DISCOVERING HEALTH DISPARITIES:
DESIGNING A SECURE MULTIPARTY ARCHITECTURE FOR SOCIAL HEALTH RESEARCH

HOW MPC CAN BE LEVERAGED TO UNITE GOVERNMENT DATASETS AND CONDUCT SECURE RESEARCH INTO THE SOCIAL DETERMINANTS OF HEALTH?

Delft University of Technology - CSE3000
Brontë Kolar
b.t.a.kolar@student.tudelft.nl
Supervisor: Zekeriya Erkin

20%

of health outcomes are attributed to social factors [1].

SOCIAL DETERMINANTS OF HEALTH

Social factors can have more influence on physical and mental health than clinical factors.

Discrimination along the social spectrum results in health inequities. For example, ethnic minorities are over-represented among COVID-19 cases and deaths [2]. In an effort to close these gaps and design new policies, public health organizations and their partners in social sectors research these determinants and their impact.

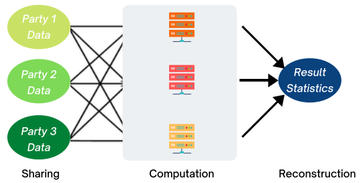
DATA CHALLENGES

Exploring how these social determinants affect health involves combining data from various siloed government ministries with healthcare data for analysis. Due to the sensitive nature of health and socioeconomic data, governments restrict its ability to be shared, even between ministries.

Modern cryptographic techniques open the door for performing large-scale secure research on these determinants in a compliant manner.

MULTIPARTY COMPUTATION

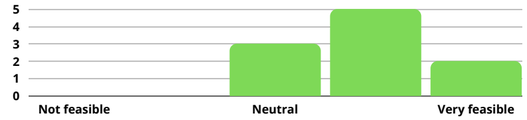
Multiparty computation (MPC) is a cryptographic technique that enables the privacy-preserving computation of a function. Two or more parties collectively compute a function on data, such that **each party learns nothing about the private inputs of the other parties**. Additive secret sharing is a common MPC technique that involves breaking a numeric secret into fragments that add up to the original secret [3].



MPC FEASIBILITY IN INDUSTRY

Survey data was collected from ten experts and stakeholders across the fields of healthcare and data privacy to record quantitative data on the feasibility of using MPC to investigate the social determinants of health.

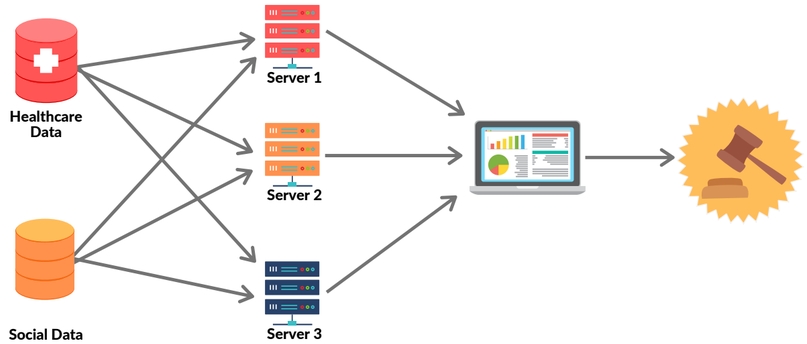
All participants were neutral or believed using MPC to combine data across institutions to investigate the social determinants of health is a feasible solution:



The top reported barriers to realising an MPC solution were:

MPC SOLUTION ARCHITECTURE

A potential solution is an MPC architecture based on 3-party additive secret sharing. The architecture accepts SQL queries and supports multiple parties submitting private inputs that are to be computed by 3 computing parties.



Data Sharing
Data is hashed, then encrypted by randomly splitting data into "secret shares".

Computation
Shares are distributed over servers and each server is controlled by a different trustee, who perform the computation jointly.

Results
Result shares are combined to reveal statistics. These can be shared with new parties or the input parties.

New Policies
Research is leveraged to enact policies that bring us closer to health equity.

THE ROAD TO HEALTH EQUITY

An established MPC platform like Sharemind or Senate could be used to improve trust in this technology and kickstart adoption.

Experts from the Netherlands and Canada reported the inability to share data between government institutions due to data regulations, **proving this a problem of global relevance.**

Scalability is a limitation, but data sharing between sectors on a smaller scale is still feasible. This technology could be used for the broad analysis of social factors within many industries, allowing for social disparities to be investigated in other relevant areas.

[1] Schroeder, S. A. (2007). We can do better—improving the health of the American people. New England Journal of Medicine, Chicago
[2] Wood D. As pandemic deaths add up, racial disparities persist — and in some cases worsen. 2020.
[3] Yehuda Lindell. Secure multiparty computation (MPC). IACR Cryptol. ePrint Arch., 2020:300, 2020.