UiO : Universitetet i Oslo

GDPR-ready datainnsamling av sensitive data til forskning

Dagfinn Bergsager
Leder for (web og) mobilapputvikling

Kort oppsummering

Forskere tilknyttet UiT har samme muligheter som forskere på UiO og andre som har avtale om bruk av UiOs forskningstjenester.

Ved bruk av Nettskjema og TSD er store deler av GDPR allerede tilfredstillt. Mange forskere har fått til mye ved bruk av våre løsninger!

For å ta i bruk TSD, Google «TSD» og klikk deg videre:)

Titan.uio.no
...ny kunnskap hver dag!

Denne USIT-gjengen utvikler apper til forskere: Fra venstre Paul Philip Mitchell, Mikael Olausson, Ida Krüger, Dagfinn Bergsager, Martine Eklund, Pål Fugelli, Kien Vu og Espen Adrian Jones. Foto: Gunhild M. Haugnes/UiO Bruk bildet.

De utvikler apper som gjør forskningen bedre

Målgruppen er forskere som har behov for å samle inn sensitive persondata. Dette kan være første steg på veien mot at hver og en kan overvåke sin egen helse på en app – på en sikker måte.

av Gunhild M. Haugnes – 30. april, 2018

– Vårt app-miljø er unikt i Skandinavia, kanskje i også i verden, mener prosjektlederne Dagfinn Bergsager og Pål Fugelli fra USIT (Universitetets senter for informasjonsteknologi).

Som den eneste aktøren er USIT-gruppen sertifisert av TSD (Tjenester for Sensitive Data til å kunne utvikle apper hvor svært sensitive persondata er involvert – som blant annet helseopplysninger.

Lowcost: En færdig app til forskere koster her 150.000 kroner

Portræt: norsk udviklergruppe udvikler apps, som hjælper med at gøre forskning bedre.

Gunhild M. Haugness / titan.iou.no / digi.no Torsdag, 3. maj 2018 - 11:20 1

FØLG

»Vores app-miljø er unikt i Skandinavien, måske også i verden,« mener projektlederne Dagfinn Bergsager og Pål Fugelli fra det norske Universitetets senter for informasjonsteknologi (USIT).

Som den eneste aktør er USIT-gruppen certificeret af norske Tjenester for Sensitive Data (TSD) t at kunne udvikle apps, hvor meget sensitive persondata er involveret – blandt andet sundhedsoplysninger.

TSD giver forskere en platform, som opfylder lovens strenge krav til behandling og lagring af sensitive forskningsdata.

Design

Vi lager moderne mobilapper og legger det oppå eksisterende infrastruktur for forskning med Nettskjema og TSD.

(slik som Vipps ligger oppå UNIX)

Hvordan klarer vi å utvikle mobilapper som samler inn sensitive personopplysninger?

-fordi vi har innebygd personvern!

…overalt

Prioriteringer for all utvikling

1. **Sikkerhet og personvern**
2. **Bruksopplevelse for den som skal levere data**
3. **Funksjonalitet for den som samler inn data**

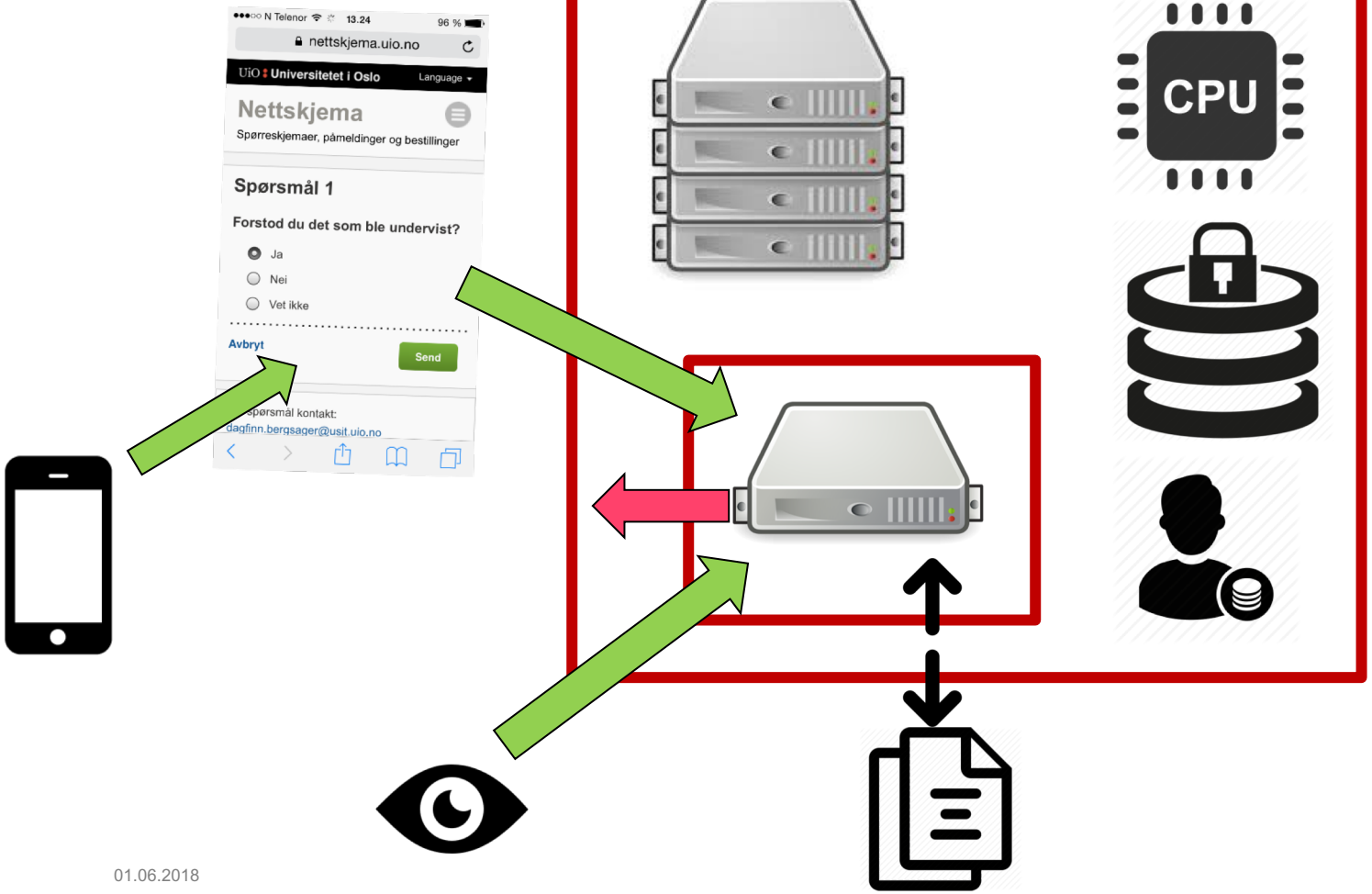
-Vi skal alltid være best på sikkerhet og personvern!

-og fungere på alt utstyr for alle personer

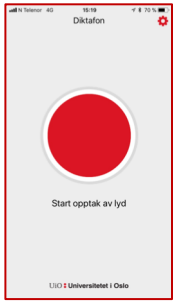
-og være enkel og bruke for datainnsamler

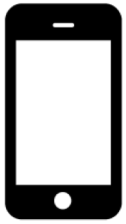
Nettskjema

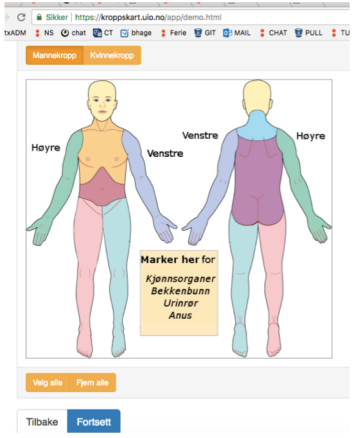
- Datainnsamling på nett
- Sektortjeneste for UH
- Stor bruk fra FHI og OUS
- Mottar 2000 – 20 000 svar per dag
- Mobilapper og webapper kan levere data via Nettskjema
- UiO utvikler og drifter
- Kan samle inn sensitive personopplysninger

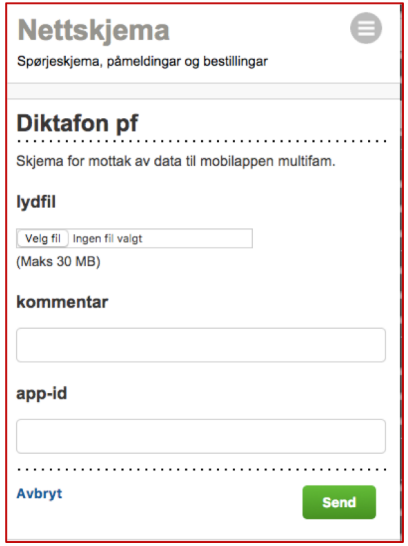

N Telenor 13.24 96 %
nettskjema.uio.no
UiO : Universitetet i Oslo
Language
Nettskjema
Spørreskjemaer, påmeldinger og bestillinger
Spørsmål 1
Forstod du det som ble undervist?
Ja
Nei
Vet ikke
Avbryt
Send
Spørsmål kontakt:
dagfinn.bergsager@usit.uio.no
CPU

- Nettskjema mottar daglig mellom 2000 og 10 000 svar
- Spesialisert for forskning og studieadministrasjon
- Nasjonal tjeneste fra UiO
- Høy sikkerhet med mye krypto…









Nettskjema vs QuestBack /GoogleForms

- UiT har fri bruk av Nettskjema
- Nettskjema alt på plass av innebygd personvern
  - Fra logging til ledetekster i skjema
- Nettskjema kan levere sensitive data til TSD
- Løsningen trenger ikke egen Risikovurdering (ROS)
- UiO/USIT garanterer for sikkerhet og oppetid

Nettskjema 2018

- Nytt design for de som svarer
  - Flere funksjoner
  - Enda mer universelt uformet
- Leverer data direkte til TSD uten forsinkelse
- Flytter til nettskjema.no
- Forventer dobling i bruk
- Bedre løsninger mot Uninett /FEIDE

Mobilapper i forskning

- Har utviklet omlag 20 apper for forskningsprosjekter
- Nettskjema /TSD er backend for alle apper
- Alle prosjekter får ROS (eks.)med fokus på hvilke data som ligger igjen på telefonen.

Nettskjema i finalen

5. mars vart pris for beste innebygde personvern delt ut av Datatilsynet. Blant dei tre finalistane var Nettskjema.

Finalistane på rekke og rad. Nummer to frå venstre er USIT sin Dagfinn Bergsager. Foto: Veronica Jarnskjold Buer/Datatilsynet

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Artikkel 25

Innebygd personvern og personvern som standardinnstilling

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører, skal den behandlingsansvarlige, både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen, gjennomføre egnede tekniske og organisatoriske tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.

2. Den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål med behandlingen, som behandles. Nevnte forpliktelse får anvendelse på den mengden personopplysninger som samles inn, omfanget av behandlingen av opplysningene, hvor lenge de lagres og deres tilgjengelighet. Nevnte tiltak skal særlig sikre at personopplysninger som standard ikke gjøres tilgjengelige for et ubegrenset antall fysiske personer uten den berørte personens medvirkning.

3. En godkjent sertifiseringsmekanisme i henhold til artikkel 42 kan brukes som en faktor for å påvise at kravene fastsatt i nr. 1 og 2 i denne artikkel overholdes.

risiki

Artikkel 5

Prinsipper for behandling av personopplysninger

1. Personopplysninger skal

a) behandles på en lovlig, rettferdig og gjennomsiktig måte med hensyn til den registrerte («lovlighet, rettferdighet og gjennomsiktighet»),

b) samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene; viderebehandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal i samsvar med artikkel 89 nr. 1 ikke anses som uforenlige med de opprinnelige formålene («formålsbegrensning»),

c) være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»),

d) være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller korrigeres («riktighet»),

e) lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for; personopplysninger kan lagres i lengre perioder dersom de utelukkende vil bli behandlet for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1, forutsatt at det gjennomføres egnede tekniske og organisatoriske tiltak som kreves i henhold til denne forordning for å sikre de registrertes rettigheter og friheter («lagringsbegrensning»),

f) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og fortrolighet»).

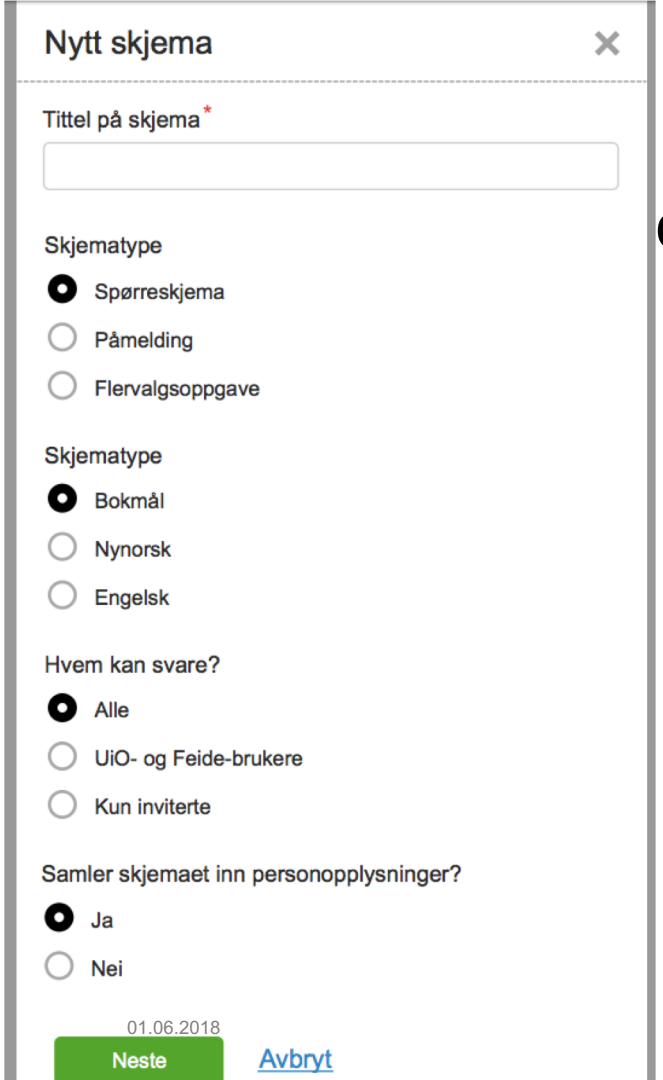
2. Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes («ansvar»).

«Lovlighet, rettferdighet og gjennomsiktighet»
(lawfulness, fairness and transparency)

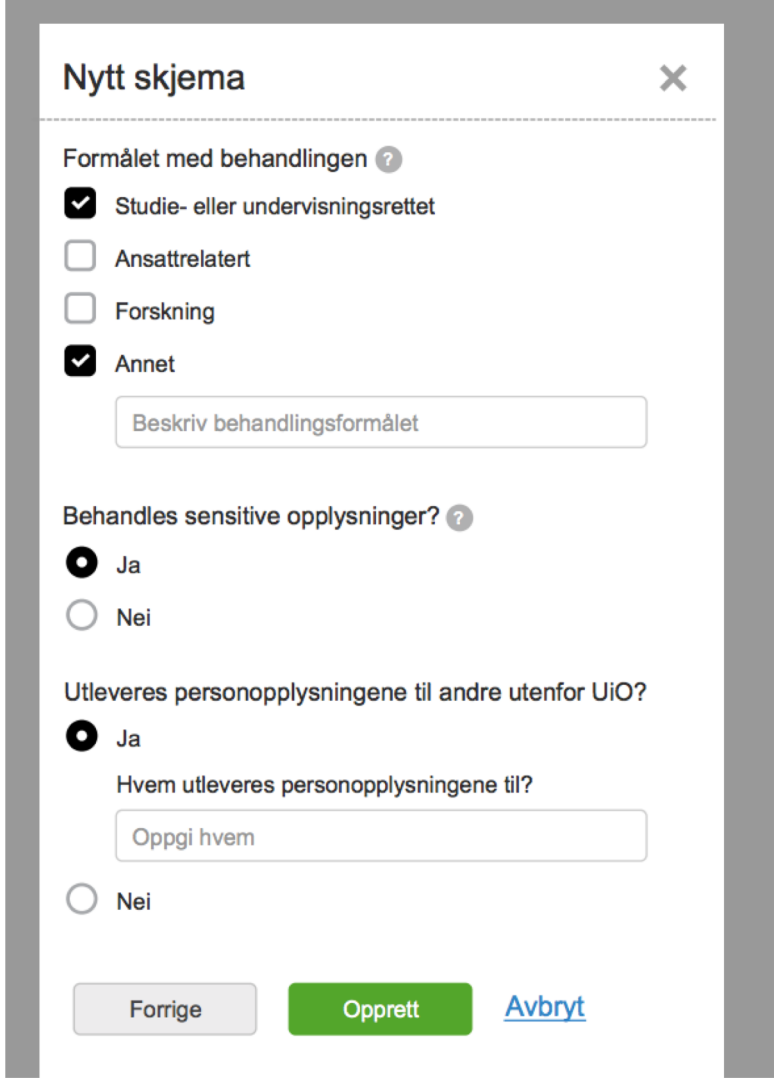
- Kan bli (og blir) sett i kortene på alle ledd i dataflyten
- Åpen kildekode og sikkerhetsdokumentasjon
- Jevnlig dialog med Datatilsynet, Personvernombud som OUSPVO, REK, NSD
- ROS-analyser for alle prosjekter og systemer som bruker vår løsning

«Formålsbegrensning» (‘purpose limitation’)

- Forskere er obs på dette; vil tilrettelegger for dem
  - Alle med rette godkjenninger får egen sikker server
  - Lett å hente inn men vanskelig å få data ut av serveren
- Overvåker at andre som samler inn holder seg til formålet

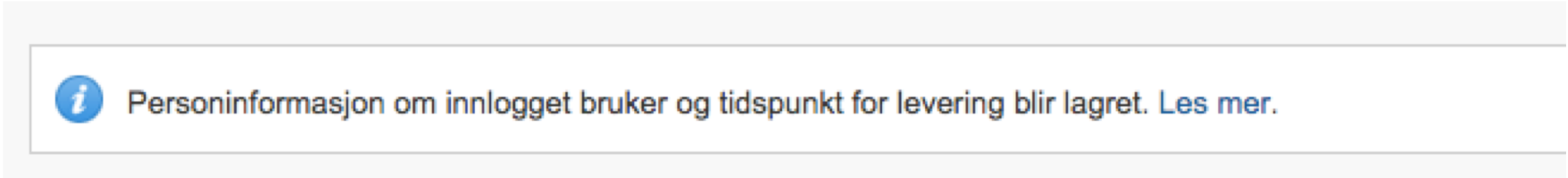

Nytt skjema
Tittel på skjema *
Skjematype
Spørreskjema
Påmelding
Flervalgsoppgave
Skjematype
Bokmål
Nynorsk
Engelsk
Hvem kan svare?
Alle
UiO- og Feide-brukere
Kun inviterte
Samler skjemaet inn personopplysninger?
Ja
Nei
01.06.2018
Neste
Avbryt

demo


Nytt skjema
Formålet med behandlingen
Studie- eller undervisningsrettet
Ansattrelatert
Forskning
Annet
Beskriv behandlingsformålet
Behandles sensitive opplysninger?
Ja
Nei
Utleveres personopplysningene til andre utenfor UiO?
Ja
Hvem utleveres personopplysningene til?
Oppgi hvem
Nei
Forrige
Opprett
Avbryt

Skanner jevnlig data utenfor TSD

- Markerer alle skjema som samler inn personinformasjon
- Fjerner automatisk persondata som vi vurderer som lite relevante
- Varsler bruker om hvilke personopplysninger som blir lagret



«Dataminimering»
(‘data minimisation’)

- Minimalt logges og slettes etter 3 mnd
  - Egne verktøy for å se trender
- Krever at skjemaeier registrerer ekstra info om de skal samle inn personopplysninger
- Oversikt over skjema som samler personinfo gjennomgås med ansvarlig enhet årlig

«Riktighet»
(‘accuracy’)

- Kun lenker til personkatalog –ikke import av kontaktinfo
- Grunndata om personer hentes fra SAP eller FS
  Forskningsprosjekter kan bruke IDporten
  - Forskjellige nivå
  - Løsning for digitalt signerte sensitive dokumenter
- Tydelig for bruker hvilke data som lagres
  - Må ha en ID til respondent for å kunne fjerne data…

«Lagringsbegrensning» (‘storage limitation’)

- Nøye gjennomgang av hva som lagres på telefonen
- Vi merker skjema som samler inn persondata
  - Avansert algoritme fjerner persondata automatisk når vi vurderer innsamlingen som irrelevant
- Forskningsprosjekter må sette sluttdato for server i TSD og plan for sletting av data

Nye utfordringer med mobilapper

- Mobilappen må lagre noe data
  - Når du leverte data sist
  - ID på hvem som har levert svaret
  - Ev. noe tilbakemelding på trend
- At du har installert appen kan kobles til at du har en diagnose
- Dersom appen mister nett, legges data i kryptert kø
- Data på mobiler blir ofte sikkerhetskopiert til Apple/Google

MittBlikk

View More by This Develope

By Universitetet i Oslo

This app is only available on the App Store for iOS devices.

This app is designed for both iPhone and iPad

Free

Category: Lifestyle
Updated: 20 June 2017
Version: 1.0.2
Size: 20.5 MB

Description

Dette er en mobilapp for innsamling av data til et forskningsprosjekt ved Universitetet i Oslo. For å bruke appen må ha fått utdelt en studieID av forsker.

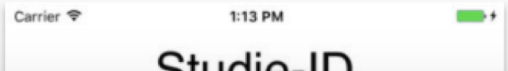
Universitetet i Oslo Web Site ▸ MittBlikk Support ▸

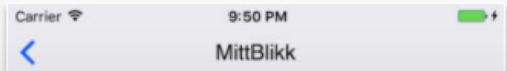
What's New in Version 1.0.2

Bugfiks og mindre designjusteringer

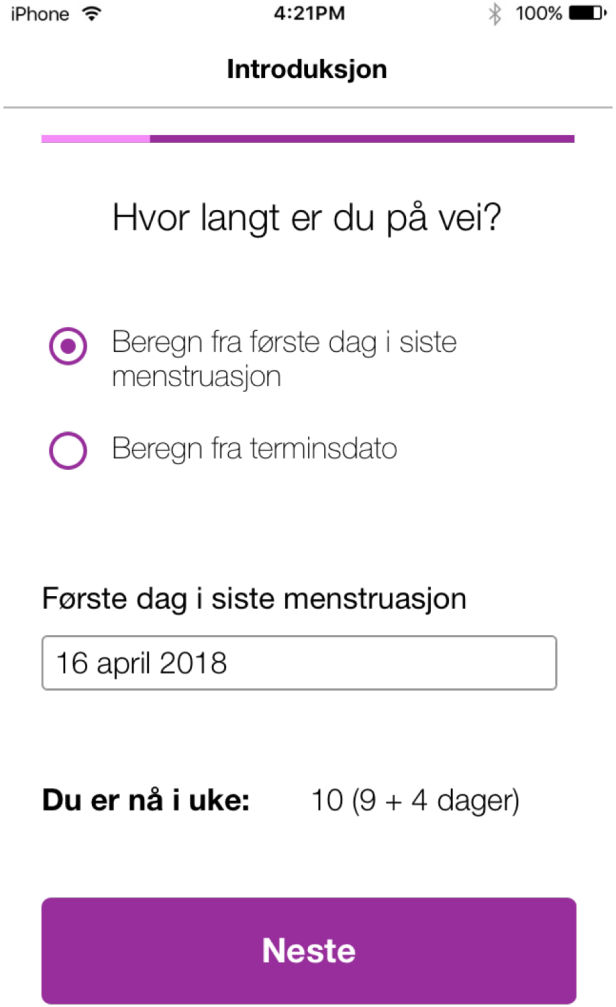
Screenshots

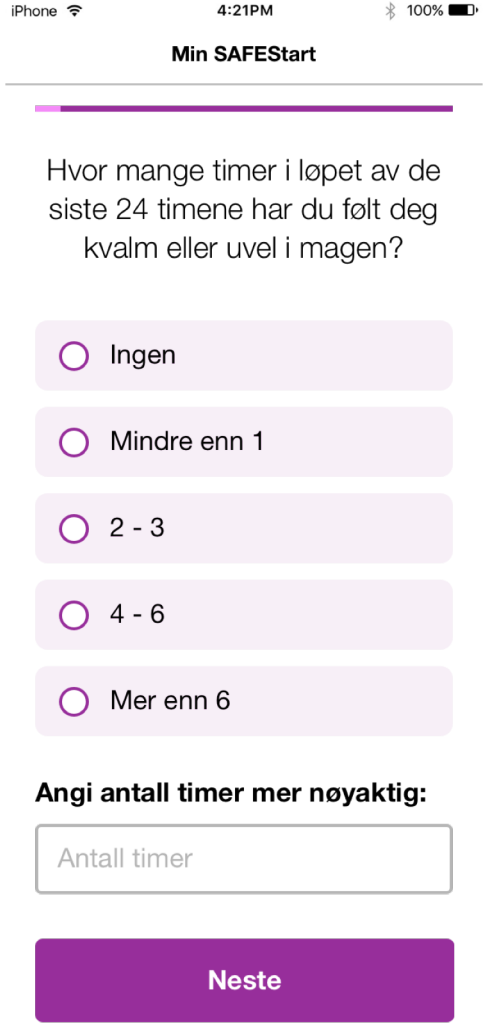
iPhone | iPad

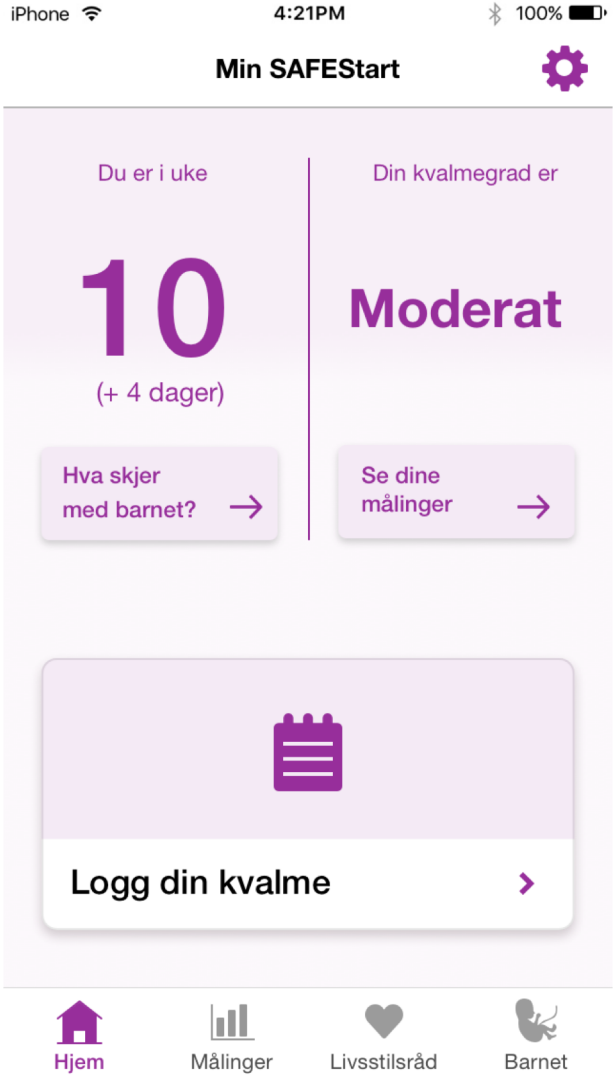


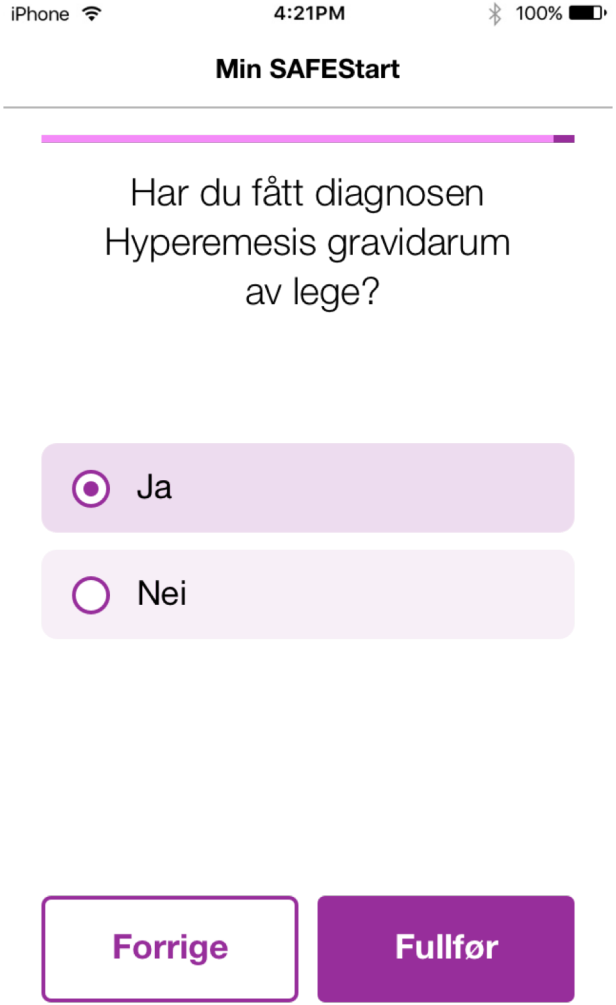



iPhone
4:21PM
100%
Min SAFEStart
SAFE start
Velkommen!
Dette er en app til deg som er gravid og ønsker å loggføre og få en oversikten over dine kvalmesymptomer i svangerskapet.
Appen er en del av en studie på UiO der man forsker på svangerskaps-kvalme hos gravide.
Neste
UiO : Universitetet i Oslo

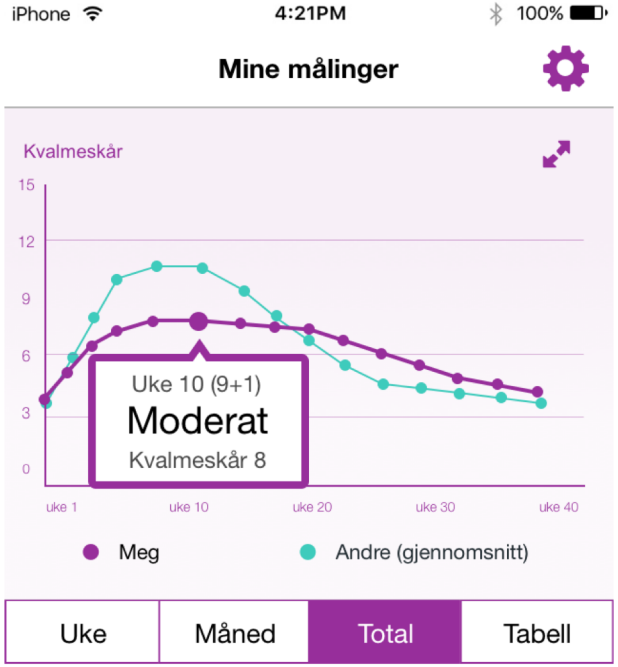

iPhone
4:21PM
100%
Introduksjon
Hvor langt er du på vei?
Beregn fra første dag i siste menstruasjon
Beregn fra terminsdato
Første dag i siste menstruasjon
16 april 2018
Du er nå i uke: 10 (9 + 4 dager)
Neste


iPhone
4:21PM
100%
Min SAFEStart
Hvor mange timer i løpet av de siste 24 timene har du følt deg kvalm eller uvel i magen?
Ingen
Mindre enn 1
2 - 3
4 - 6
Mer enn 6
Angi antall timer mer nøyaktig:
Antall timer
Neste


iPhone
4:21PM
100%
Min SAFEStart
Du er i uke
10
(+ 4 dager)
Din kvalmegrad er
Moderat
Hva skjer med barnet?
Se dine målinger
Logg din kvalme
Hjem
Målinger
Livsstilsråd
Barnet


iPhone
4:21PM
100%
Min SAFEStart
Har du fått diagnosen Hyperemesis gravidarum av lege?
Ja
Nei
Forrige
Fullfør


iPhone
4:21PM
100%
Min SAFEStart
Din kvalme
Basert på målingene dine har du hatt kvalmeskår på 13 eller over, 1 uke i strekk. Dette regnes som Alvorlig svangerskaps-kvalme.
Vi anbefaller at du oppsøker legen din.
OK


iPhone
4:21PM
100%
Mine målinger
Kvalmeskår
15
12
9
6
3
0
Uke 10 (9+1)
Moderat
Kvalmeskår 8
uke 1
uke 10
uke 20
uke 30
uke 40
Meg
Andre (gjennomsnitt)
Uke
Måned
Total
Tabell
Grafen baseres på dine målinger.
Kvalmegraden indikerer hvor alvorlig din situasjon er.
Mild (Skår 3 - 6)
Moderat (Skår 7-12)
Alvorlig (Skår 13 - 15)
Hjem
Målinger
Kvalmeråd
Barnet

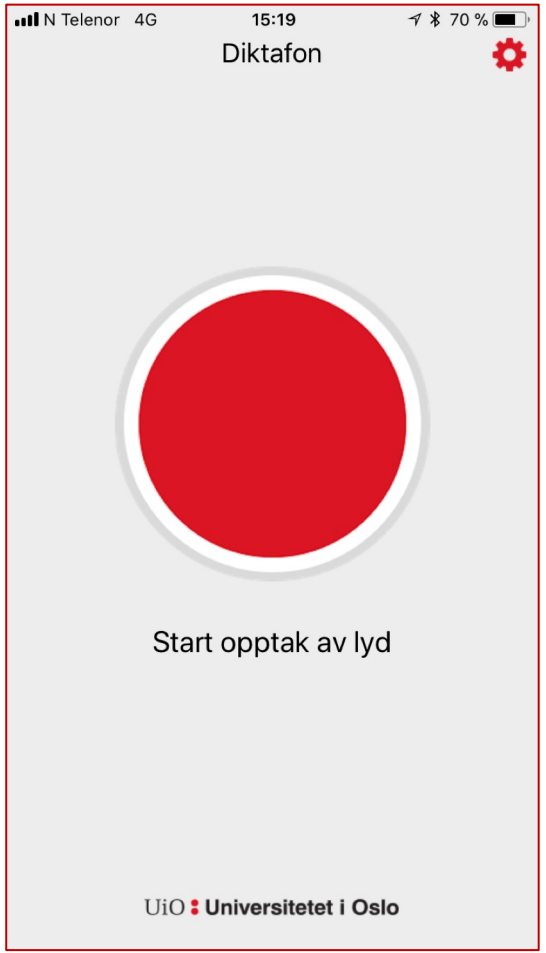
Brukerne elsker premier…

Status apper

- Vi klarer å lage apper raskt og billig
  - Fra 200k per app
- Standard malverk og regler for hvordan vi lager dem
- Om vi skal gå god for sikkerheten må vi lage appen
- Miljøer med egne utviklere lager apper som leverer til oss
- Har driftsavtaler for apper som skal leve lengre enn 1 år
  - Garanterer at de fungerer på nye telefon-versjoner

Diktafon-app

- Generell app for opptak av lyd
- Alle nettskjemabrukere kan bruke den
  - Spesialskjema med filopplasting
- Fungerer også uten nett
  - Kryptert kø
- Designet for opptak av sensitive data
  - Ikke mulig å høre på opptaket i appen
- uio.no/tjenester/it/applikasjoner/nettskjema/hjelp/tips-triks/diktafon.html



VideoApp

- Vi har utviklet app for NKVTS til opptak av video med sensitive personopplysninger
- Filmer terapauter i krisepsykiatri med iPads
- Krypterer filmen og legger den i kø
- Lastes direkte opp i TSD; designet for dårlig nett på ipad
- Forsker ser på filmen i TSD
- VI kan nålaste opp større data til TSD uten TSD-bruker
- Ikke generelle løsning enda…

Mytsd.uio.no med appen MinMat

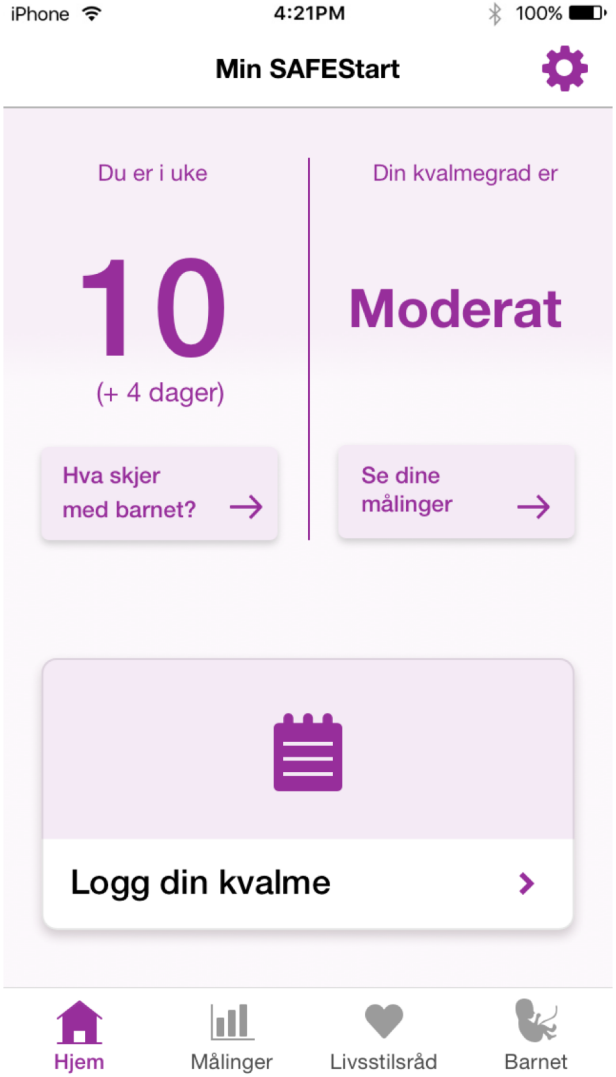
- Lene Frost Andersens prosjekt for underernæring er ferdig utviklet og pilotert
- Full prod på avd for blodsykdommer v/Riksen i aug
- Pasienter logger hva de spiser på iPad
- Får tilbakemelding i app om de har nådd dagens mål
- Rapport av data lagres i TSD
- Sykepleier logger inn (ID-porten nivå 4) og får rapport av alt de har spist og forslag til tiltak

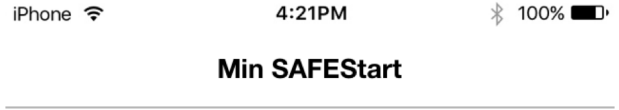
Mytsd.uio.no fremover

- Prosjektet MinMat skal nøye evalueres før løsning brukes klinisk på flere prosjekter
- Vurderer prosjekter som ønsker å gi data tilbake til respondenter
  - Eks. prosesserte biodata

Vi lagrer mer data i appen

- Enklere (sikrere) å lagre litt data i appen enn å hente data ut fra TSD
- Flere prosjekter har fått løsning for tilbakemeldinger i appen
- Lagrer noen datapunkter å hardkoder et gjennomsnitt
  - Forsker definere gjennomsnitt i pilot
  - Ny versjon av app må ut om snittet skal endres
- Gir alarmer i app når bruker registrer data som overstiger terskelverdier
  - Får eks. beskjed om å ta kontakt med behandler /legevakt


iPhone
4:21PM
100%
Min SAFEStart
Du er i uke
10
(+ 4 dager)
Din kvalmegrad er
Moderat
Hva skjer med barnet?
Se dine målinger
Logg din kvalme
Hjem
Målinger
Livsstilsråd
Barnet

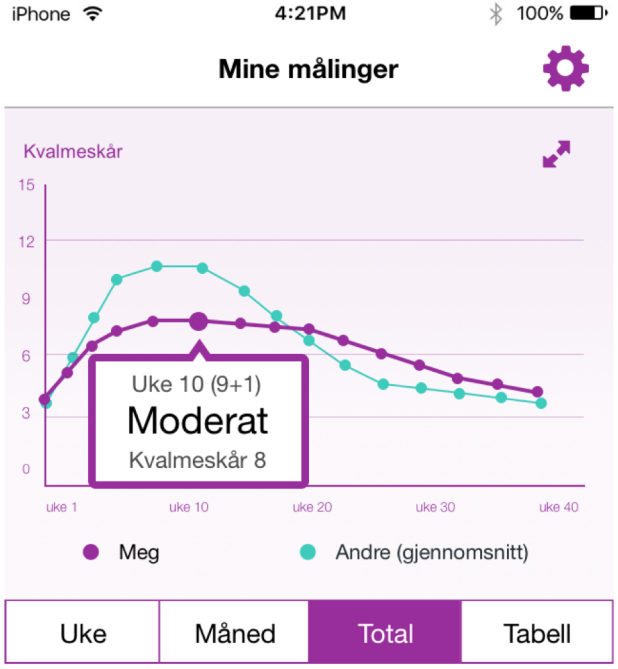


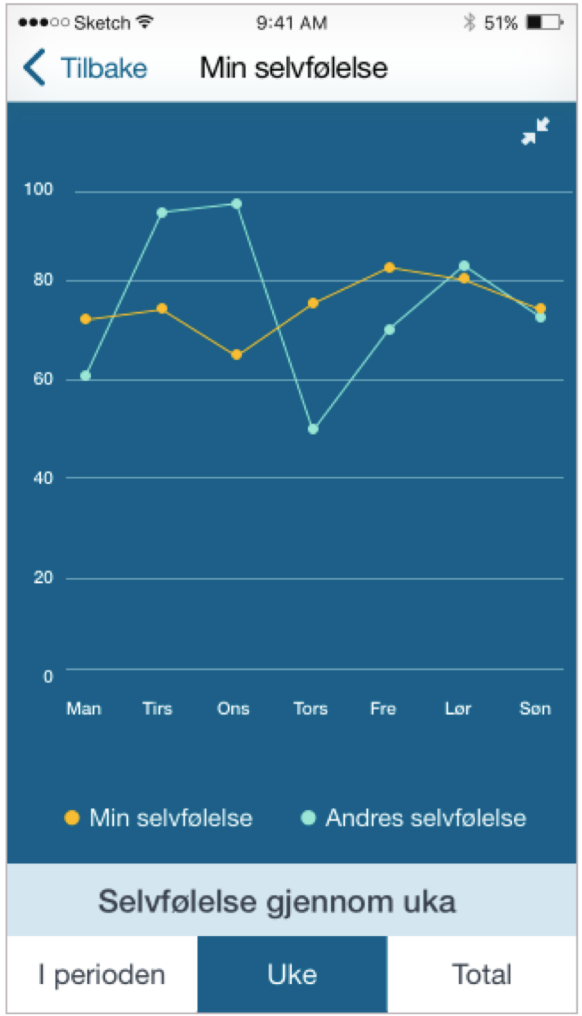
Din kvalme

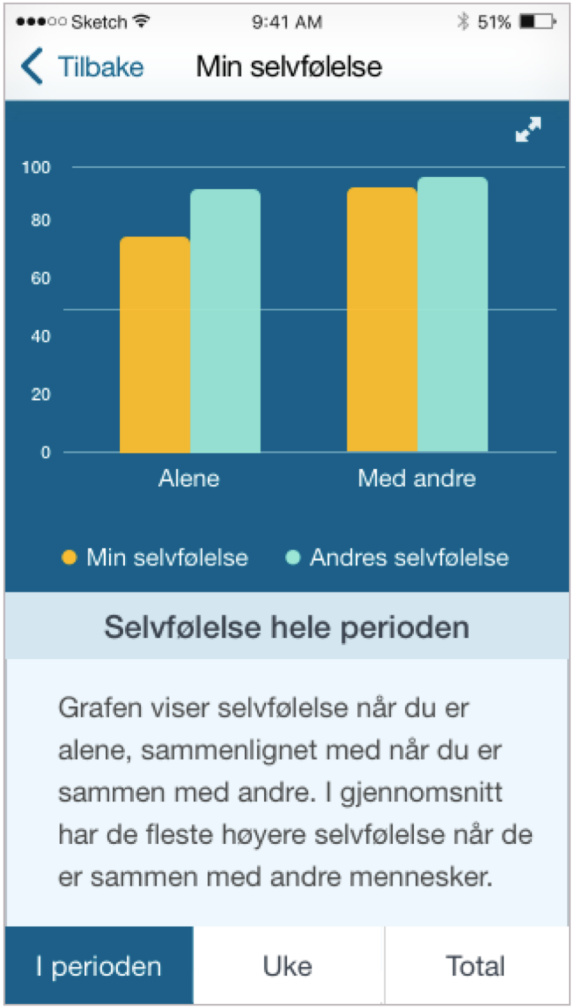
Basert på målingene dine har du hatt kvalmeskår på **13** eller over, 1 uke i strekk. Dette regnes som **Alvorlig** svangerskaps-kvalme.

Vi anbefaller at du oppsøker legen din.

OK

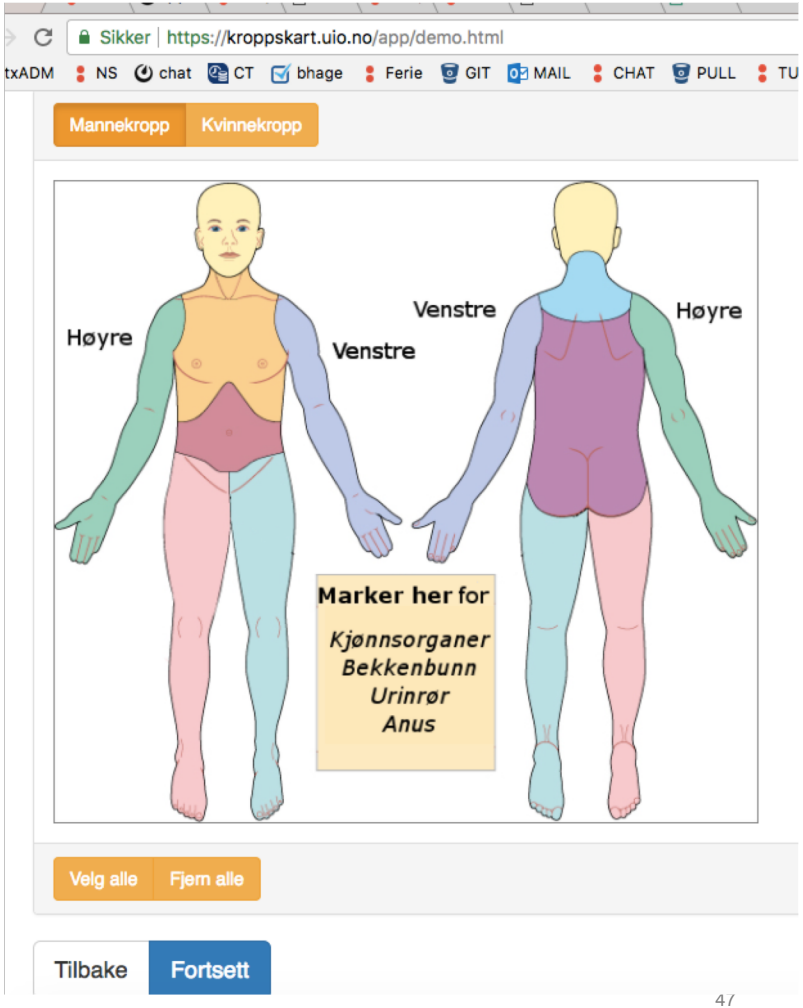

iPhone
4:21PM
100%
Mine målinger
Kvalmeskår
15
12
9
6
3
0
Uke 10 (9+1)
Moderat
Kvalmeskår 8
uke 1
uke 10
uke 20
uke 30
uke 40
Meg
Andre (gjennomsnitt)
Uke
Måned
Total
Tabell
Grafen baseres på dine målinger.
Kvalmegraden indikerer hvor alvorlig din situasjon er.
Mild (Skår 3 - 6)
Moderat (Skår 7-12)
Alvorlig (Skår 13 - 15)
Hjem
Målinger
Kvalmeråd
Barnet


Sketch
9:41 AM
51%
Tilbake
Min selvfølelse
100
80
60
40
20
0
Man
Tirs
Ons
Tors
Fre
Lør
Søn
Min selvfølelse
Andres selvfølelse
Selvfølelse gjennom uka
I perioden
Uke
Total


Sketch
9:41 AM
51%
Tilbake
Min selvfølelse
100
80
60
40
20
0
Alene
Med andre
Min selvfølelse
Andres selvfølelse
Selvfølelse hele perioden
Grafen viser selvfølelse når du er alene, sammenlignet med når du er sammen med andre. I gjennomsnitt har de fleste høyere selvfølelse når de er sammen med andre mennesker.
I perioden
Uke
Total

Egne webapper

- Kan nå levere data til TSD fra webapper også
- Smertekart utviklet for FHI
  - Sendt alle ungdommer i januar (Shoot2018)
- Samme arkitektur som mobilapper
  - Nettskjema → TSD



«Integritet og fortrolighet»
(‘integrity and confidentiality’)

- (Vanvitting) streng tilgangstyring til TSD
  - Eksportrettigheter revideres jevnlig
- Kun forsker har tilgang i TSD
  - Ikke IT-drift…
- Eks.: Påbegynte forskningsprosjekter får ikke endre skjema
  - Unngå juks
  - Dataintegritet
- Kun UiOs Apple /Google –konto legger ut apper

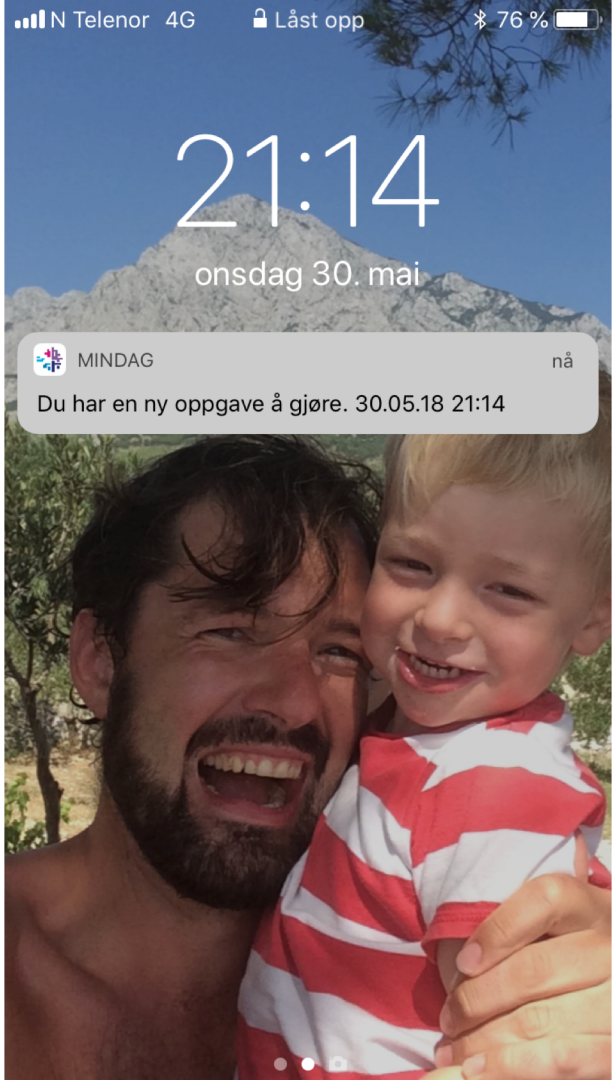
«Ansvar»
(‘accountability’)

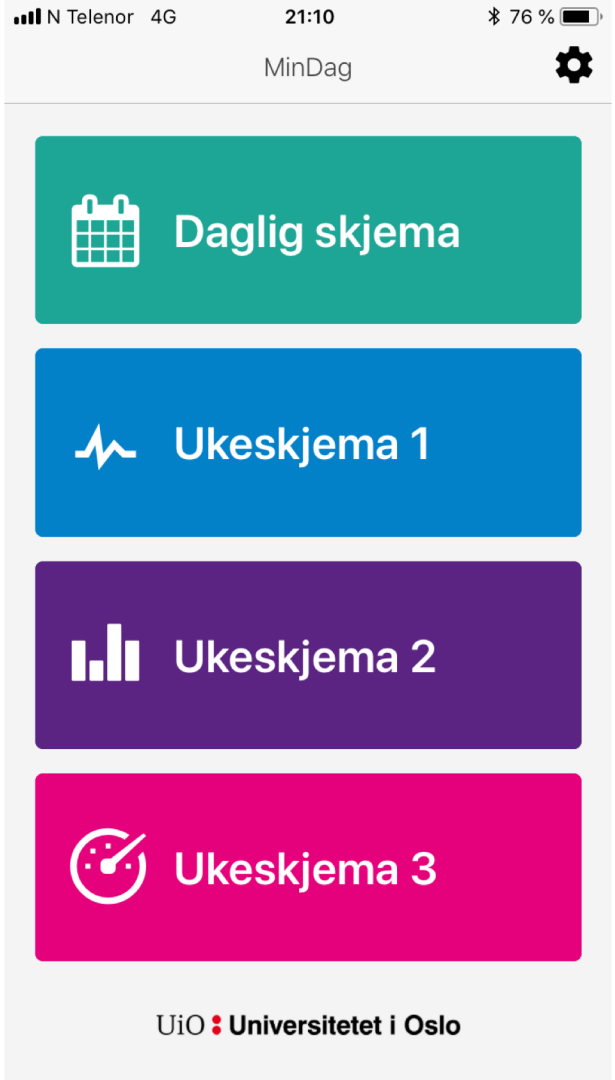
- Jevnlig varsling til de som samler inn data om de har skjema som bør ryddes /slettes
- Egne strenge krav til hva vi krever om vi skal ta et oppdrag
- Rutiner for avvikshåndtering – god erfaring!
- Hjelper forskere med å ROS for alle prosjekter
  - All data samles og lagres i samme løsning
  - Baserer ROS på eksisterende ROS
- Krever NSD/REK –godkjenning for alle prosjekter

Det viktigste er at alle i prosjektet forstår at innebygd personvern og innebygd sikkerhet er noe alle er ansvarlig for

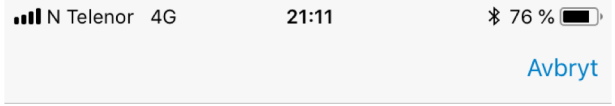
-det svakeste punktet…

demo


N Telenor 4G
Låst opp
76 %
21:14
onsdag 30. mai
MINDAG
nå
Du har en ny oppgave å gjøre. 30.05.18 21:14


N Telenor 4G
21:10
76 %
MinDag
Daglig skjema
Ukeskjema 1
Ukeskjema 2
Ukeskjema 3
UiO : Universitetet i Oslo


N Telenor 4G
21:10
76 %
Avbryt
Timer med søvn
Bruk hjulet nedenfor for å indikere omtrent hvor mange timer søvn du fikk i natt.
Når sovnet du?
-:-
Når våknet du?
-:-
Antall oppvåkninger
Ingen
Jeg sov ikke noe i natt
Neste



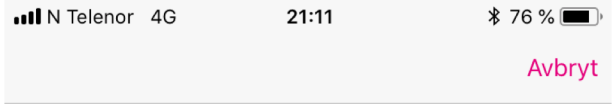
Hjelp

Den siste uken:

Jeg er mindre følsom for farger enn vanlig

Jeg er mer følsom for farger enn vanlig

Neste



Hjelp

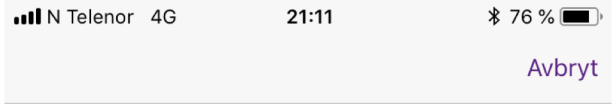
Jeg har hørt stemmer som andre ikke kan høre

Nei | Ja

Jeg har sett ting som andre ikke kan se

Nei | Ja

Neste



Har du brukt noen av disse rusmidlene siste uken?

- [ ] Hasj/marihuana
- [ ] Amfetamin/metamfetamin
- [ ] Ecstasy/MDMA/LSD
- [ ] Kokain
- [ ] Heroin
- [ ] GHB/GBL
- [ ] Anabole steroider