Data Enclave

Wade Iuele, HPD Consultant, HCAI
HPD Data Enclave

- Secure environment for accessing potentially identifiable information
- Has controls so users can only access the data they are approved to see
- Protects against unapproved use of personal information
What is an Enclave?

• Centralized service to remotely access sensitive data
• Houses data in a secure and scalable environment
• Protects data in accordance with state and federal security and privacy rules
• Data is accessed via a virtual machine launched from the user's computer
• Virtual machine operates on a remote server
• Data products can only be downloaded to user’s computer with administrator authorization
How is an Enclave Used?

• Makes approved data available to approved users for approved projects
  – Each project’s data are segregated from other projects
  – May allow users to upload and link their own datasets
• May include access to:
  – Interactive, query-based tools
  – Suite of statistical tools (e.g., SQL, SAS, Stata, R, Python)
  – May allow users to access their own software tools
• Provides scalable computing power to perform analysis on a high volume of data
• Data products can only be downloaded with administrator authorization
Enclave Timeline

2022
Research
Conduct market research, interview other state APCDs, determine HPD Enclave requirements.

Selection
Select technology and vendor, initiate necessary procurements, plan and start project.

2023
Implementation
Build Enclave, create and house datasets, establish workflows, user testing, HCAI approval.

2024
Access
Begin intake and processing of data use requests, onboard approved users, collect fees, review analysis, authorize data product downloads.
Discussion Questions

• What are your experiences using data enclaves?

• What should HCAI consider in developing requirements for the Enclave?