RÅD FOR IT &
PERSONDATASIKKERHED

Beskyttelse af Patientdata

IT-Sikkerhed som en løsningsfaktor

Et råd under DANSK IT

www.itsikkerhedsraad.dk

Agenda

- Præsentation
  - Situation, perspektiv og løsning
  - Råd for IT- og Persondatasikkerhed
- IT-Sikkerhed omkring sundhedsdata
- Opsamling / konklusion
- Spørgsmål

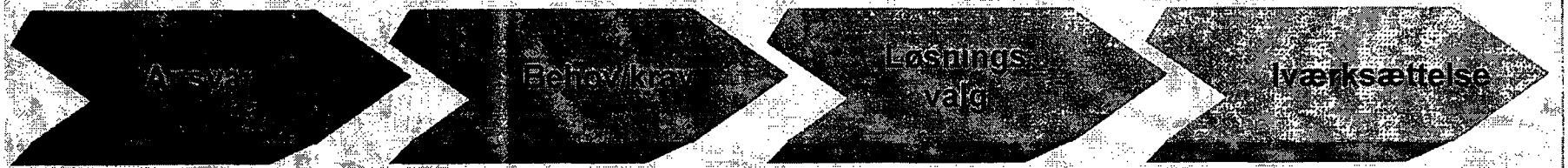
Situationen er den, at vi befinder os i et politisk behovs-skisma, hvor det ene behov forlanger bedre sundshedsbehandling, og hvor digitalisering spiller en afgørende rolle, mens det andet behov er at beskytte den enkelte borger mod misbrug af vedkommendes personfølsomme oplysninger...

Kompliceres yderligere af, at der allerede eksisterer en række systemer regionalt, hvor patientdata håndteres elektronisk, men forskelligt fra andre regioner. Endvidere er det vanskeligt at pege på enkeltpersoner eller organisationer, der har det overordnede ansvar for databehandlingen eller beskyttelsen

Løsningen er IT-Sikkerhed

- IT-Sikkerhed er ikke blot en irriterende hindring for yderligere digitalisering
- **Det er som bremserne i en bil**..
- IT-Sikkerhed er den "vaccine" der kan få digitaliseringen til at tage fart, på god og betryggende vis

Hvad betyder det i praksis?



Styring…?

- DANSK IT's Råd for IT- og Persondatasikkerhed:
  - etableret i foråret 2006 for at styrke debatten om it-sikkerhed i virksomheder, hos det offentlige og for de private it-brugere.
- Temaer
  - **Borgerbeskyttelse (herunder patientdata..)**
  - **Lovgivning & standarder**
  - **Uddannelse**
  - **Leverandører**
- Rådet behandler sikkerhedsspørgsmål teknologi-neutralt
  - Herunder også hvad angår leverandører og produkter.
- Rådets kommissorium er fastsat af DANSK IT's bestyrelse
  - Dog i tæt dialog med Rådets medlemmer, der ikke nødvendigvis alle er medlemmer i DANSK IT.
- Medlemmerne i rådet:
  - dels ud fra deres personlige kompetencer
  - dels som repræsentanter for en bestemt organisation, kreds eller forening.

Medlemmer af rådet:

- Formand
  Kim Aarenstrup, A.P. Møller - Mærsk Gruppen
- Næstformand
  Adser Leick, LEGO Koncernen
- **Per Buchwaldt**, tidl. formand for DANSK IT's bestyrelse, Deloitte Business Consulting
- **Vibe Valentin Jensen**, Post Danmark
- **Jørn Knudsen**, HS:direktionen
  (Medlem som repræsentant for IT-Sikkerhedschefkredsen, DANSK IT)
- **Morten Klitgaard Friis**, KPMG
  (Medlem som repræsentant for IT-Sikkerhedsfagrådet, DANSK IT)
- **Martin von Haller Grønbæk**, Bender von Haller Dragsted
- **Poul Otto Schousboe**, Danske Bank
- **Faruque Abu Sayed**, PriceWaterhouseCoopers
- **Agnete Sigurd**, udpeget af Forbrugerrådet
- **Kim Mikkelsen**, Microsoft
- **Henning Mortensen**, udpeget af ITEK
- **Jørgen Torp**, udpeget af Foreningen af Statsautoriserede Revisorer
- **Brian Birkvald**, IBM Danmark
- **Tony Franke**, direktør Dansk IT

- Ansvarsplacering
- Trusler og konsekvenser
- Borgernes retsstilling & interaktion
- Løsninger & synergier
- Revision

- Ansvarsplacering
  - Mangel på placering af dataansvarlig ifht persondataloven
  - Har betydning for det IT-Sikkerhedsmæssige
  - Undtagelse er dog lægemiddelstyrelsen / Medicinprofilen
  - Hvis registrene bliver centrale, bør ansvaret ligge centralt
  - **i en overgangsfase** måske acceptabelt med regionalt ansvar for de regionale systemer
  - I tilfælde af flere dataansvarlige myndigheder, bør der i loven fastsættes bestemmelser om
    - At Indenrigs- og Sundhedsministeren f.eks. kan fastsætte regler om system-, data- og driftssikkerheden.
    - En lignende praksis findes i finanssektoren, hvor de finansielle institutioner i praksis tilslutter sig de sikkerhedsbestemmelser, der udstedes af fælles datacentraler.

- Trusler og konsekvenser
  - IT-Sikkerhed er andet end hvem der har formelt adgang til hvad
  - Mindst lige så væsentlige områder som:
    - Datakvalitet eller integritet
    - Datatilgængelighed
    - Ekstern uautoriseret adgang (ved hackning eller systemlækager).
  - **Datakvaliteten:**
    - Hvis patientdata ikke har en høj integritet (ved f.eks. backup og genindlæsning eller forskelle i data-tabel formater), så kan det betyde fejl-behandlinger
  - **Utilgængelighed:**
    - Banalt driftsnedbrud eller dataødelæggelse (virus/orme angreb, fjendtlig overtagelse)
    - Betyder manglende adgang til livsvigtige patientdata
    - Standser eller farliggører behandlingsprocessen
    - Nødprocedurer for manuel håndtering
  - **Ekstern skadelig adgang:**
    - Manglende systemvedligeholdelse og/eller kontroller skaber bagdøre til systemerne
    - Hacktivisme / journalister / penge
  - **Adgangskontrol:**
    - Efter behov
    - Godkendt af patienten
    - Systemkontroller til håndtering af "autorisations niveau"

- Borgernes retsstilling & interaktion
  - Udgangspunktet bør være at borgeren bestemmer
    - Hvem der har adgang
    - Hvornår..
    - Hvor meget (livslangt, tidsbegrænset eller slet ikke)
  - Krav om patient-behandler relation
  - Må ikke kunne krænkes, bortset fra nødsituationer
  - Effektiv individuel adgangskontrol
  - Logning af aktiviteterne, samt revision af disse
  - Statistik skal være person uidentificerbart
  - Flexibilitet
    - Forskellige borgere, forskellige ønsker/behov
  - Bør princip-styres via lovgivningen
  - Løbende revision af IT-Sikkerheden som for finanssektoren - det er ikke en opgave for Datatilsynet

- Løsninger & synergier
  - Patienten kan også være skatteyder, institutionsbruger, socialklient, biblioteksbesøgende oma.
  - Forskellige beskyttelses behov
  - Samme IT-sikkerhedsteknologier og koncepter
- Sigt efter en national helhedsløsning
  - Offentlig certifikat-infrastruktur eksisterer allerede (OCES)
  - Internetsikkerhed via borgerens personlige certifikat
  - Rygraden i en offentlig IT-Sikkerhedsløsning
  - Sygesikringsbevis med chip som borgerens garanti
  - Kortlæsere hos læger, på apoteker og på hospitalerne
  - Internetportal giver borgeren mulighed for at sætte standardbegrænsninger – definere sin åbenhed
- Eksisterende løsninger justerer over tid

- Politisk styret fyrtårns-effekt
  1. Centralt ansvar for IT-Sikkerhed – (bredt offentligt sigte)
  2. Ensartede nationale data-/tabel definitioner
  3. Udnyt OCES certifikat infrastrukturen bedst muligt
  4. OCES er pt. underlagt en opdatering/ændring - optimal timing
  5. Effektiv individuel adgangskontrol (krav om behandler relation)
  6. Logning nødvendig/lovpligtig - erstatter ikke adgangskontrol
  7. Undgå silo-dannelse / sub-optimering
  8. Patienten bestemmer - certifikat/fysisk kort m. chip og certifikat
  9. Kortet bør kunne bruges bredt i det offentlige
- Professionalisme
  - IT-Sikkerheden afhænger af system-kvaliteten
  - Dansk Standard for IT-Sikkerhed DS484
  - Perimeter sikkerhed, interne (tekniske) kontroller
  - Intern og ekstern revision - ikke Datatilsynets opgave

Spørgsmål?