Gradueret adgang til EPJ

Folketingets Sundhedsudvalg, November 2006

Michael Erichsen
på vegne af PROSA
merichse@csc.com

Talerens Baggrund

- Over 20 års beskæftigelse med store, integrerede systemer, både i den private og offentlige sektor
  - Heraf 10 år som chefkonsulent hos CSC
- Arbejder med IT ud fra forretningsmæssige, arkitektoniske og teknologiske synsvinkler
- Rådgivet om og deltaget i design af bl.a. CPR, SU, Den Ny Kirkebog, Tinglysning/Web og Schengen systemet, herunder sikkerhed
- Har mest arbejdet for CPR, Rigspolitiet og Økonomistyrelsen de seneste år
- Har selv ingen særlig erfaring med EPJ eller fra sundhedssektoren
  - Har konsulteret fagekspertise under forberedelsen til mødet

De Stillede Spørgsmål

- Belysning af de nuværende teknologiske muligheder for at begrænse/graduere adgangen til oplysninger i EPJ (f.eks. personfølsomme intime oplysninger uden betydning for den aktuelle behandlingssituation) – hvilke barrierer er der (økonomiske, tekniske m.v.)?
- Hvilke tekniske forhold skal der tages hensyn til nu, så man ikke iværksætter/starter op med tekniske løsninger, hvor det ikke senere hen er muligt at foretage politisk ønskelige udbygninger/tilpasninger i takt med udviklingen af de teknologiske muligheder (bl.a. i forhold til siden hen at give andre faggrupper end de nu foreslåede samt patienten selv direkte adgang til EPJ)?
- Hvilke tekniske forhold skal der lægges vægt på/tages højde for, når det skal sikres, at der ikke sker uretmæssig brug, og at man ikke kan hacke sig ind i systemerne - og er de tekniske løsninger herpå tilgængelige i dag?
- Hvilke sikkerhedsmæssige krav bør der stilles i forhold til log-in (bl.a. synspunkter på fælles log-in contra individuel person log-in), og er modellerne teknisk mulige?
- Hvilke tekniske muligheder er der i forhold til logning, så man kan se, f.eks. hvem der har søgt, hvornår og i hvilken sammenhæng, og hvor stor betydning har logning ud fra en sikkerhedsmæssig vinkel?

PROSA

Det Korte Svar

- JA, DET KAN MAN GODT!
  - En naturlig del af alle moderne IT-sikkerhedssystemer
  - Fremmes af de pågående standardiseringsbestræbelser
- Svaret er teknisk; men spørgsmålet er i høj grad politisk
  - Den tekniske løsning hedder "rollebaseret sikkerhed"
  - Den afgørende forudsætning er, at opgaver, roller og journalernes struktur er veldefinerede
  - Fremtidige, ændrede krav til gradueret adgang vil hænge uløseligt sammen med ændret anvendelse af systemet og ændringer i magtstrukturerne inden for sundhedsområdet

PROSA

Et Lidt Længere Svar

- Sikkerhed for datakommunikation og datalagring er i dag gennemstandardiseret og "kendt stof"
  - Baserer sig på kryptering, f. eks. med et digitalt certifikat
- Standarden for adgangssikkerhed er rollebaseret sikkerhed
  - Understøttes af alle leverandører på alle platforme, såvel Windows som Unix som IBM mainframes
  - Kan spille sammen på tværs af leverandører og platforme – og på tværs af organisationer og sektorer
  - Kan implementeres i platforme og operativsystemer – evt. i samspil med applikationernes indre sikkerhedssystemer

Rollebaseret Sikkerhed, Teknisk Overblik

- Brugere autenticeres og autoriseres
- Autenticering (bekræftelse af identitet)
  - Pålogning med userid, password og/eller digitalt certifikat, hvorved personlig userid og roller tildeles
- Autorisering
  - For hver ressource i systemet kontrolleres, om brugerens roller har adgang
  - Hermed kan opnås gradueret adgang – hvis ressourcerne kan beskrives entydigt i den virkelige verden
  - Hver bruger kan tillægges en eller flere roller, herunder arbejdsfunktioner og geografiske lokaliteter
  - Jo mere "finkornet" graduering, jo dyrere kan implementeringen blive, hvis eksisterende applikationer skal modificeres hertil
- Standardiseret strukturerede data er lettere at graduere end ustruktureret tekst
- Roller kan fungere på tværs mellem systemer, **FORUDSAT AT ROLLERNE ER VELDEFINEREDE OG STANDARDISEREDE**

PROSA

Roller og Adgang

- Roller bør knyttes til arbejdsopgaver, specialer, afdelinger og patientgrupper, ikke blot til oprindelig uddannelse
- Skriveadgang medfører ikke nødvendigvis læseadgang
  - Datafangst bør kunne ske af alle personalegrupper, også sådanne, som ikke har læseadgang
- Nødadgang ("slå glasset ind") skal kunne tildeles i akutte situationer med særlig logning og efterkontrol
- Visse områder bør kunne skjules (aborter), mens andre kan være synlige for alle
- Det bør kræves, at leverandørerne udvikler grænseflader, hvor medarbejdere kan tildeles gradueret adgang på en nem, logisk og overskuelig måde, svarende til deres roller

PROSA

Systemforudsætninger

- Hvis en journal blot er ét stort tekstdokument, bliver adgang et enten-eller spørgsmål
- Journaler bør struktureres i adskilte afsnit, der afspejler veldefinerede roller
- Dette stiller både krav til systemerne og til anvendernes datadisciplin

PROSA

Typiske Adgangsveje

- Sikkerheden kan også knyttes til adgangsvejen til et system
- Direkte adgang
  - Ofte en "tyk klient"
- Webadgang
  - Kræver digital signatur
- System-til-system adgang
  - Når flere og flere myndigheder indfører serviceorienterede arkitekturer (kendt som SOA), vil det blive almindeligt at kalde services i andre systemer, herunder EPJ-systemer
- Geografisk opdelte eller helt anonymiserede statistiske udtræk
  - Leveres ofte som CD-ROM, filoverførsel, webadgang eller print

Sandsynlige Fremtidige Tendenser

- Alle brancher vil møde øgede krav fra "besværlige", "urimelige" og "krævende" kunder og medarbejdere
  - "Politiske forbrugere", små årgange
- Det vil også gælde sundhedssektoren
  - "Kompetente patienter" og bekymrede døtre i 50-års alderen, øget teamwork på tværs af faggrænser
- Perspektivforskydning fra sygdomsforløb til personers fulde livsforløb
- EPJ primært som del af...
  - Hospitalers forretningsgange for sygdomsforløb
  - Individuelle borgeres digitale brugerservice (selvbetjening)
- Akkreditering vil kræve stor datadisciplin og standardisering
- Internationalisering
  - Tværeuropæisk EPJ?

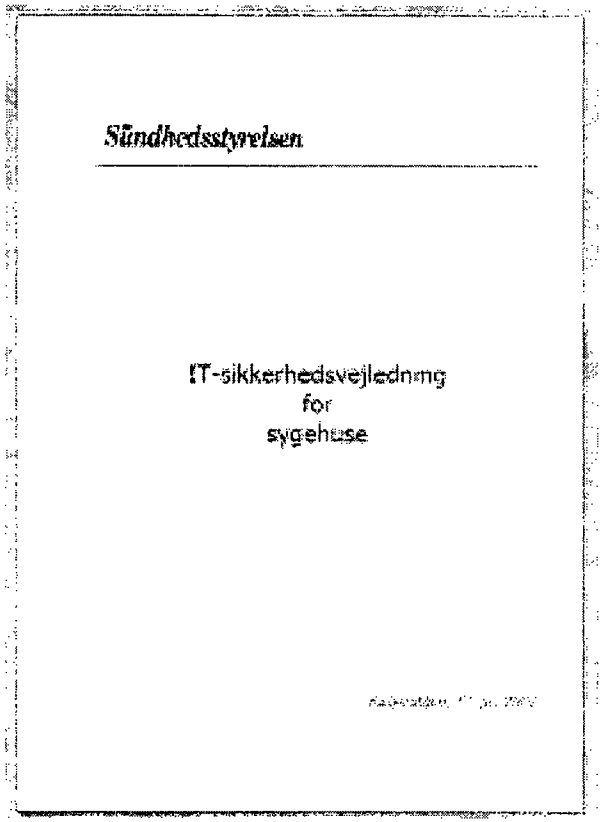
PROSA

Praktiske Spørgsmål

- Personlig Login
  - Fordelen ved personlig login er at kunne logge al adgang og efterforske "snagen"
  - Ulempen med tiden og besværet ved at logge personligt ind kan løses teknisk
    - For eksempel med chipkort (som i detailhandelen) eller med biometrisk udstyr
- Logning
  - Logning kan ske på system- eller applikationsniveau
    - Systemniveau anses for sikrest
  - Hvem kigger i loggene?
    - Stikprøver? Ekstern revision? Ekspertsystemer til at finde uregelmæssigheder? Borgerens adgang til at se logge over hvem, der har set dennes data?
  - Nem adgang til at kontrollere loggene er i sig selv adfærdsregulerende
- Fysisk sikkerhed
  - Uautoriseret overførsel af fortrolige data til mindre sikre systemer
  - Åbne terminaler
  - Print

En Læseanbefaling

- Sundhedsstyrelsens "IT-sikkerheds-vejledning for sygehuse" fra 2002 beskriver både den tekniske og den forretningsmæssige side af problemet



PROSA