Sikkerhet i kjernejournal

Rune Røren

HelsIT 2013 - Sikkerhetsdagen

Trondheim, 19. september 2013

Agenda

- Kort om kjernejournal
- Hvem får tilgang til hva?
- Hovedtruslene ifht. informasjon på avveie
- Hovedtiltakene
- Noen erfaringer

Behovet for kjernejournal (fase 1)

Planlagt forløp

Uplanlagt forløp

Fastlege

Sykehus

Apotek

Uplanlagt hendelse
(2/3 av døgnopphold
i spesialisthelsetjenesten
starter uplanlagt)

AMK / Legevakt /
Akuttmottak

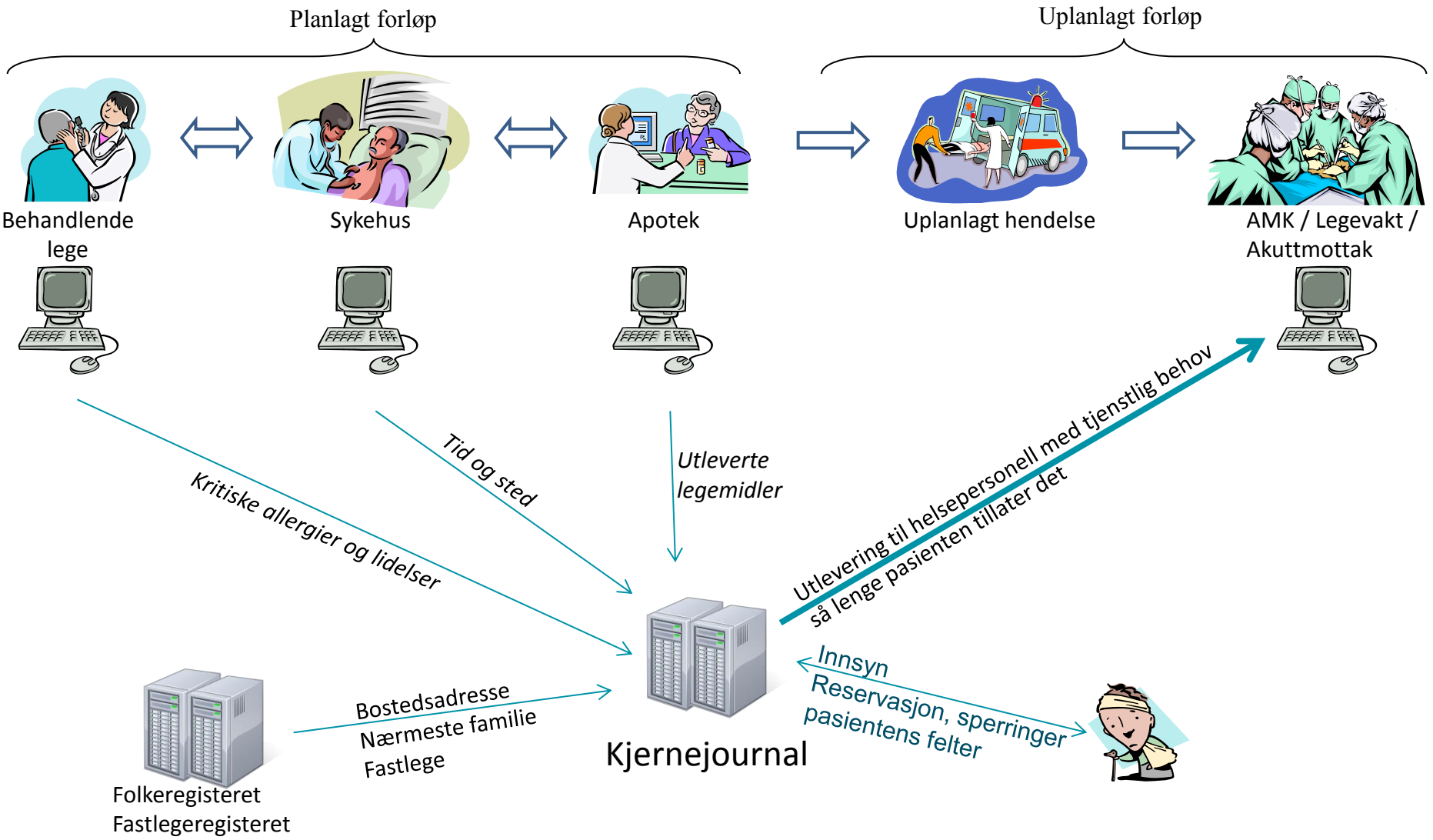
?

?

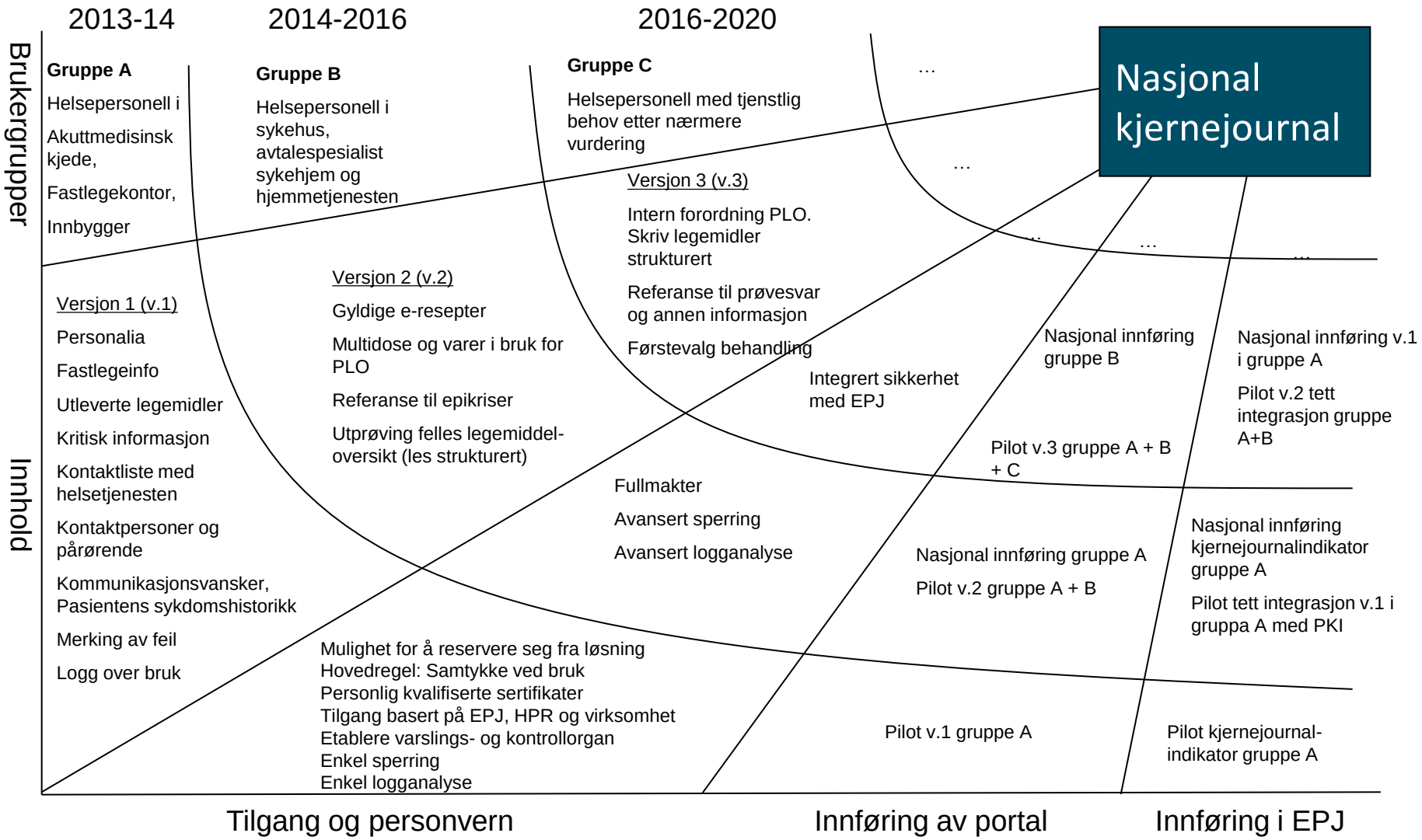
?

Ingen elektronisk utveksling

Løsningen med kjernejournal (fase 1)



Utvikling av kjernejournal



Status 17.09.13

- Forskrift trådte i kraft i juni
- Leveranse 1 er utviklet, testet og satt i produksjon
- 5 av 6 EPJ leverandører har utviklet, testet og satt i produksjon v.1
- Pilot i Trondheims-regionen startet 30. august
  - Innbyggerne i Trondheim, Malvik, Melhus og Klæbu har fått kjernejournal
  - Innbyggerne får tilgang via helsenorge.no
  - Et lite utvalg av helsepersonell får tilgang til EPJ-løsningen (brøytekjøring)
  - Innhenting av legemiddelinformasjon har begynt
  - HELFO (800HELSE) tar imot henvendelser fra innbyggere
  - Norsk Helsenett drifter løsningen
- November 2013 kommer leveranse 2
  - Helsepersonell tar løsningen i bruk
  - Innbyggerportalen (helsenorge.no) utvides slik at alt innhold i kjernejournal vises
- Vi tar sikte på pilot i Stavanger i 2014
- Vi tar sikte på landsdekkende utrulling i 2015

Agenda

- Kort om kjernejournal
- Hvem får tilgang til hva?
- Hovedtruslene ifht. informasjon på avveie
- Hovedtiltakene
- Noen erfaringer

Tilgang for innbygger

- Innbygger får tilgang til sine opplysninger på helsenorge.no
- Innbygger må autentisere seg på nivå 4 hos ID-porten
- Innbyggere uten fødselsnummer eller D-nummer får ikke kjernejournal
- Innbyggere med bostedsadresse utenfor innføringsområdet får ikke kjernejournal (ikke informert om løsningen)
- Trusselutsatte personer (kode 6 og 7) får ikke kjernejournal
- Barn under 16 år får ikke tilgang til helsenorge.no
- På sikt skal foreldre og de med fullmakt får innsyn
- Innbyggere skal kunne reservere seg og sette sperring
- Innbyggere skal kunne fylle ut «pasientens felter»

Tilgang for helsepersonell

- Kun helsevirksomheter på Norsk Helsenett kan få tilgang
- Foreløpig gjelder tilgangen den akuttmedisinske kjeden (AMK-sentral, akuttmottak, legevakt) og fastlege
- Helsepersonell skal være autorisert i virksomheten for tilgang til kjernejournal, og de må ha gjennomgått opplæring
- Helsepersonell skal gi helsehjelp for å kunne slå opp
- Oppslag kan kun gjøres fra lokal EPJ (Elektronisk pasientjournal)
- Helsepersonell må autentisere seg på eID nivå 4 for å få tilgang
- Helsepersonell kan slå opp på alle innbyggere som finnes i lokal journal
- Helsepersonell kan foreløpig se alt i kjernejournal
- Alt helsepersonell kan hjelpe pasienten fylle ut sine felter
- Kun leger kan fylle ut kritisk informasjon

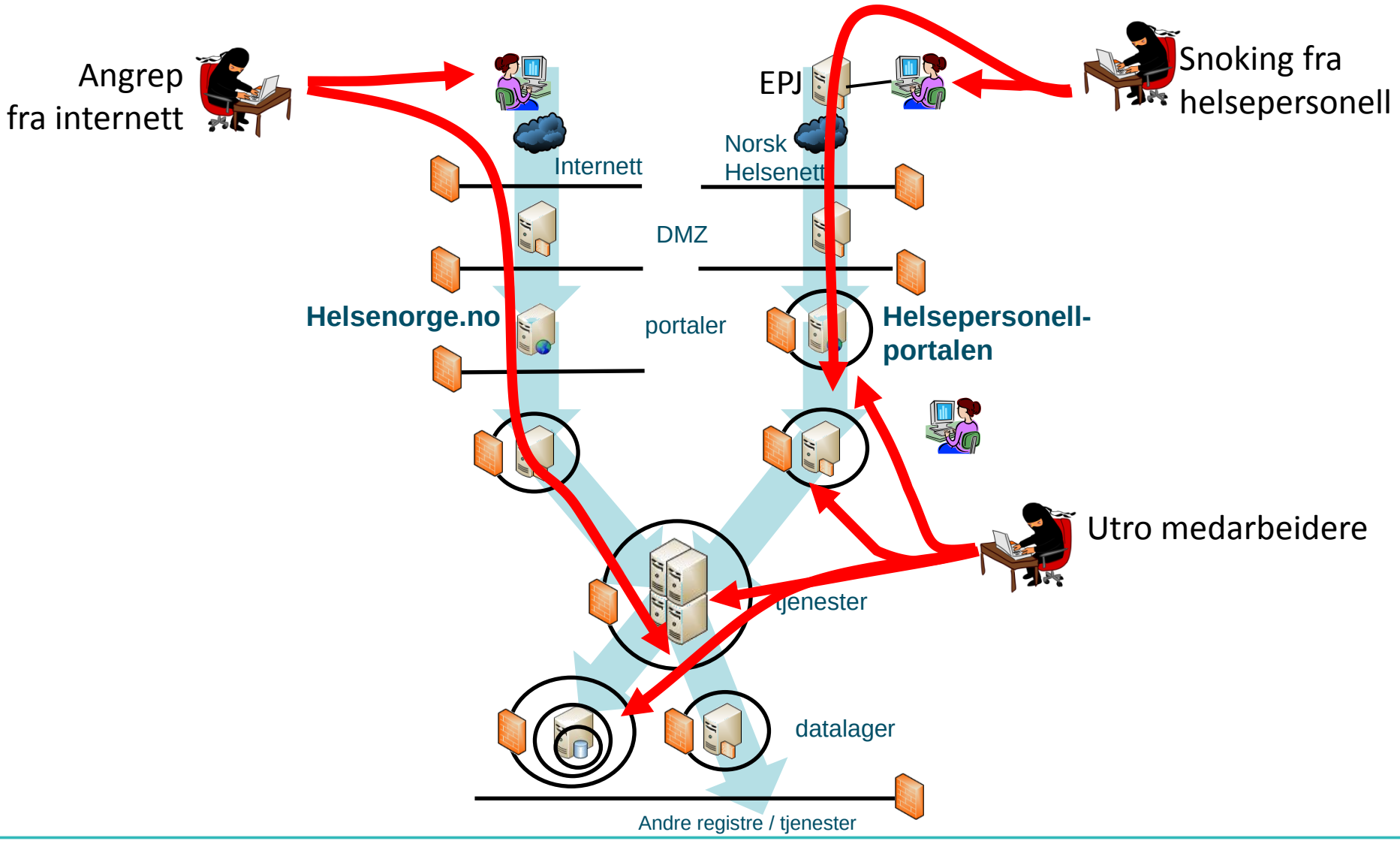
Tilgang for andre

- Brukerstøtte får tilgang til å hjelpe innbyggerne med reservasjon og sperringer, men de får ikke tilgang til helseopplysninger
- Et fåtall saksbehandlere hos Helsedirektoratet får tilgang til innbyggernes kjernejournal for å kunne følge opp feil, innsynskrav, krav om retting og sletting m.fl.
- Driftspersonell skal ikke ha tilgang til helseopplysninger, men i praksis kan et fåtall få tak i det
- Utviklere skal ikke ha tilgang til helseopplysninger, men i praksis kan de legge inn «bakdører» i løsningen

Agenda

- Kort om kjernejournal
- Hvem får tilgang til hva?
- Hovedtruslene ifht. informasjon på avveie
- Hovedtiltakene
- Noen erfaringer

Hovedtruslene



Angrep fra Internett

Forebyggende tiltak

- Informasjonsbegrensning
- Teknisk dybdesikkerhet mht. nettverk/transport, applikasjon og database
- Utstrakt bruk av sikkerhetsprodukter
- Sikkerhet som del av utviklingsmetodikken
- Patching og herding
- Penetrasjonstesting

Oppdagende tiltak

- Kontinuerlig overvåking. Rask varsling

Reagerende tiltak

- Beredskapsplaner og øvelse
- Rask «Lock down»
- Backup og restore

Snoking fra helsepersonell

Forebyggende tiltak

- Informasjonsbegrensning
- Avtale med virksomhet om bruk av løsning
- Tilgangskontroll for helsepersonell
- Opplæring og godkjenning av helsepersonell
- Svartelisting av helsepersonell

Oppdagende tiltak

- Tilgangslogg tilgjengelig for pasient på Internett
- Automatisk logganalyse
- Stikkprøver
- Automatisk varsling til pasient ved oppslag (kommer senere)

Reagerende tiltak

- Beredskapsplaner og øvelse
- Anmeldelser til Helsetilsynet
- Informere pasient om hendelsen

Utro medarbeidere

Forebyggende tiltak
- Informasjonsbegrensning
- Valg av drifts- og utviklingsleverandører
- Rolledeling, kryptering, pseudonymisering og splitting av data
- Sikkerhetsklarering
- Sikkerhet som del av utviklingsmetodikken
- Sikkerhetsrevisjon og kodegranskning

Oppdagende tiltak
- Tilgangslogg tilgjengelig for pasient på Internett
- Automatisk logganalyse
- Stikkprøver
- Automatisk varsling til pasient ved oppslag (kommer senere)

Reagerende tiltak
- Beredskapsplaner og øvelse
- Sparken

Agenda

- Kort om kjernejournal
- Hvem får tilgang til hva?
- Hovedtruslene ifht. informasjon på avveie
- Hovedtiltakene
- Noen erfaringer

Sikkerhet i kjernejournal

Helhetlig fokus på sikkerhet

Ledelse	Innføring	Teknisk løsning	Drift	Forvaltning
• Tydelig organisering og ansvar • Finansiering • «Levende» ROS • Skape en god sikkerhets-kultur	• Kartlegging og oppkobling av virksomheter • Opplæring og godkjenning av helsepersonell • Informasjon til innbyggere	• Sikkerhet i dybden • Dedikerte sikkerhets-produkter og –teknologi • Sjekklister og standarder • Pen.tester og revisjoner	• Fysisk sikring • Nettverks-sikkerhet • Redundans • Overvåking • Herding og patching • Backup og restore	• Beredskap og øvelser • Internkontroll • Logganalyse • Misbruks-oppfølging • Anmeldelser

Krav (lov og forskrift, Normen, sikkerhetspolicy)

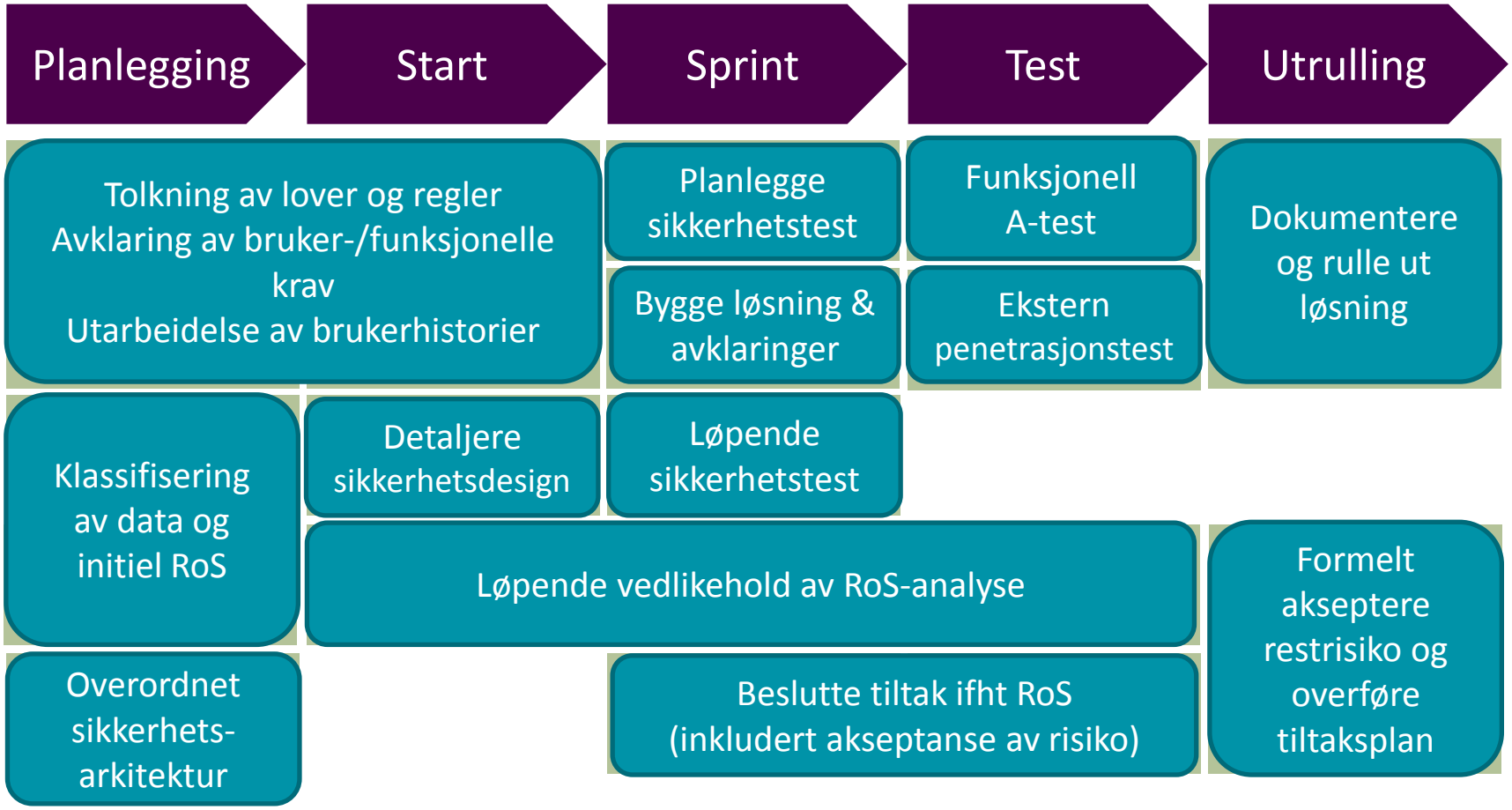
Organisering og finansiering av sikkerhet (2012-13)

- Sikkerhetspersoner
  - 2 personer i anskaffelse
  - 1 sikkerhetsleder fast i prosjektet m/medhjelper
  - 1 produkteier sikkerhet
  - 1 dedikert SCRUM-team på sikkerhet (8 personer)
  - 2 sikkerhetsarkitekter
- Økonomi – ca. 55 MNOK på sikkerhet
  - ca. 10 MNOK på krav, oppfølging og RoS
  - ca. 6 MNOK på sikkerhetsprodukter
  - ca. 32 MNOK på design, utvikling og systemtest (45%)
  - ca. 7 MNOK Akseptansetest (45%)
- Sikkerhetstjenester i NHN/drift kommer i tillegg

Sikkerhetskultur

- Sikkerhet var viktigste kriterium i anskaffelsen
- Fokus på sikkerhet i opplæring bl.a. med gjennomgang av trusselbildet og Normen
- Sikkerhetsklarering av tekniske ressurser
- «Levende» RoS med egen plass i ukentlig risikovurdering
- Åpenhet om sikkerhetsutfordringene (ledelsen eier problemet)
- Sikkerhet som del av utviklingsmetodikken

Sikkerhet som del av utviklingsmetodikken



Teknisk dybdesikkerhet i løsningen

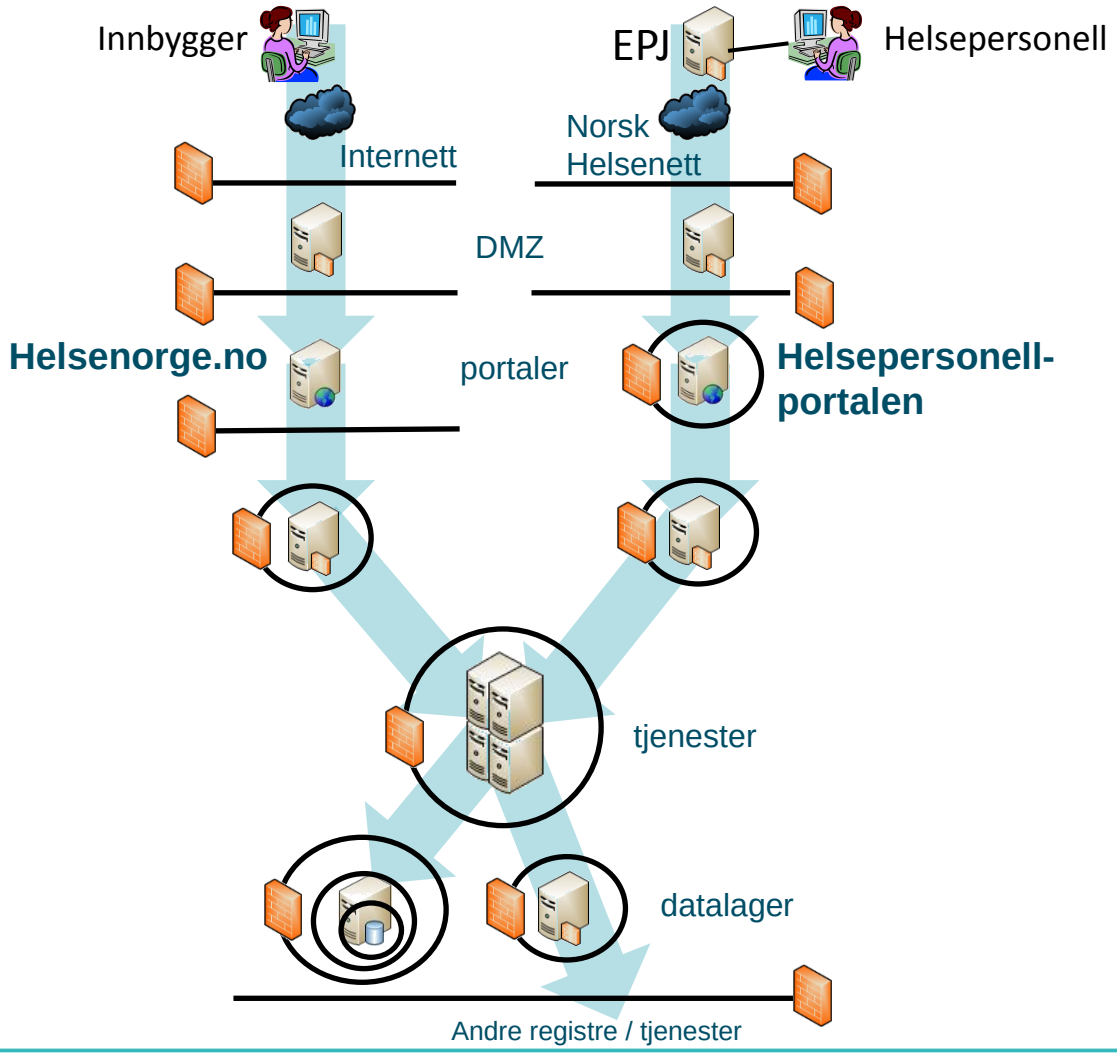
Fysisk
Datahall
Lastbalansering

Nettverk/transport
Brannmurer/IDS
SSL/sertifikater

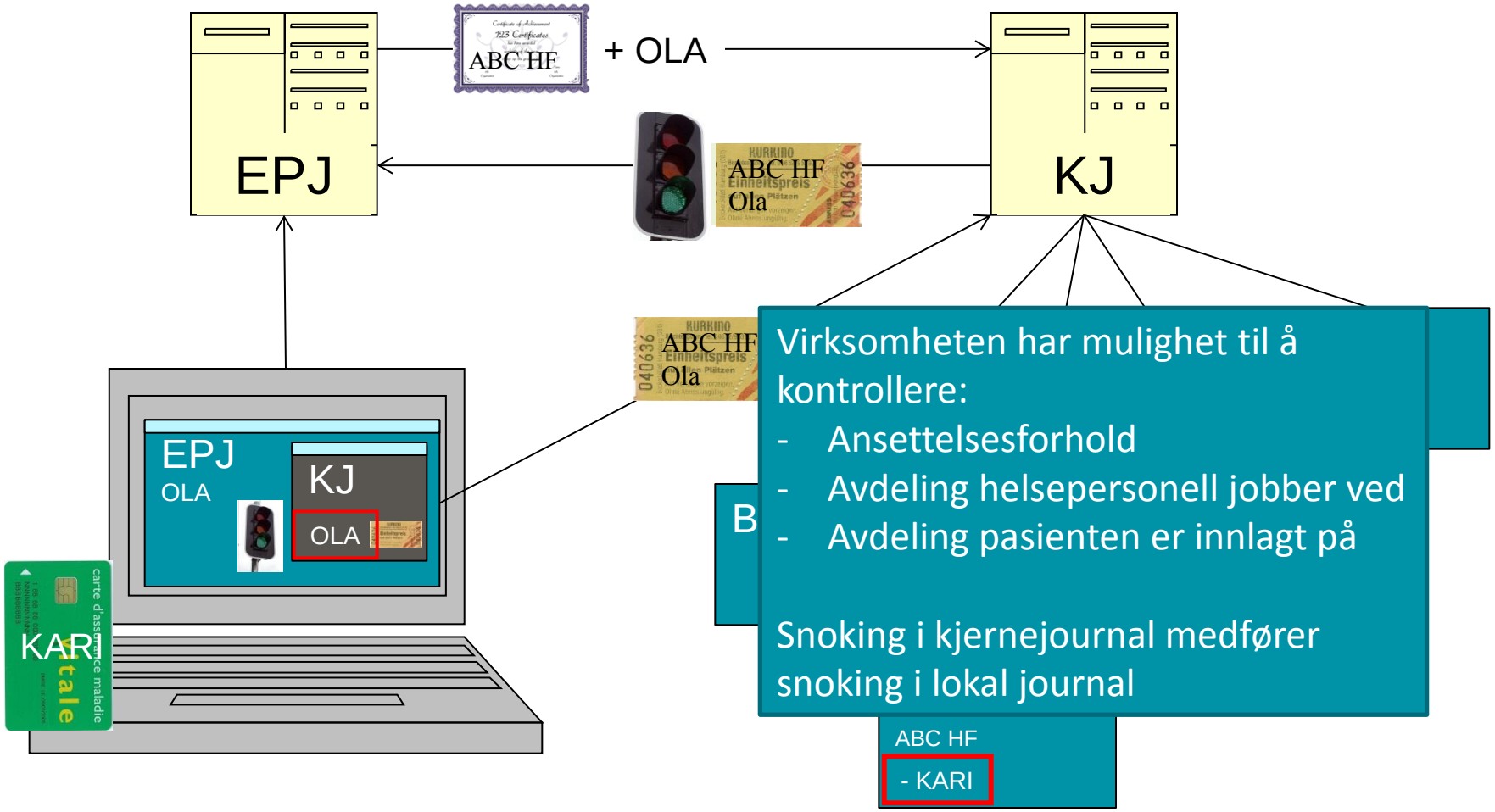
Applikasjon
Tilgangsstyring – I&AM
Inputvalidering
Pseudonymisering

Database
Splitting av data
Kryptering
Rolledeling

Drift
Overvåkning



Tilgang for helsepersonell er knyttet til tilgang i lokalt EPJ



Sikkerhet i innføring

- Godkjenning av EPJ
  - Tilgang skal skje gjennom lokal journal
- Oppkobling av virksomhet
  - Kartlegging av sikkerhet
  - Ansvarliggjøring av virksomhet og lokal administrator
- Opplæring av helsepersonell
  - Opplæringsmaterialet fokuserer på konsekvensen av sikkerhetsbrudd
  - Godkjenningstest krever kunnskap om sikkerhet
- Informasjon til innbyggere

Personverntiltak innbyggeren kan velge

Forebyggende tiltak

- Reservasjon mot løsning – helseopplysningene slettes, innsamling stopper
- Sperring mot internett – fortsatt tilgjengelig for helsepersonell
- Sperring av opplysninger – helsepersonell må be om samtykke eller bruke nødretten for å få tilgang

Oppdagende/reagerende tiltak

- Følge med på innsynsloggen av og til
- Melde mulige sikkerhetsbrudd til HELFO – som videresender saken til Helsedirektoratet

Informasjonsbegrensning

- Mange innholdselementer er tatt ut
  - Fullstendig journal
  - Sykdomshistorikken
  - Epikriser, prøvesvar, gravidekort m.fl.
  - Blodtype, smittesykdommer m.fl..
- Innholdselementene er tidsbregrenset
  - Kritisk informasjon lagres kun så lenge det er relevant
  - Legemidler lagres i 3 år
  - Kontaktliste med primærhelsetjenesten lagres i 3 år
  - Kontaktliste med spesialisthelsetjenesten lagres med full historikk
  - Pasientens felter lagres så lenge pasienten ønsker

Agenda

- Kort om kjernejournal
- Hvem får tilgang til hva?
- Hovedtruslene ifht. informasjon på avveie
- Hovedtiltakene
- Noen erfaringer

Noen erfaringer

- Lovverket vektlegger personvernet mer enn pasientsikkerheten
- Utviklere vil legge inn bakdører for å forenkle utvikling
- Drift vil oppgradere komponenter uten å ha hatt nok tid til gode nok risikovurderinger
- Helsepersonell vil finne snarveier hvis sikkerhet blir for komplekst/tidkrevende
- Det er stor variasjonen av IT-utstyr der ute
  - SHA256-signering på .Net 3.5 på XP fungerer ikke
  - Klokke-problematikk
- Samtidig oppdatering av sertifikater skalerer dårlig. Støtte til to sertifikater bør bygges fra starten

Spørsmål?

Ekstra

Fra informasjonsbrosjyre

Reservasjon og sperring

Reservasjon
Du får automatisk kjernejournal hvis du ikke aktivt reserverer deg. Du kan reservere deg når som helst. Det innebærer at alle helseopplysninger om deg slettes, og at nye opplysninger ikke samles inn. En reservasjon vil kun gjelde kjernejournal.

Reserverer du deg, vil ikke helsepersonell kunne se opplysningene i kjernejournal når du får behandling.

Du kan alternativt reservere deg slik at du ikke kan logge på kjernejournal via helsenorge.no. Da er kjernejournalen kun tilgjengelig fra datasystemene som helsepersonell bruker.

Sperring
Du kan sperre hele eller deler av kjernejournalen din slik at helsepersonell må be om samtykke for å se opplysningene. Sperringen kan åpnes dersom du ikke kan gjøre rede for deg.

Les mer om reservasjon og sperring på **www.helsenorge.no/kjernejournal** eller ring 800HELSE (altså 80043573).

Sikkerhet og personvern

- Kun godkjente virksomheter i helsetjenesten får tilgang i et lukket helsenett.
- Kun autorisert helsepersonell får slå opp i kjernejournal, og bare når de gir deg helsehjelp.
- Helsepersonell må identifisere seg på høyeste sikkerhetsnivå og all aktivitet loggføres.
- Du kan selv følge med på hvem som har gjort oppslag i kjernejournalen din.
- Kun du får tilgang til helseopplysningene dine på helsenorge.no. Du må identifisere deg på høyeste sikkerhetsnivå og all aktivitet loggføres.
- Personer med hemmelig adresse blir automatisk reservert fra kjernejournal.
- Sikkerheten overvåkes kontinuerlig og sikkerhetsbrudd blir anmeldt.

Løsningsskisse