PRIVACY-PRESERVING ELIGIBILITY VERIFICATION

Program Integrity Alliance

Verify the fact, not the file.

Government can confirm what applicants say against authoritative records it already holds, without moving that data or exposing more of it than the answer.

THE PROBLEM TODAY

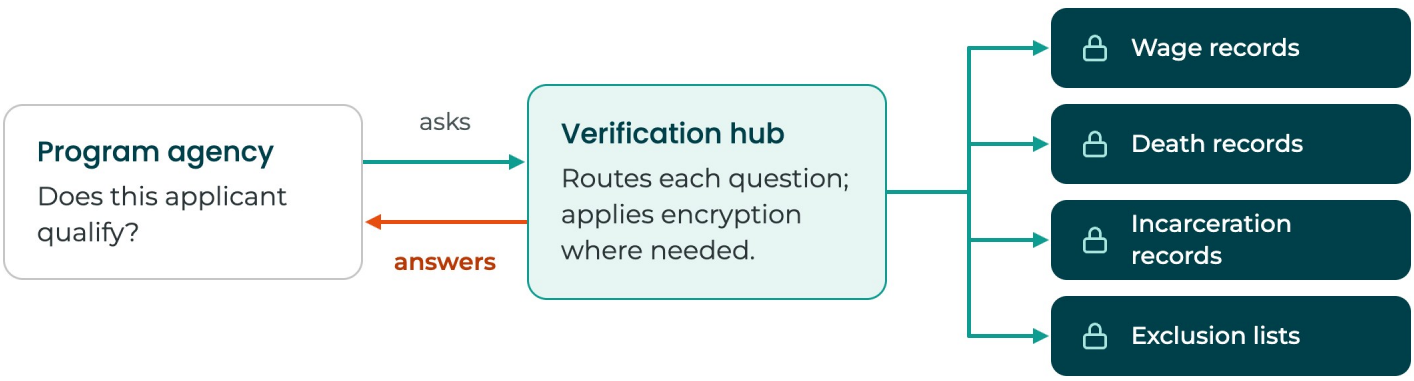
EITHER: TAKE THEIR WORD FOR IT

With little ability to check, agencies ask honest people for pay stubs and letters, while fraud rings with stolen identities and forged documents pass through.

OR: COPY THE DATA TO CHECK IT

Wage, tax and benefit records get pooled into new systems reachable by new users, exposing them to theft and misuse. Every new dataset meets resistance.

A BETTER MODEL



Answers are categorical: supported, not supported, or insufficient data. The underlying record never moves, and each source stays with the agency that collects it.

1

Authoritative data

Claims are checked against records government already holds, not documents that applicants supply or forgers fabricate.

2

Federated architecture

Each agency keeps custody of its own data and answers standardized questions about it. No copies, no central pool to breach.

3

Minimum disclosure

Only the answer travels. Privacy-enhancing cryptography, where needed, means even the hub never sees the record.

WHAT CHANGES

Easier access

Eligible people skip the document hunt. If data can't answer, today's process still applies.

Harder fraud

Invented facts on a stolen identity come back "not supported" and go to review.

Stronger privacy

No new databases to breach, and nothing moves that a yes-or-no answer can settle.

Privacy-enhancing technologies include zero-knowledge proofs, secure multiparty computation and homomorphic encryption. Verifying facts about an identity does not prove the applicant is that person; this model pairs with strong identity verification rather than replacing it.