

**Ohio Department of Health HIV Surveillance Program
Data User Agreement for Data to Care (D2C)
(Revised December 2023)**

Requester information:

Requester Name:	Requester title:	
Organization:	Email Address:	
Telephone:	Date requested:	Desired Completion Date:

**Additional persons who will access
data:**

Name:	Title:	Email:
Name:	Title:	Email:
Name:	Title:	Email:

Detailed Description of HIV Surveillance Data Request:

Disease Category (check all that apply):

☒ Reported Persons Living with HIV Infection

Time Period:

☒ Living with HIV Infection as of MM/DD/YYYY, no evidence of care as of MM/DD/YYYY

Geographic Area:

☒ Other (specify): Region ____

Purpose of Request:

☒ Data-to-Care

Format:

☒ patient identifier, patient last name, patient first name, date of birth, sex at birth, current gender, HIV diagnosis date, race/ethnicity, HIV transmission category, current patient address, most recent CD4 count/percent, most recent viral load, date of specimen collection, test result, health care facility, and health care provider.

How will the data be used? Please be specific:

Use HIV Surveillance and other data to identify persons with diagnosed HIV infection who may not be receiving regular HIV medical care.

By signing this document, I certify that I understand that I may be provided access to confidential information about persons who are HIV infected, persons counseled during HIV clinical or prevention activities, HIV study participants, and/or clients. This information includes surveillance information including paper and/or electronic laboratory and/or medical records, study-related forms and/or records, information obtained through oral and/or written interviews, and/or other related contact information. This information may also originate from the records of health care providers, health care facilities, medical and health clinics, drug treatment centers, correctional institutions and jails, and/or other institutions and facilities responsible for diagnosing, treating and/or counseling HIV infected individuals. Examples of confidential information include but are not limited to patient names, addresses, telephone numbers, risk behaviors and modes of HIV transmission, medical, psychological and/or health related conditions and treatment, personal finances, living arrangements, and social history. If confidential information has been disclosed to me in other than a summary, statistical, or aggregate form, I shall make no further disclosure of this information without the specific, written, and informed release of the individual to whom it pertains, or as otherwise permitted by state law.

Terms of Agreement:

- Efforts will be made to ensure the security of all confidential information by limiting the work area to employees with approved access.
- Personally identifiable information (PII) will not be discussed except in the performance of job-related duties. These discussions must not take place in hallways, elevators, restrooms, lunchrooms or other public areas, and/or at any time outside of business hours.
- Telephone conversations and/or conference calls requiring the discussion of identifiers will only be conducted in confidential work areas.
- Appropriate security measures to ensure that privileged, confidential, or private information remains protected will be adhered to when transporting information.
- Any document to be disposed of that contains patient identifiers shall be shredded per the Ohio Department of Health records retention policy.
- The computer where HIV surveillance data is accessed by the employee will be protected by screen saver passwords. The passwords will not be disclosed/shared, nor access allowed to unauthorized persons.
- To prevent unauthorized access to confidential data and databases, users must log off from the network before work breaks, work lunches, and when leaving work until the next business day.
- Information on back-up or portable devices (e.g., laptops, compact disks, flash drives, diskettes) must be encrypted, password-protected and the device must be sanitized when the information is no longer needed or upon completion of the activity/project.
- All confidential files, including compact discs and flash drives must be kept in a physically secure location such as a secure file cabinet or locked desk drawer when not in use, when the work area is left unattended, and/or other persons need to enter the secure work area.
- When transferring data electronically, secure electronic methods (e.g., encrypted file, sFTP) must be used in accordance with CDC S&C Guidelines. Confidential PII should never be transmitted via email, even within an individual agency as content of email can be subject to Freedom of Information Act (FOI) requests.
- Reports, records and/or information may only be released in accordance with relevant, established Ohio Department of Health Directives (Data Stewardship), the ODH HIV Surveillance Program Security and Confidentiality Policy, and the ODH HIV Surveillance Program Data Release Policy.
- The HIV surveillance data generated and used while employed by the Ohio Department of Health or local public health authority is the property of the Ohio Department of Health.
- Obligations under this Agreement will continue after termination.
- Each employee with access to HIV Surveillance data is responsible for monitoring security practices. Potential, suspected or known security breaches must be immediately reported to the authorized person's supervisor. The authorized

person's supervisor will report the breach to the ORP. A breach that results in the release of PII about one or more individuals will be reported immediately to CDC. The ORP will consult with ODH Office of General Counsel (OGC) to determine whether the nature and extent of the breach warrants reporting to law enforcement agencies, and document OGC recommendations.

By signing this statement, I am indicating my understanding of my responsibilities and agree to abide by the Ohio HIV Surveillance Security and Confidentiality Policy and Ohio Revised Code Sections 3701.17 and 3701.24.

Authorized Person Name (Print)

Authorized Person Signature

Date

First Additional Authorized Person Name (Print)

First Additional Authorized Person Signature

Date

Second Additional Authorized Person Name (Print)

Second Additional Authorized Person Signature

Date

Third Additional Authorized Person Name (Print)

Third Additional Authorized Person Signature

Date

Authorized Person's Immediate Supervisor Name (Print)

Authorized Person's Immediate Supervisor Signature

Date

HIV Prevention Coordinator Signature (LHD)

Date

HIV Surveillance Coordinator Signature (ODH)

Date

HIV Surveillance Program Overall Responsible Party Signature (ODH)

Date