
Syntetiske datasett kan gi bedre KI-modeller for helsetjenesten

KRONIKK

VIBEKE BINZ VALLEVIK

vibeke.binz@gmail.com

Vibeke Binz Vallevik er ph.d.-stipendiat ved Universitetet i Oslo og seniorforsker ved Group Research and Development Healthcare i DNV. Forfatteren har fylt ut ICMJE-skjemaet og oppgir ingen interessekonflikter.

ANNE KJERSTI C. BEFRING

Anne Kjersti C. Befring er jurist og professor ved Universitetet i Oslo. Hun er nestleder i Nordic Permed Law og i Den nasjonale forskningsetiske komité for medisin og helsefag. Forfatteren har fylt ut ICMJE-skjemaet og oppgir ingen interessekonflikter.

HELGA MARIA BERGEM BRØGGER

Helga Maria Bergem Brøgger er spesialist i radiologi og seniorforsker ved Group Research and Development Healthcare i DNV. Hun er medlem av Legeforeningens utvalg for forskning, kvalitetsforbedring og innovasjon og av ekspertgruppen i Nordic Innovation (under Nordisk ministerråd). Hun er styremedlem i Norsk radiologisk forening og medlem i Norsk råd for digital etikk. Forfatteren har fylt ut ICMJE-skjemaet og oppgir ingen interessekonflikter.

COURTNEY NADEAU

Courtney Nadeau er seniorforsker ved Group Research and Development Healthcare i DNV. Forfatteren har fylt ut ICMJE-skjemaet og oppgir ingen interessekonflikter.

Å lage syntetiske pasientdata reduserer risikoen for personvernbrudd når KI-verktøy tas i bruk i helsevesenet. Samtidig kan syntetiske data medføre andre typer risiko.

Kunstig intelligens (KI) defineres i EUs nye KI-forordning (1) som et maskinbasert system som opererer med en varierende grad av autonomi, og utleder prediksjoner, innhold, anbefalinger eller beslutninger basert på inputdata. Dataene vil avhenge av behovet og brukskonteksten og kan være bilder, tabeller, tidsserier, tekst eller lydfiler (2).

For å sikre at KI-verktøy for bruk i pasientbehandling faktisk blir presise og trygge, trenger produsentene store mengder data til å utvikle og trene KI-produktene sine. I tillegg trenger helsetjenesten data til å validere og teste KI-verktøyene, eventuelt for å tilpasse dem til lokale populasjoner (3).

«Syntetiske data kan produseres med utgangspunkt i ekte pasientdata ved bruk av generative KI-modeller, og kan bestå av prøvesvar, radiologiske bilder og journalnotater som ser ekte ut, selv om de ikke er det»

Syntetiske datasett lages nå for disse formålene og avhjelper behovet for helsedata. Syntetiske data kan produseres med utgangspunkt i ekte pasientdata ved bruk av generative KI-modeller, og kan bestå av prøvesvar, radiologiske bilder og journalnotater som ser ekte ut, selv om de ikke er det. Det er stor optimisme på dette feltet knyttet til dype generative metoder, som de fleste nå kjenner fra ChatGPT.

Syntetiske data skal i prinsippet ikke kunne knyttes direkte til enkeltpersoner, og kan dermed benyttes friere (4). I EUs personvernforordning (GDPR) (5), som er tatt inn i norsk lovgivning, er alle opplysninger som kan knyttes til enkeltpersoner, definert som persondata. Alle persondata som benyttes til KI-utvikling, også de som benyttes til syntetiske data, er dermed regulert av GDPR. Andre relevante reguleringer er plikten til å ivareta retten til privatliv og konfidensialitet som er gitt av Grunnloven § 102 og pasient- og brukerrettighetsloven § 3-6 (6).

KI-modeller for helsevesenet skal dessuten være forsvarlige og ivareta pasientsikkerheten, for eksempel ved at de stiller korrekt diagnose eller foreslår kostnadseffektiv behandling. Dette er argumenter for å gi tilgang til persondata og helseopplysninger.

Tilgangen til person- og helsedata begrenses imidlertid av både lovreguleringer og av knapphet på data. Mangel på helsedata er gjerne mest uttalt ved sjeldne tilstander og sykdom hos barn. For disse kan syntetiske data representere både den beste og raskeste muligheten for å skaffe tilstrekkelig data til utviklingen av nye KI-modeller. (7).

Taushetsplikten

Taushetsplikten i helsevesenet er til for at enhver skal kunne oppsøke helsetjenesten med tillit til at personlige opplysninger ikke spres eller gjøres tilgjengelig for uvedkommende (8). Offentlige helseregistre kan være et utgangspunkt for å generere syntetiske data som i langt mindre grad utfordrer taushetsplikten og tilliten til helsetjenesten. Det lagres nå betydelige mengder helsedata i de nasjonale medisinske

kvalitetsregistre og andre helseregistre. Registerdata med pasientopplysninger kan overføres for sekundære formål som gitt av helseregisterloven; også disse opplysningene er underlagt taushetsplikt [\(9\)](#).

Data som omfattes av taushetsplikten, kan unntas fra plikten og komme til anvendelse dersom det er lite sannsynlig at de kan føres tilbake til personen, og hvis nytte og risiko ved dette er forholdsmessig. Syntetiske data som ikke kan føres tilbake til personer, er ikke personopplysninger og omfattes dermed ikke av taushetsplikten.

For å kunne vurdere risikoen for identifisering og risikoreduserende tiltak, må KI-modellen være transparent og med åpenhet om dataene som er brukt [\(10, 11\)](#).

Risiko og utfordringer

Syntetiske datasett må være representative for den populasjonen de er ment å brukes på. Kvalitetskontroll er nødvendig gjennom hele syntetiseringsprosessen, fra kontroll av det originale treningsdatasettet, måling av statistiske likheter mellom treningsdatasettet og det syntetiske datasettet, til testing av ytelsen til en modell trent på datasettet [\(11\)](#). I motsatt tilfelle kan KI-modellene introdusere ny risiko for pasientene når de brukes i diagnostikk og behandling.

Bruk av generative KI-metoder for å produsere syntetiske data er ressurs- og energikrevende, som har konsekvenser knyttet til miljø og bærekraft [\(12\)](#).

Skjevheter i treningsdatasettet kan uforvarende forsterkes gjennom syntetiseringsprosessen. Genereringsmetoder som ikke fanger opp underrepresenterte minoritetsgrupper i originaldataene, kan føre til diskriminering av personer og pasientgrupper ved at algoritmene i KI-modellene har for lav presisjon og reliabilitet for enkelte undergrupper [\(13\)](#). Samtidig kan syntetisering benyttes til å motvirke diskriminering, for eksempel ved å korrigere for opprinnelige skjevheter i den generative prosessen.

Sikring av personvernet

Risikoen for at personer kan identifiseres, minimaliseres gjennom bruk av syntetiske data, og mulighet for friere bruk og deling kan gi stor nytteverdi for helsevesenet. Når generative KI-modeller er optimalisert for å skape syntetiske data med størst mulig likhet med det originale datasettet, vil det likevel være en risiko for identifisering. Enkelte modeller kan gi nøyaktige kopier av deler av de originale dataene eller datapunkter som er materielt like, selv om det ikke finnes noen en-til-en relasjon mellom de reelle persondataene i treningsdatasettet og de syntetiske datapunktene. Dette betegnes som restrisiko for identifisering i det syntetiske datasettet [\(11\)](#), der restrisikoen øker med graden av kjennskap til genereringsmetodene [\(14\)](#).

Et sentralt spørsmål ved generering av syntetiske data er grenseoppgangen mellom når dataene fortsatt er personopplysninger og når er de syntetiske og kan behandles uten hensyn til GDPR eller taushetsplikt. En vesentlig hensikt med syntetiske data er jo at de

er anonyme og ikke omfattet av disse reguleringene. Den rettslige grensen for identifiseringsrisiko tar utgangspunkt i GDPR art. 4 (1) og flere ulike rettskilder (15–17). Et viktig moment er hvor sannsynlig det er at personer kan identifiseres.

«Mulighetene for identifisering når data genereres til syntetiske data, vil variere ut fra datasettets kompleksitet – antallet variabler og pasienter, statistiske uteliggere, eller genereringsmetoden som er brukt sammen med tilgangen til annen relevant informasjon»

Det er dessverre ikke umulig å utlede personlige data fra syntetiske datasett (18). Mulighetene for identifisering når data genereres til syntetiske data, vil variere ut fra datasettets kompleksitet – antallet variabler og pasienter, statistiske uteliggere, eller genereringsmetoden som er brukt sammen med tilgangen til annen relevant informasjon. Identifiseringsrisikoen vil også avhenge av hvor ressurskrevende det er å identifisere dataene, og om det er benyttet sikkerhetstiltak i genereringen.

Ved sikkerhetstiltak som er ment å hindre identifisering fra syntetiske data, kan det tilkomme økt risiko for at datasettet ikke lenger er representativt, noe som igjen kan svekke forsvarligheten og nytteverdien av dataene og KI-verktøyet (19).

«I et konsekvensetisk perspektiv kan samfunnsnyttene ved å ta i bruk KI-verktøy i helsevesenet rettferdiggjøre en høyere risiko for personidentifisering»

Etiske betraktninger

Etiske hensyn og prinsipper begrunner deler av lovene og kan inngå i rettslige avveininger, for eksempel i forsvarlighetsvurderinger. I konsekvensetikken legges det til grunn at en beslutning er riktig om den i sum optimaliserer mengden gode konsekvenser (20, 21). Det innebærer at beslutninger må vurderes helhetlig for å kunne ta stilling til om de er etisk holdbare. De totale positive virkningene må balanseres mot den totale skaden forårsaket av en handling (21). I et konsekvensetisk perspektiv kan samfunnsnyttene ved å ta i bruk KI-verktøy i helsevesenet rettferdiggjøre en høyere risiko for personidentifisering. Et annet hensyn er nytten dataene kan ha for fremtidige generasjoner, konsekvensetikerne legger fremtidige generasjoner betydelig mer vekt. (22). Dette står i kontrast til det klassiske økonomiske verdenssynet der fremtidig nytte har lavere verdi sammenlignet med dagens nytte, såkalt diskontering.

I et pliktetisk perspektiv kan også plikter for fremtidige generasjoner ha betydning. I rettslig sammenheng kan slike perspektiver omfattes av samfunnshensyn. Pliktetiske teorier skiller seg fra konsekvensetikken ved at det legges større vekt på individets verdi, autonomi og rettigheter enn den samlede samfunnsnyttene (21). I det pliktetiske rammeverket er det positive plikter til å hjelpe andre og negative plikter til ikke å påføre skade. Med KI-modeller skal nytte ses i et bredere perspektiv enn hensynet til den enkelte, da det kan ha nytte for flere, også fremover i tid. Holdninger i samfunnet og hvilken risiko mennesker er villige til å akseptere for å oppnå et felles gode, kan

også være relevante hensyn. Aksept av risiko kommer blant annet til uttrykk i undersøkelser om viljen til å avgi personlige data til forskning for å gagne andre (23, 24).

For at syntetiske data skal bidra til å løse utfordringen med tilgang til helsedata for utvikling av KI til det beste for våre pasienter, forutsettes det at de enten kan behandles som anonyme data eller i henhold til unntak i lov. Dersom de behandles som personopplysninger, vil bruken bli begrenset og nytteverdien betydelig redusert. Det at dataene er syntetiske, kan i seg selv anses som et risikoreduserende tiltak. Tilgangen til større datamengder gjennom bruk av syntetiske data kan også gjøre helsesektoren mindre avhengig av globale teknologiselskaper som besitter enorme mengder lukket, proprietær data til bruk i KI-utvikling.

Særskilte reguleringer av syntetiske data i helsesektoren, samt klarhet i myndighetenes krav til godkjenning av utstyr trent på slike data, vil kunne skape økt forutsigbarhet for utviklere og produsenter av KI-modeller, samt for brukere og pasienter innenfor helsesektoren.

Pasienter må akseptere en viss risiko ved andre tiltak i helsetjenesten. Et tema som hittil er belyst i liten grad, er hva slags risiko vi som samfunn mener enkeltindivider bør akseptere som en konsekvens av at dataene brukes som grunnlag for bedre tilgang til moderne medisinsk behandling, til fellesskapets beste.

REFERENCES

1. The Artificial Intelligence Act - Regulation (EU) 2024/1689. <https://www.artificial-intelligence-act.com/> Lest 12.9.2024.
2. Oussidi A, Elhassouny A. Deep generative models: Survey. 2018 International conference on intelligent systems and computer vision (ISCV). <https://ieeexplore.ieee.org/document/8354080> Lest 12.9.2024.
3. Sarker IH. Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions. SN Comput Sci 2021; 2: 420. [PubMed] [CrossRef]
4. Gonzales A, Guruswamy G, Smith SR. Synthetic data in health care: A narrative review. PLOS Digit Health 2023; 2: e0000082. [PubMed][CrossRef]
5. EU. 2016/679 The General Data Protection Regulation (GDPR). <https://eur-lex.europa.eu/eli/reg/2016/679/oj> Lest 12.9.2024.
6. Helse- og omsorgsdepartementet. LOV-1999-07-02-63. Lov om pasient- og brukerrettigheter (pasient- og brukerrettighetsloven). <https://lovdata.no/dokument/NL/lov/1999-07-02-63?q=Pasient%20og%20brukerrettighetsloven> Lest 12.9.2024.
7. Giuffrè M, Shung DL. Harnessing the power of synthetic data in healthcare: innovation, application, and privacy. NPJ Digit Med 2023; 6: 186. [PubMed] [CrossRef]
8. Helse- og omsorgsdepartementet. LOV-1999-07-02-64. Lov om helsepersonell m.v. (helsepersonelloven). <https://lovdata.no/dokument/NL/lov/1999-07-02-64?>

q=helsepersonelloven Lest 12.9.2024.

9. Helse- og omsorgsdepartementet. LOV-2014-06-20-43. Lov om helseregistre og behandling av helseopplysninger (helseregisterloven).

<https://lovdata.no/dokument/NL/lov/2014-06-20-43> Lest 12.9.2024.

10. Rajotte JF, Bergen R, Buckeridge DL et al. Synthetic data as an enabler for machine learning applications in medicine. *iScience* 2022; 25: 105331. [PubMed] [CrossRef]

11. Vallevik VB, Babic A, Marshall SE et al. Can I trust my fake data - A comprehensive quality assessment framework for synthetic tabular data in healthcare. *Int J Med Inform* 2024; 185: 105413. [PubMed][CrossRef]

12. Lavi H. Measuring greenhouse gas emissions in data centres: the environmental impact of cloud computing. *Climatiq*. <https://www.climatiq.io/blog/measure-greenhouse-gas-emissions-carbon-data-centres-cloud-computing> Lest 12.9.2024.

13. Bhanot K, Qi M, Erickson JS et al. The problem of fairness in synthetic healthcare data. *Entropy (Basel)* 2021; 23: 1165. [PubMed][CrossRef]

14. Wang Z, Myles P, Tucker A. Generating and evaluating cross-sectional synthetic electronic healthcare data: preserving data utility and patient privacy. *Comput Intell* 2021; 37: 819–51. [CrossRef]

15. Befring AK, Sand IJ. Big data og kunstig intelligens i helsesektoren. Oslo: Gyldendal, 2020.

16. EUR-Lex. Patrick Breyer v. Bundesrepublik Deutschland. Case C-582/14. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582> Lest 12.9.2024.

17. EUR-Lex. Single Resolution Board v. EDPS. Case T-557/20. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020TJ0557> Lest 12.9.2024.

18. Sun C, van Soest J, Dumontier M. Generating synthetic personal health data using conditional generative adversarial networks combining with differential privacy. *J Biomed Inform* 2023; 143: 104404. [PubMed][CrossRef]

19. Ghatak D, Sakurai K. A Survey on Privacy Preserving Synthetic Data Generation and a Discussion on a Privacy-Utility Trade-off Problem. I: *Science of Cyber Security - SciSec 2022 Workshops*. New York, NY: Springer, 2022.

20. Beachamp TL, Childress JF. *Principles of Biomedical Ethics*. Oxford: Oxford University Press, 2001.

21. Peach L. An introduction to ethical theory. I: Penslar RL. *Research Ethics: Cases and Materials*. Bloomington, IN: Indiana University Press, 1995: s. 13–26.

22. Parfit D. *Reasons and persons*. Oxford: Oxford University Press, 1987.

23. Kamm FM. Harming some to save others. *Philos Stud* 1989; 57: 227–60. [CrossRef]

24. Tosoni S, Voruganti I, Lajkosz K et al. Patient consent preferences on sharing personal health information during the COVID-19 pandemic: "the more informed we are, the more likely we are to help". BMC Med Ethics 2022; 23: 53. [PubMed] [CrossRef]

Publisert: 11. november 2024. Tidsskr Nor Legeforen. DOI: 10.4045/tidsskr.24.0328

Mottatt 10.6.2024, første revisjon innsendt 14.8.2024, godkjent 12.9.2024.

Opphavsrett: © Tidsskriftet 2026 Lastet ned fra tidsskriftet.no 8. september 2026.