

Limited Data Sets

Health care organizations may use or disclose PHI in a limited data set for purposes of research, public health, or health care operations [45 CFR §164.514(e)]. The limited data set must remove the following direct identifiers of a person or the person's relatives, employers, or household members:

1. Names.
2. Postal address information, other than town or city, State, and zip code.
3. Telephone numbers.
4. Fax numbers.
5. Electronic mail addresses.
6. Social security numbers.
7. Medical record numbers.
8. Health plan beneficiary numbers.
9. Account numbers.
10. Certificate/license numbers.
11. Vehicle identifiers and serial numbers, including license plate numbers.
12. Device identifiers and serial numbers.
13. Web Universal Resource Locators (URLs).
14. Internet Protocol (IP) address numbers.
15. Biometric identifiers, including finger and voice prints.
16. Full face photographic images and any comparable images.

Data use agreement is required

Health care organizations must have data use agreements with any recipients of PHI in limited data sets. The agreements must state that the recipient will only use or disclose the PHI for limited purposes.

The agreements must:

- Establish the permitted uses and disclosures of the PHI by the recipient. For example, an agreement may not authorize any use or disclosure that violates HIPAA (such as for marketing purposes).
- Establish who is permitted to use or receive the limited data set.
- Require that the recipient:
 - Not use or disclose the information other than as permitted by the agreement or as otherwise required by law;
 - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the agreement;
 - Report to the health care organization any use or disclosure of the information that it is aware is not permitted in the agreement;