National HIV Surveillance System (NHSS)

Attachment 7(a)

Assurance of Confidentiality Statement for HIV Surveillance and Surveillance-related Data

ASSURANCE OF CONFIDENTIALITY STATEMENT
FOR THE NATIONAL HUMAN IMMUNODEFICIENCY VIRUS (HIV)
SURVEILLANCE SYSTEM (NHSS) AND SURVEILLANCE-RELATED DATA
(INCLUDING SURVEILLANCE INFORMATION, CASE INVESTIGATIONS,
TRANSMISSION CLUSTER INVESTIGATIONS, SUPPLEMENTAL SURVEILLANCE
PROJECTS, RESEARCH ACTIVITIES, AND EVALUATIONS)
October 2019

The national HIV surveillance program is coordinated by the HIV Incidence and Case Surveillance Branch (HICSB) and the Behavioral and Clinical Surveillance Branch (BCSB) of the Division of HIV/AIDS Prevention (DHAP), in the National Center for HIV/AIDS, Viral Hepatitis, STD and TB Prevention (NCHHSTP), a component of the Centers for Disease Control and Prevention (CDC), an agency of the United States Department of Health and Human Services. The surveillance information requested by CDC consists of reports of persons with suspected or confirmed HIV infection at any clinical stage of disease, including children born to mothers infected with HIV, and reports of persons enrolled in studies designed to evaluate the surveillance program and to assess behaviors, medical care, and health status of people living with HIV or at risk of acquiring HIV. The information is collected from laboratory, clinical, and other medical or public health records of suspected or confirmed HIV cases; and from surveys or investigations that interview persons in recognized HIV risk groups or known to have a diagnosis of HIV.

Surveillance data collection is conducted by state and territorial health departments which forward information to CDC after deleting patient and physician names and other identifying or locating information. Records maintained by CDC are identified by computer-generated codes, patient date of birth, and a state/city assigned patient identification number. The data are used only for public health purposes, including public health statistical, epidemiologic, and analytic summaries and for public health evaluations, investigations and research by CDC scientists and cooperating state and local health officials to understand and control the spread of HIV. In rare instances, expert CDC staff, at the invitation of state or local health departments, may participate in research or case investigations of unusual transmission circumstances or cases of potential threat to the public health. For example, CDC staff may conduct epidemiologic and laboratory investigations of cases that may have rare or previously unidentified modes of HIV transmission, unusual clinical manifestations, unusual laboratory test results, or molecular HIV sequence data that indicate recent or rapidly growing HIV transmission clusters. These include, but are not limited to, transfusion and transplant-related cases, cases of HIV transmitted in occupational settings, cases of HIV-2 infection, cases transmitted through female-to-female sexual contact, cases with potentially unusual HIV strain variants, cases with clinical evidence of HIV infection but negative HIV test results, investigation of false positive clusters and discordant results, and breakthrough infections in the presence of pre-exposure prophylaxis. In these rare instances, with authorization, CDC staff may collect and maintain information that could directly identify individuals.

Information collected by CDC under Sections 304 and 306 of the Public Health Service Act (42 U.S.C. 242b and 242k) as part of the HIV surveillance system that would permit direct or indirect identification of any individual or institution on whom a record is maintained, and any identifiable information collected during the course of an investigation on either persons supplying the information or persons described in it, is collected with a guarantee that it will be held in confidence, will be used only for the purposes stated in this Assurance, and will not otherwise be disclosed or released without the consent of the individual or institution in accordance with Section 308 (d) of the Public Health Service Act (42 U.S.C. 242m(d)). This protection lasts

forever, even after death. Information that could be used to identify any individual or institution on whom a record is maintained by CDC will be kept confidential. Full names, street addresses, social security numbers, and telephone numbers will not be reported to this national HIV surveillance system. Medical, personal, and lifestyle information about the individual, and a computer-generated patient code (e.g., soundex code) will be collected and reported to the national HIV surveillance system.

Surveillance information reported to CDC will be used only for public health purposes without identifiers primarily for public health statistical, epidemiologic, and analytic summaries and for public health evaluations in which no individual or institution on whom a record is maintained can be identified, and secondarily, for special public health research or investigations of the characteristics of populations suspected or confirmed to be at increased risk for infection with HIV and of the natural history and epidemiology of HIV. When necessary for confirming surveillance information or in the interest of public health and disease prevention, CDC may confirm information contained in case reports or may notify other medical personnel or health officials of such information; in each instance, the number of persons with access to the information will be kept to a minimum, only the minimum information necessary for the applicable activity will be disclosed, and de-identified data will be used whenever possible.

Surveillance data will only be released only for public health purposes and in accordance with the policies for data release established by the Council of State and Territorial Epidemiologists and data re-release agreements with health departments. Surveillance data will only be released to other components of CDC; health agencies of federal, state, or local governments; and select members of the public. CDC HIV surveillance or research information that could be used to identify any individual or institution on whom a record is maintained, either directly or indirectly, will not be made available to anyone for non-public health purposes. In particular, HIV surveillance or research information that could be used to identify any individual or institution on whom a record is maintained, either directly or indirectly, will not be disclosed for commercial purposes, nor disclosed to the public; to family members; to parties involved in civil, criminal, or administrative litigation; or to non-health agencies of the federal, state, or local governments.

Information in this surveillance system will be kept confidential. Only authorized employees of DHAP in HICSB, BCSB, the Quantitative Sciences and Data Management Branch and Laboratory Branch, their contractors, other authorized staff and other authorized agents granted access, guest researchers, fellows, visiting scientists, authorized external collaborating researchers, research interns, and graduate students who participate in activities jointly approved by CDC and the sponsoring academic institution, and the like, will have access to the information.

Authorized users of protected information are required to handle the information in accordance with procedures outlined in the Confidentiality Security Statement for the National Human Immunodeficiency Virus (HIV) Surveillance System (NHSS) and Surveillance-Related Data (including surveillance information, case investigations, transmission cluster investigations, supplemental surveillance projects, research activities, and evaluations).

CDC is in compliance with applicable federal law requiring the protection of federal computer networks from cybersecurity risks like hacking, internet attacks, and other security weakness; computer network experts working for, or on behalf, of the government, may intercept and review information sent through government networks for cyber threats if the information is sent through the government network triggers a cyber threat indicator.