Implementering af Privacy Enhancing Technologies i EPJ

- Hvordan sikrer vi overholdelse af Patientdatalovgivningen?

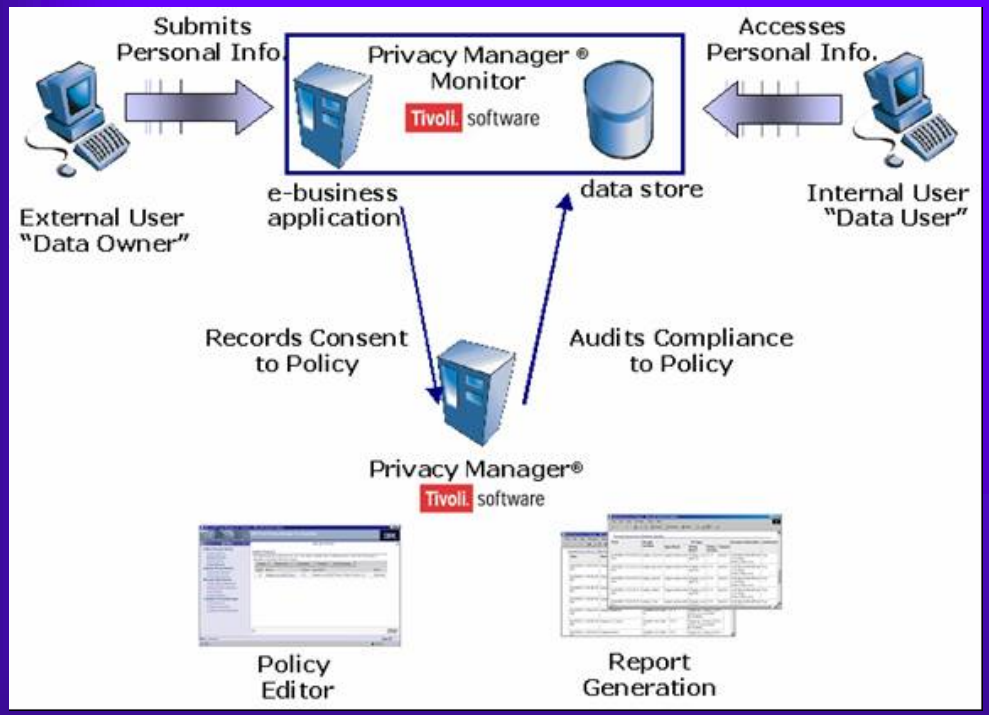
Privacy Management – Baggrund/funktion
Erfaringer fra Storstrømmens Amt – Pilotprojekt
Patientdataloven med og uden Privacy Management
Samspil mellem Identity, Access og Privacy Management

Søren Duus Østergaard
Senior eGovernment Advisor
IBM Europe, Middle East & Africa

Enterprise Privacy Architecture Language

- IBM's laboratorie i Zürich, der har ansvaret blandt andet for sikkerhedsløsninger, har udviklet et XML-sprog, der kan oversætte sikkerhedspolitikker til et maskinlæsbart format.
- EPAL er overgivet til W3C som forslag for en åben standard, der væsentligt udvider P3P-mulighederne
- Sproget indgår i IBM Privacy Manager, der er en del af IBM sikkerheds-SW.
- Løsningen fungerer som et filter mellem eksisterende applikationsprogrammer og databaser og kan sikre at læsning/visning/forsendelse på feltniveau kun sker til autoriserede brugere i en godkendt proces, d.v.s. formåls- og identitetsstyret adgang.
- Systemet genererer automatisk log af alle events

Privacy Management - Løsning

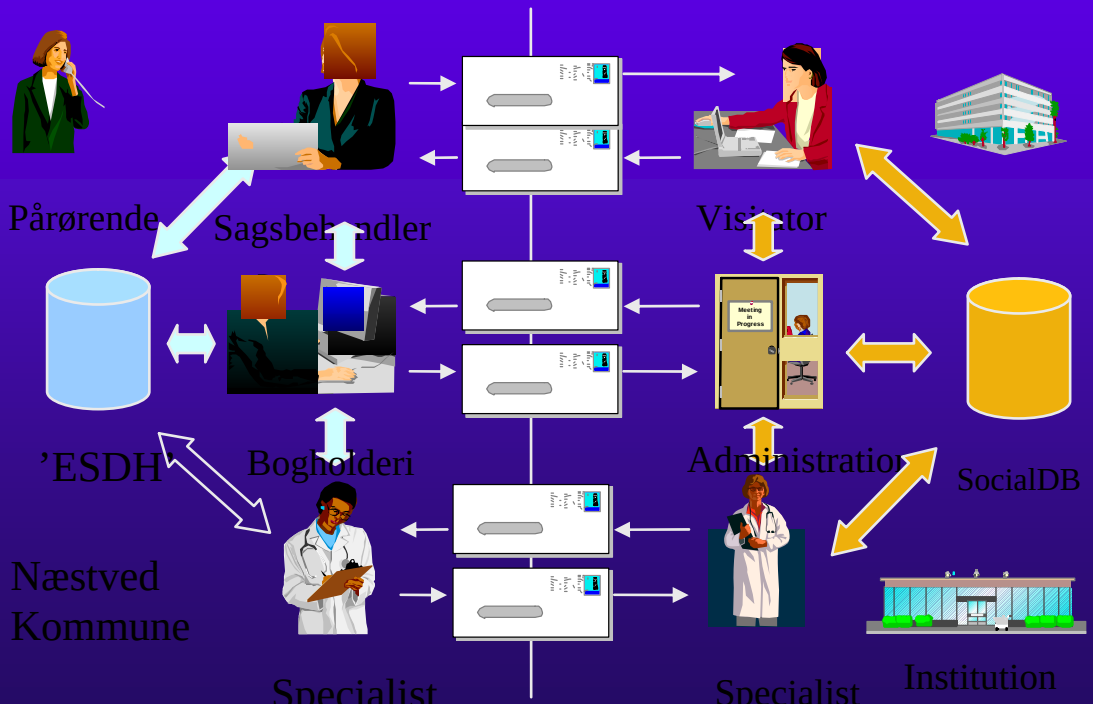


Policy databasen indeholder EPAL-kodede politikker. Mellem applikation og DB etableres en monitor, der Uden at afbryde operationen opsnappes databasekald og sammenholdes med policy. Datarecords filtreres ved returnering til programmet.

Privacy Manager er implementeret bl.a. i Australiens Health Insurance Company (Sygesikring) med 19 mio patientrecords

Case: Storstrømmens Amt :

Storstrømmens Amt har etableret en SQL/ISS-baseret 'socialdatabase', der indeholder både sundhedsmæssige, Sociale og økonomiske patientdata for institutionsanbragte Personer i Amtet. På grund af fortrolighedskrav kunne eksterne brugere og kommunale sagsbehandlere ikke få adgang – medførte dyre, langsomme sagsgange for alle

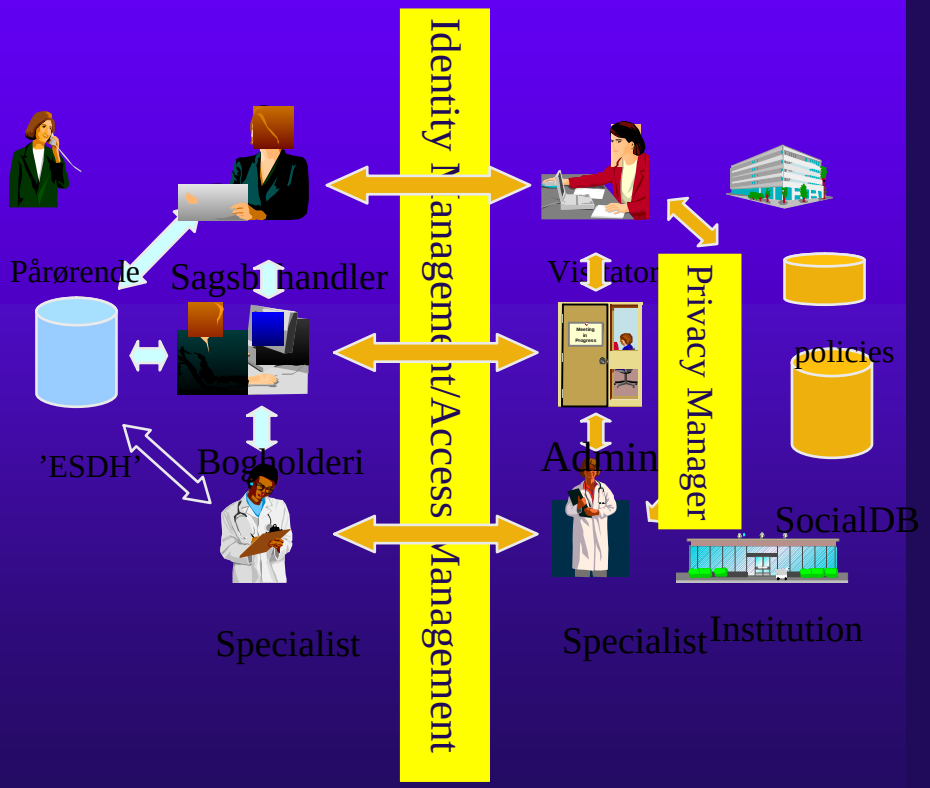


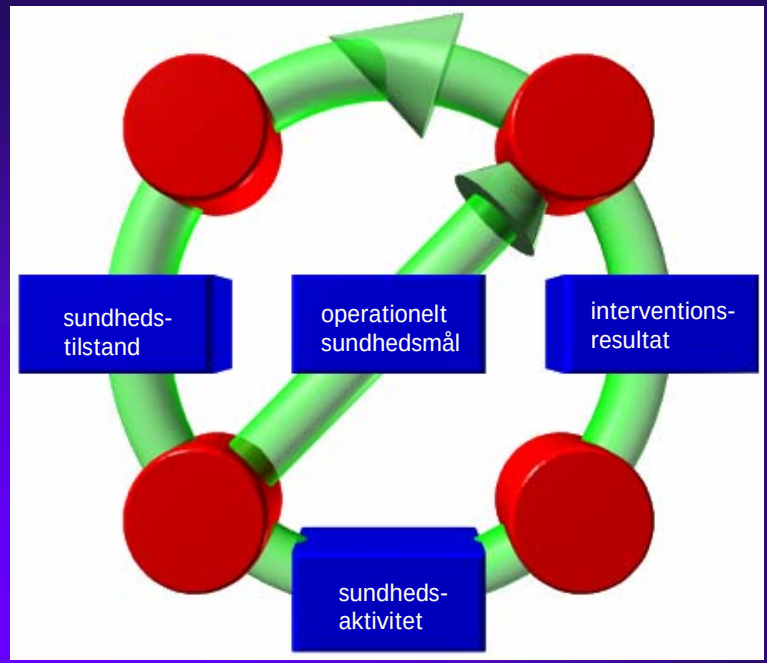
Projekt:
Test en kombination af OCES certifikater til alle ansatte og Privacy Manager på den bestående SQL/IIS-løsninger

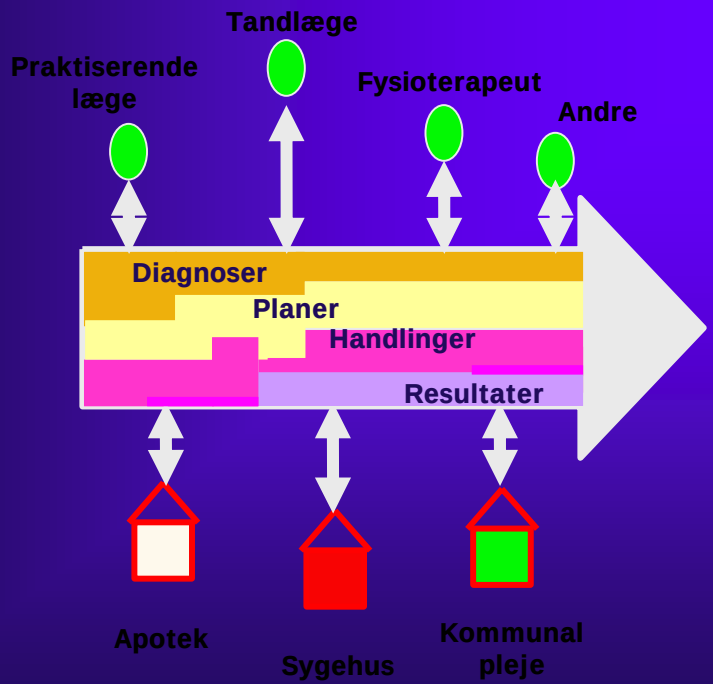
Case: Storstrømmens Amt

Resultat:
Ved indførelse af medarbejdercertifikater og rollebaseret, fælles adgangskontrol checkes identiteten.
Gennem de opstillede politikker får applikationer med kendte identer adgang til at se de felter i databasen, som politikken har godkendt.

Løsningen kan overføres til enhver EPJ-lignende applikation / Database







Fælles information – G-EPJ

EPJ – sikkerhed:

-Identifikation af alt sundheds-personale ved digitale signaturer

-Styring af adgangsrettigheder

-Overholdelse af regler om patientdata/datasikkerhed/ videregivelse af info

Hvilke funktioner skal udføres?

- Opstil samtykke politik for den enkelte EPJ
- Uddan alt personale i regler og anvendelse, dokumentationsregler, logning o.l.
- Informer patienter og registrer samtykker i journalen
- Påfør i journalen hver gang der videregives oplysninger og marker om samtykke er OK
- Udfør kontrol af om reglerne overholdes
- Gennemfør periodiske stikprøver
- Gennemfør periodisk check af om personalet har forstået reglerne ’tro og love’ eller ...
- Håndter klagesager – fremhentning af dokumentation

Konklusion: En dyr, mandskabskrævende og ikke 100% sikker proces

Styring af samtykker med Privacy Manager:

- Definer samtykke politik ved hjælp af XML-lignende sprog (EPAL)
- Opret ’policy database’ og etabler filtre mellem applikationen og EPJ
- Patientsamtykke registreres elektronisk
- Overvåg identitet, formål og brug af data
- Log enhver adgang eller forsøg på adgang til PII automatisk
- Generer detaljerede revisionsrapporter

Minimerer uddannelsesbehov og manuel håndtering – og giver 100 pct. styring i henhold til de nedskrevne politikker via EPAL

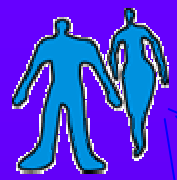
EPAL eksempler mod EPJ:

- **Sygesikringskontoret vil bruge cpr-nummer, navn og addresse information, medicin-ID for at sende hjem-amtet en opdateret status over forbrug**
- **Læge xx kan få læseadgang til epikrise-information for de patienter, der har valgt ham/hende hvis samtykke ikke er ældre end 12 mdr. fra dato**
- **Hvis du giver samtykke, vil speciallæge yy få adgang til din sygejournal for seneste indlæggelse for at indkalde dig til efterbehandling og dit samtykke ikke er ældre end 12 mdr. fra dato**
- **Professor zz vil benytte operationskode og information om indlæggelsessted/varighed fra din sygejournal til brug for forskningsstatistik hvis OK fra sundhedsstyrelsen medmindre du nægter at deltage eller du ikke er dansk statsborger**

EPAL eksempel:

<STATEMENT>
<EXTENSION optional="**yes**">-
<STATEMENT-EXT xmlns="**http//www.ibm.com/BTB/ALPHA/P3P**">
<DESCRIPTION>**Epikriseinfo praktLaege**</DESCRIPTION>
</STATEMENT-EXT>
</EXTENSION>
<**CONSEQUENCE**>**Laege XX kan få adgang til din epikriseinfo ved udskrivelse fra hospital YY**</**CONSEQUENCE**> -
<PURPOSE> <other-purpose required="**samtykke**">**Meddelelse: Patient vil modtage nen email når epikrisebrev er sendt til læge XX** </other-purpose> </PURPOSE>-
<RECIPIENT>- <ours>
<recipient-description>**Hospital YY, afdeling ZZ, doktor VV**</recipient-description> </ours> </RECIPIENT>-
<RETENTION> <stated-purpose /> 24.5.2004 </RETENTION>-
<DATA-GROUP base="">- <DATA optional="**no**" ref="**#laegeXX.email.address**">-
<CATEGORIES> <online /> </CATEGORIES> </DATA> </DATA-GROUP>
</STATEMENT>

Samlet løsning af sikkerhed



In-house Apps

Webified Apps

Non Web Apps

Revision – Hvad har jeg gjort?

Privacy– Hvornår har andre adgang til mine data?

Access kontrol – Kan jeg komme ind og udføre dette?

Authenticer – bevise at det er mig

Authoriser Hvad har jeg lov til at gøre?

Adskilte øer, adskilt administration administration og expertise

Dublerede identitets funktioner i hver 'ø'

Transaction Processing

Operating Systems

EPJ

Sikkerhed

Autoritative Identitets myndigheder

Admin. data

Høje driftsomkostninger

Dårlig identitetskontrol goiver dårlig sikkerhed

Høje udviklingsomkostninger