



Erfaringer med håndtering af informationssikkerhed i klinikken

Mogens Engsig-Karup, informatikchef, Århus Amt

Informationssikkerhed er mange ting

- Fortrolighed.
 - Hvem har adgang til hvilke data?
- Ejerskab
 - Hvem bestemmer over data ?
- Kvalitet
 - Er data korrekte?
- Tilgængelighed
 - Kan vi håndtere en teknisk katastrofe ?

"De kanoniske skrifter:"

- Patientrettighedsloven
- Persondataloven
- Diverse vejledninger
 - Redegørelse om patientrettigheder og EPJ (Sundhedsministeriet april 2001)
 - IT-sikkerhedsvejledning for sygehuse (SST juli 2002)

De grundlæggende principper:

- Sundhedspersonalet på den aktuelle afdeling har adgang til informationer under det aktuelle behandlingsforløb
- Sundhedspersonalet bør spørge patienten, inden oplysninger videregives
- Sundhedspersonalet har adgang til alle oplysninger, hvis patienten giver samtykke mundtligt

Århus Amts sikkerhedsmodel

- Baseres på et relevans-princip.
- Brugeren har adgang til *relevante* data og funktioner
- Relevans knyttes til patientdata i forhold til brugerens rolle og organisatoriske placering.
- Relevans knyttes til funktioner (læse, ændre osv.) i forhold til brugerens rolle og organisatoriske placering

Udfordring for sikkerhedsmodellen

- Skal man - i en tværfaglig journal - differentiere adgang til patientdata efter roller ?
- Er journalen tværfaglig, hvis data "forsvinder", når anden bruger logger på ??
- Kan logistikken rumme tværsektorielt samarbejde i behandlingsforløbet ?
- Er 'Behandlingsforløb' foreneligt med G-EPJ ??

Udfordringer i sikkerhedsmodellen 2 ?

- Samtykke kan håndteres som journalnotat eller som sikkerhedsfunktion

Samtykket og den, som modtager det, skal registreres i journalen og samtykket markeres på de pågældende oplysninger med fornøden detaljeringsgrad af dets omfang (hvilke typer oplysninger, til hvem og til hvilke(t) formål). Samtykkemarkeringen bør henvise til det dataobjekt, hvor samtykket er registreret i journalen.

Den enkelte patient har dog direkte indflydelse på den udstrækning, hvori fortroligheden omkring vedkommendes helbredsoplysninger skal være gældende. Patienten kan nemlig modsætte sig, at en eller flere sundhedspersoner får adgang til visse af den pågældende patients data, fx oplysninger vedr. visse indlæggelser. Denne ret bør afspejles i den normale adgangsbegrænsning, som bør advisere den pågældende bruger om, at en påtænkt adgang til netop disse oplysninger ikke er tilladt. Der skal altså ikke opsættes en total spærring, men IT-systemet bør vejlede brugeren i at overholde gældende regler.

Udfordringer i sikkerhedsmodellen 3

- Kan afdelingen/sygehuset undgå samtykkekravet ved at lægge data i Sundhedsportalen ?

Udfordringer i sikkerhedsmodellen 4

- EPJ skal leve op til de overordnede målsætninger
 - tilgængelighed af data
 - ingen dobbeltregistrering
 - relevant sammenstilling af data
 - fagligt samarbejde på tværs af sektorer
- EPJ skal konfigureres løbende indenfor rimelige ressourcerammer
- Systemet skal teknisk performe tilfredsstillende

Sikkerhed bør ikke blive et problem for udvikling og implementering

Brugeren skal kunne få adgang til alle relevante data med ét logon selv, om data er registreret i forskellige systemer.

Data registreres kun én gang- og skal kunne genanvendes mange gange - evt. i forskellig sammenhæng.

En EPJ skal være tilgængelig for flere adgangsberettigede personer på én gang.

Man skal i en given situation let kunne fremfinde samtlige relevante data for den enkelte patient og for ønskede problemstillinger på tværs af patienter.

EPJ skal understøtte det sundhedsfaglige samarbejde omkring det enkelte patientforløb dels internt i de enkelte organisationer, dels på tværs af organisationer og sektorer.

EPJ skal dokumentere patientbehandlinger mhp. understøttelse af en bedre retssikkerhed for både patient og behandler.

Rapportering til sundhedsmyndigheder, herunder Landspatientregisteret skal kunne ske fra EPJ

EPJ skal opfylde krav til digital forvaltning

EPJ skal indeholde en regeleditor til brug ved alarmer og påmindelser.

EPJ skal være tilgængelig, hurtig og nem at anvende.

EPJ-data skal være beskyttet mod misbrug, tab og fejl.

Journalen skal kunne udskrives på papir ud fra specifikt definerede kriterier, eks. skal notater kunne udskrives i kronologisk orden.

Implementering af sikkerhed

Under alle omstændigheder bliver alle aktiviteter logget.

Der udvikles en "Log-browser"

- Blokering af forkert håndtering af data
- Diverse støtte-funktioner (advarselsblink)
- Ingen teknisk implementering

Patientens adgang til egen journal

- En naturlig rettighed.
- I afdelingens/sundhedspersonalets interesse bl.a. af hensyn til fejlrettelser
- Må også omfatte loggen
- Bør normalt kunne håndteres uden bistand af kliniker
- Kan eventuelt baseres på OCES-certifikater og WWW-teknologi

Amterne/sygehusene kan ikke bare henvise til Sundhedsportalen