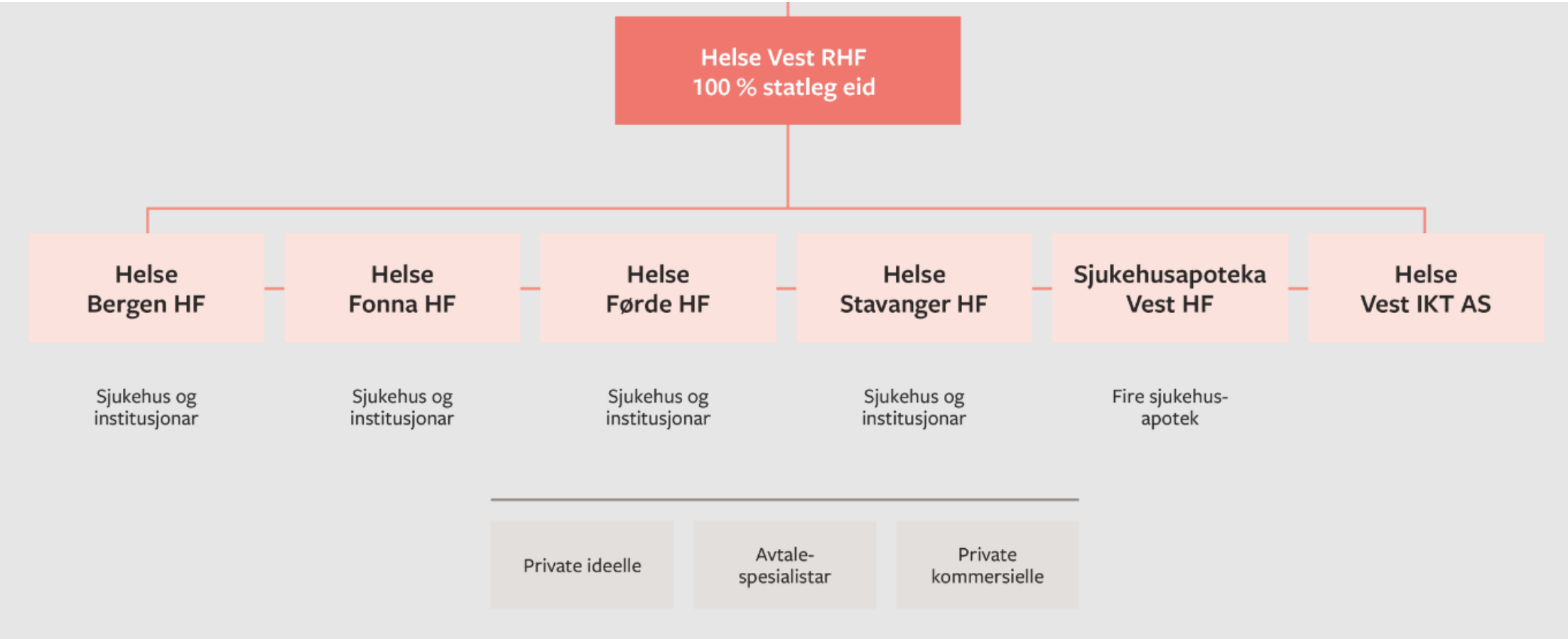
HELSE VEST IKT

Vil du være forsøkskanin?

Testdata og personvern
Sikkerhetsfestivalen 29.08

Elisabeth Meling – Testmiljøforvaltning
Randi Gjerde – Informasjonssikkerhet

Helse Vest IKT



Tema for presentasjonen

- Er snoking greit så lenge det er test?
- Er det greit å «behandle» svigermor for gonoré i testmiljøet dersom du har en god grunn?

- **Hvilke krav stilles ved bruk av reelle data til testformål?**
- **Hvilke andre strategier finnes?**

Vil du låne ut journalen din for testing?

Hva sier loven?

Behandlingen er bare lovlig dersom ...

Behandling? Pasientbehandling da eller?

- **Behandling**:
- Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks.
    - innsamling
    - registrering
    - organisering
    - strukturering
    - lagring
    - tilpasning
    - eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring,

Behandling av personopplysninger er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt:

- Samtykke (ex. Kundeklubb)
- Avtaleoppfyllelse (ex. Ansatt)
- Rettslig forpliktelse (ex. Journal)
- Vitale interesser (Liv eller død!)
- Allmennhetens interesse eller offentlig myndighet/pålegg (ex. FHI)
- Berettiget interesse (AI?)

1.

Behandling av personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, ***er forbudt****.*

Nr. 1 får ikke anvendelse dersom et av følgende vilkår er oppfylt...

- **Den registrerte har gitt uttrykkelig samtykke til behandling av slike personopplysninger for ett eller flere spesifikke formål, unntatt dersom det i unionsretten eller medlemsstatenes nasjonale rett er fastsatt at den registrerte ikke kan oppheve forbudet nevnt i nr. 1.**
- **Behandlingen er nødvendig for at den behandlingsansvarlige eller den registrerte skal kunne oppfylle sine forpliktelser og utøve sine særlige rettigheter på området arbeidsrett, trygderett og sosialrett i den grad dette er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett, eller en tariffavtale i henhold til medlemsstatenes nasjonale rett som gir nødvendige garantier for den registrertes grunnleggende rettigheter og interesser.**
- **Behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser dersom den registrerte fysisk eller juridisk ikke er i stand til å gi samtykke.**
- **Behandlingen utføres av en stiftelse, sammenslutning eller et annet ideelt organ hvis mål er av politisk, religiøs eller fagforeningsmessig art, som ledd i organets berettigede aktiviteter og med nødvendige garantier, forutsatt at behandlingen bare gjelder organets medlemmer eller tidligere medlemmer eller personer som på grunn av organets mål har regelmessig kontakt med det, og at personopplysningene ikke utleveres til andre enn nevnte organ uten de registrertes samtykke.**
- **Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte har offentliggjort.**
- **Behandlingen er nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav eller når domstolene handler innenfor rammen av sin domsmyndighet.**
- **Behandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser.**
- **Behandlingen er nødvendig i forbindelse med forebyggende medisin eller arbeidsmedisin for å vurdere en arbeidstakers arbeidskapasitet, i forbindelse med medisinsk diagnostikk, yting av helse- eller sosialtjenester, behandling eller forvaltning av helse- eller sosialtjenester og -systemer på grunnlag av unionsretten eller medlemsstatenes nasjonale rett eller i henhold til en avtale med helsepersonell og med forbehold for vilkårene og garantiene nevnt i nr. 3.**
- **Behandlingen er nødvendig av allmenne folkehelsehensyn, f.eks. vern mot alvorlige grenseoverskridende helsetrusler eller for å sikre høye kvalitets- og sikkerhetsstandarder for helsetjenester og legemidler eller medisinsk utstyr, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett der det fastsettes egnede og særlige tiltak for å verne den registrertes rettigheter og friheter, særlig taushetsplikt.**
- **Behandlingen er nødvendig for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1 på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser.**

F.eks. EPJ

- Vi er LOVPÅLAGT å journalføre. Dermed må vi behandle personopplysninger, inkludert helseopplysninger.

- Kan vi overføre dette direkte til testformål?

Med prodlike data må man ha prodlike tiltak…

- Forankring hos dataansvarlig (behandlingsansvarlig)
- Ivaretakelse av taushetsplikt
- Innsyn
- Retting
- Sletting
- Innsyn i logger
- Trekke samtykke

Men hvordan kan jeg slippe å tenke på lovhjemler?

Forskjellige strategier

- Reelle data i test
- Maskering / pseudonymisering
- Anonymisering
- Syntetiske data

Maskering / pseudonymisering

- Kopi av reelle personopplysninger
- Unike identifikatorer erstattes
- Kan re-identifiseres
- Kan kreve personverntiltak, f.eks. logging

Anonymisering

- Kopi av reelle personopplysninger
- Unike identifikatorer erstattes
- Identifiserende attributter erstattes og grupperes
- Reidentifiserende nøkler slettes
- Kan ikke reidentifiseres

→ Personvernforordningen gjelder ikke!

Syntetiske data

Helt fiktive data opprettet for testformål, og er helt fristilt fra produksjonsdata.

Normen / Faktaark 43

eHelse har kommet med ny versjon av Normens Faktaark 43 – «Bruk av testdata i systemer som inneholder helse- og personopplysninger»

- Fokus på syntetiske testdata økes
- Fokus på sikkerhet, logging og personvernrettigheter økes

normen.no

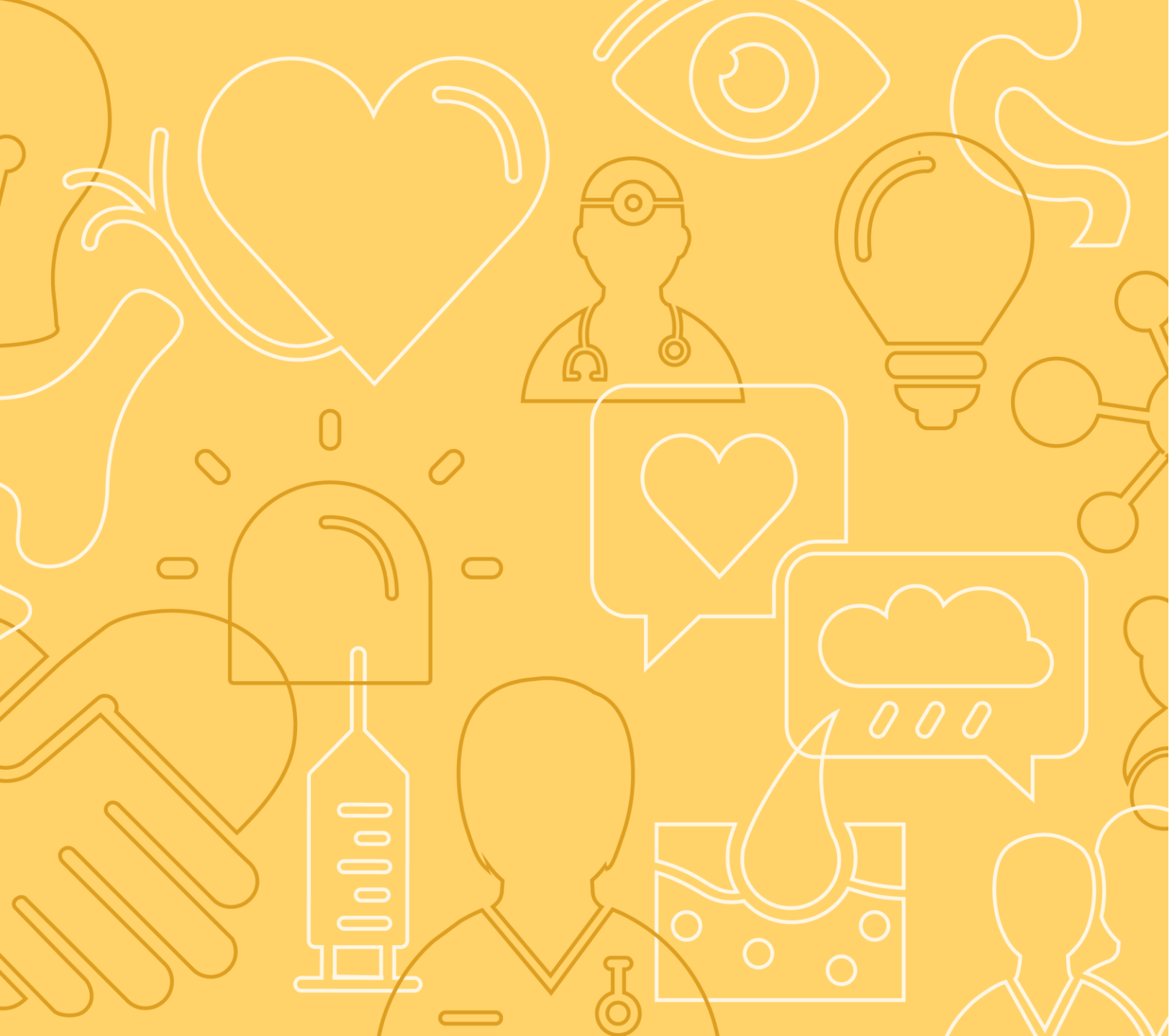
Modernisert folkeregister / persontjenesten

- Folkeregisteret har etablert nytt syntetisk folkeregister for test: Modernisert Folkeregister.
- Syntetiske personnummer med egen syntaks og fiktive hendelser (har +80 og +65 i månedsnummer).
- Skatt tilbyr i dag Tenor som søke-/uttrekksløsning fra Syntetiske folkeregister.
- Krav om å bruke syntetiske personer for testing på tvers.
- Persontjenesten (NHN) bruker syntetisk folkeregister som datagrunnlag i sine nye testmiljø.

Fremover

- Kvaliteten på syntetiske data blir så høy at det ikke vil være produktivt å benytte relle persondata!
- Leverandør har også ansvar for å ivareta personopplysningssikkerhet!
  - Vi (kundene) må stille krav!
- Ola og Kari Nordmann blir stadig mer oppmerksomme på sine rettigheter og risiko for at persondata kan bli eksponert.

Personvern og beskyttelse av sensitive data er viktig for alle!!



HELSE VEST IKT

Takk for oss!

Spørsmål?

randi.gjerde@helse-vest-ikt.no

elisabeth.meling@helse-vest-ikt.no