

Appendix F

Privacy and Security

Fair Information Practices

Consistent with laws and regulations requiring States to incorporate Fair Information Practices into new and existing electronic systems, States should implement the following best practices to address FIPs in new and existing State eligibility and enrollment systems:

- *Collection and Use Limitation:* State systems should be designed to collect and use the minimum data necessary for an eligibility and enrollment determination. This should be balanced with the desire to reuse information for multiple eligibility decisions.
- *Data Integrity & Quality:* States should establish a minimum threshold level for data matches, adopting a glidepath toward achieving advanced probabilistic matching.
- *Openness & Transparency:* Clear, transparent policies about authorizing access and use of data should be provided to the consumer in the Privacy Notice.

Consumer Mediated Approach

We believe that the following best practices should be used to facilitate a consumer-mediated approach to data sharing:

- Provide consumer information to the consumer in a human-readable form that allows them to view, print, or save data in a format they can use and reuse;
- Enable data to be exported into commonly-used software formats such as spreadsheets, text files, etc.;
- Develop separate pathways for download requests from the consumer and download requests via automated processes acting on the consumer's behalf; and,
- Limit data use to that specified in the Privacy Notice unless the consumer consents to additional uses.

OAuth is an example of a consumer mediated authorization mechanism between third parties and their data origins. OAuth is a delegated authorization platform that allows a consumer to selectively grant, limit or revoke specific privileges to third parties without revealing their private credentials to those third parties or developers.

Consistent with the Privacy Act, the Privacy Notice provided to the consumer during the application process will govern the consumer's rights to confidentiality and privacy. The Privacy Notice should be provided to the consumer prior to or at the time of collection of personally identified information in a method the consumer can understand. The Privacy Notice should also clearly indicate all entities that will be permitted to use a consumer's eligibility data, as well as the permissible uses of such data.