Nasjonalt senter for
e-helseforskning

Føderert læring

Normen-webinar: Kunstig intelligens, sikkerhet og personvern

Alexandra Makhlysheva, seniorrådgiver
Nasjonalt senter for e-helseforskning

Problemstilling

Mye helsedata ved helseinstitusjoner -> stort potensial til forbedring av helsetjenester, MEN tid- og ressurskrevende

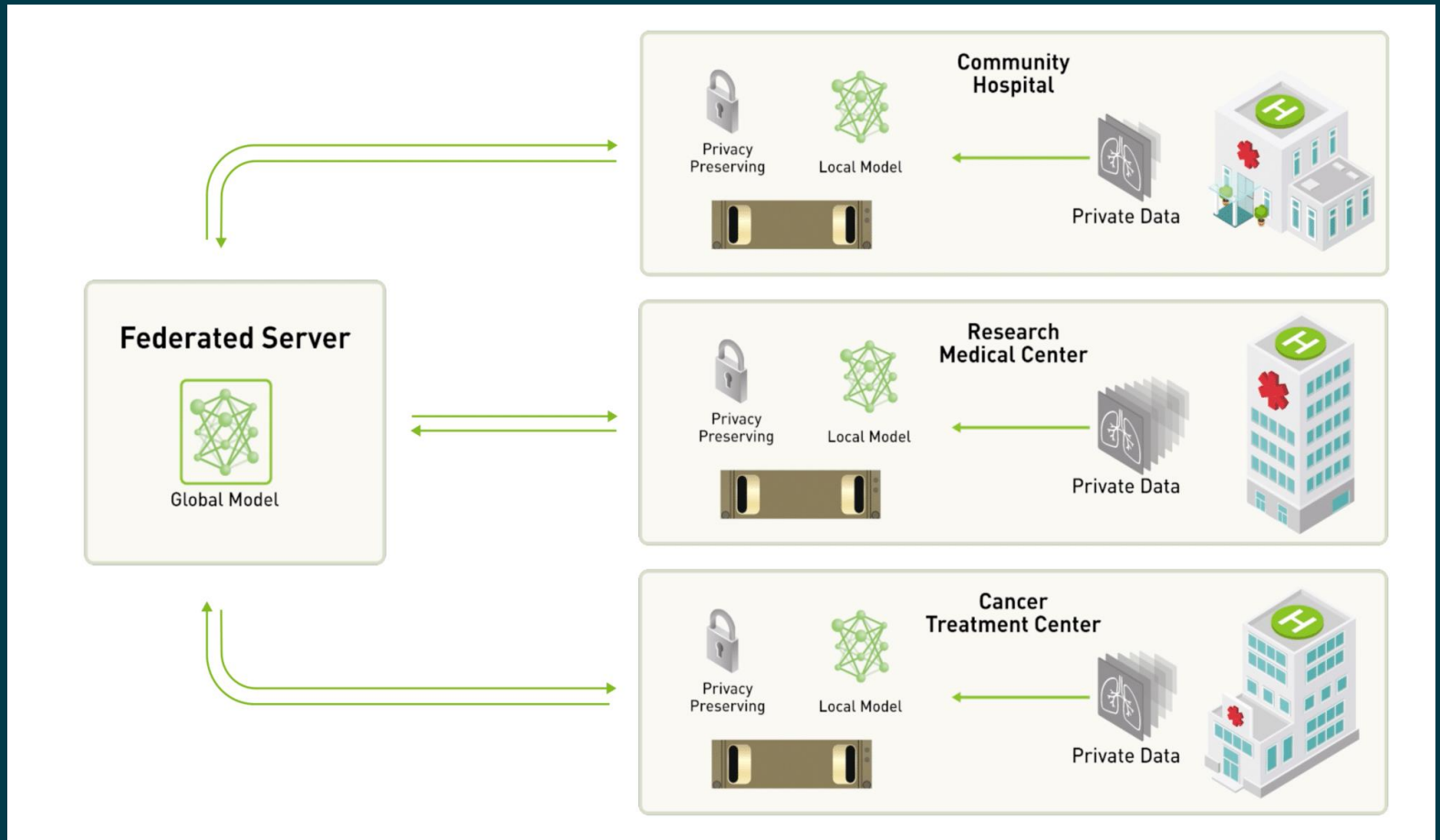
KI er til hjelps, den trenger mye data til trening/validering/testing

MEN helsedata er sensitive personopplysninger -> strengt regulert OG personvern og informasjonssikkerhet MÅ ivaretas

Føderert læring

- Personvernfremmende teknologi
- Gjør det mulig å analysere dataene der de ligger og unngå at de blir synlige for eller deles med eksterne aktører
- Et føderert konsortium for å trene en ML-modell uten å utveksle sensitive data med hverandre
- Ulike roller: delta i selve modelltreningen, validere ferdig trente modeller eller kun tilby enkle spørringer

FL-modelltreningsrunde

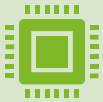


Fordeler

Ivaretatt personvern, bedre kontroll over data og redusert risiko for datainnbrudd

Større og mer representativt datagrunnlag –> bedre helsehjelp

Utfordringer



Variasjoner i tekniske parametere

Variasjoner i dataegenskaper

Kommunikasjonsflaskehalser

Ressursbruk

Potensielle sikkerhetstrusler

Potensielle angrep

- Forgiftningsangrep på data og modell
- Uttrekkingsangrep
- «Gratispassasjer»-angrep

Beskyttelsesmekanismer

Differensiert personvern	• Forgiftningsangrep • Uttrekkingsangrep
Sikker flerpartsberegning	• Uttrekkingsangrep
Oppdagelse av anomalier	• «Gratispassasjer»-angrep • Forgiftningsangrep
Robust aggregering	• Forgiftningsangrep • Uttrekkingsangrep
Kunnskapsdestillasjon	• Uttrekkingsangrep
Klarert utførelsesmiljø	• Forgiftningsangrep • Uttrekkingsangrep
Blokkjede	• Forgiftningsangrep • «Gratispassasjer»-angrep

Prosjekter med FL

Internasjonale prosjekter	Prosjekter med Norges deltakelse
AI4VBH	HealthData@EU
Samarbeid mellom Moorfields øyesykehus og Bitfount	FederatedHealth: A Nordic Federated Health Data Network
Bigpicture	Elixir
HealthChain	Samarbeid innen kreftforskning med Nederland
MELLODDY	FLORENCE
Federated Tumor Segmentation	Workflow-integrated machine learning
Trustworthy Federated Data Analytics	PraksisNett
OPTIMA	
Epiverse	

Oppsummering

- Flere fordeler vs flere problemstillinger å ta hensyn til
- Mange helserelaterte prosjekter som bruker FL med lovende resultater
- Behov for mer forskning, videreutvikling og praktiske erfaringer

Takk for meg!
Spørsmål?