet

Helsepersonell som arbeider ved flere avdelinger/enheter:

- interne henvisninger
- Aktualisering

- Intern henvisning fungerte ikke

79% har rett til å ”aktualisere”

Helsepersonell	Aktualiseringsrett
Lege	99 %
Bioingeniør	99 %
Sekretær	98 %
Psykolog	97 %
Pedagog	96 %
Fysioterapeut	85 %
Sykepleier	72 %
Vernepleier	31 %
Hjelpepleier	15 %
Andre	84 %
Totalt	79 %

Hvilke pasientopplysninger får helsepersonell tilgang til

I utgangspunktet er journalopplysningene inndelt i grove kategorier: personellgrupper og innhold

Helseforetaket dokumenterer adgangsfunksjoner som ikke er i samsvar med faktisk tilgang

Tidsbegrenset tilgang: a) ” normalt” 30 dager
b) ”aktualisering” ingen tidsbegrensning

Datatilsynets konklusjon

Hensiktsmessig å begrense tilgangen til :

- inneliggende eller ”aktive” pasienter
- bør i større grad følge pasientforløpet
- Spesielt unødvendig at personell har generell tilgang til journaler til pasienter som ikke er under behandling

- Helseforetaket har ikke etablert nødvendig tilgangsstyring i samsvar med helseregisterloven § 13.
- Den mangelfulle tilgangsstyringen gir ikke tilfredsstillende konfidensialitetssikring etter helseregisterloven § 16, jf. Personopplysningsforskriftens § 2-11

Tilgangsstyring
Status

- For mange har tilgang til for mye
- En funksjonell tilgangsstyring må på plass
- Kombinasjon av vid tilgang og liten evne til å avdekke uautoriserte oppslag
- Det kreves systemendringer
- Tilgang må i større grad følge prosessene
  - Prosesstyrt, flytorientert, beslutningsstyrt

4. Logging

Vi er på vei fra tilstanden:

- Fraværende,
- Ubrukelige, eller
- Ikke i bruk

Til noe som er langt bedre

I dag er loggen stort sett

- Slått på, og
- Egnet for av bekrefte eller avkrefte mistanke

Logging
Veien videre

- Mot et verktøy for å avdekke uautorisert bruk
- Loggene må brukes i sikkerhetsarbeidet
- Logganalyse er nøkkelen

  - Det er viktig at vi lykkes med prosjektene
  - Regelbasert, profilbasert eller en kombinasjon
    - Det er målet som teller
  - Viktig å også ivareta de ansatte
    - Klare rammer
    - Informasjon
    - Begrense inngrepet mest mulig

5. Endringene
Hva nå

- Ny forskrift
- Tilgang på tvers blir tillatt
- Kjernejournal

Hva innebærer det i praksis?

Endringene
Hva nå - Internt

- Ingen lettelser
- Klarere krav
- En skjerpelse?
- Bl.a. krav om
  - Strukturering

Endringene
Hva nå – Samhandling

- Den planlagte rutinemessige kommunikasjonen
  => Fortsatt meldinger

  Få det på plass!

- Etter Datatilsynets syn må lokal sikkerhet spille en sentral rolle for sikker bruk av kjernejournal og tilgang på tvers
  - For tilgang på tvers – forankret i forskriften §§ 6 og 14
  - Der hvor pasienten er kan vi
    - Styre tilgangen
    - Følge opp bruken av tilgangen

Endringene
Hva nå – Samhandling …

- Dere må få på plass lokal tilgangsstyring og logging
  - Bruk av fremtidens verktøy forutsetter dette

- Bygg personvern inn i løsningen fra starten

Hva gjør Datatilsynet?
Strategi – Tilgangsstyring i journalsystem

- Bidra til **klarere rammer** for hva som kan gis av tilganger.
- kommunisere viktigheten av **beslutningsstyrt tilgangsstyring**
- følge forsøksprosjektene for **logganalyse** nøye
- **veilede publikum** om rett til innsyn i logger og sperringer i journaler
- kjenne og påvirke **leverandørene**
- arbeide for å styrke "**normen**" - innholdet og utbredelse
- **kontroll** med tilgangsstyring i journalsystemer, fortrinnsvis i samarbeid med Helsetilsynet
- samarbeide med RHFene for å få til **logganalyse**