CROSS-JURISDICTIONAL DATA SHARING: **LEGAL, PRACTICAL, AND ETHICAL CONSIDERATIONS FOR IMPROVED INFECTIOUS DISEASE CLUSTER RESPONSE**

INTRODUCTION

Communicable disease surveillance data are routinely collected by state, territorial, and local public health surveillance systems to conduct activities, such as assessing disease prevalence, implementing data-to-care activities, and responding to disease outbreaks or clusters. Evidence-based and innovative public health data-use and data-sharing practices allow health departments to leverage public health and healthcare systems data more effectively.[1] These practices often include sharing of disease surveillance data, which are generally collected in accordance with state and local laws but without explicit patient consent. While these data-sharing activities fall under the umbrella of legal public health action, they have raised questions about appropriate data privacy, confidentiality protections, and ethical issues related to sharing data.

In light of increasing HIV and hepatitis C incidence among people who use and inject drugs in the United States, as well as substantial HIV clusters and outbreaks over the past several years, the Association of State and Territorial Health Officials (ASTHO) spearheaded a 2019 project to identify cross-jurisdictional outbreak preparedness measures that would enable a more streamlined and effective response to clusters in neighboring jurisdictions. This project highlighted the experiences of three neighboring jurisdictions—Kentucky, Ohio, and West Virginia—that, in recent years, have experienced HIV outbreaks and conducted cluster response efforts near their state borders. This resource will highlight the experiences of these states, as well as other jurisdictions that have successfully created systems for cross-jurisdictional data sharing. Analysis and dissemination of these case studies may have broader utility for other jurisdictions.

This resource, developed in partnership with the National Alliance of State and Territorial AIDS Directors (NASTAD), addresses legal, practical, and ethical considerations to support health department decision-making concerning cross-jurisdictional data-sharing practices relating to HIV and viral hepatitis clusters and outbreaks, and offers recommendations for how health departments can improve outbreak preparedness measures through preemptive cross-jurisdictional data-sharing arrangements.

METHODOLOGY

Research for this project included assessments of legal public health data-sharing authority in Kentucky, Ohio, West Virginia; interviews with Kentucky, Ohio, and West Virginia health department staff to understand data-sharing practices and interpret jurisdictional statutes; and legal analysis coupled with informant interviews to identify successful data-sharing practices in other jurisdictions. Based on this research, researchers identified six key steps to guide cross-jurisdictional data-sharing efforts.

---

[1] NASTAD, *HIV Data Privacy and Confidentiality: Legal & Ethical Considerations for Health Department Data-Sharing* (June 2018), https://www.nastad.org/resource/hiv-data-privacy-and-confidentiality.

KEY FINDINGS AND RECOMMENDATIONS

Steps for Implementing Cross-Jurisdictional HIV and Viral Hepatitis Surveillance Data Sharing for Improved Outbreak Detection and Response

1. **Identify the types of data** to be shared with neighboring jurisdictions.
2. **Assess legal authorities and barriers** related to cross-jurisdictional data sharing.
3. **Assess ethical considerations** for cross-jurisdictional data sharing, particularly as it pertains to people who use drugs.
4. **Engage legal counsel** about legal and regulatory considerations for emerging data-sharing activities.
5. **Identify data platforms and processes** that allow for secure data transmission.
6. **Monitor data-sharing activities** for privacy compliance, assessment of emerging issues, and potential need for modifications in data-sharing protocols.

STEP 1: IDENTIFY THE TYPES OF DATA TO BE SHARED WITH NEIGHBORING JURISDICTIONS.

HIV Surveillance Data

Cross-jurisdictional sharing of data reported in Enhanced HIV/AIDS Reporting System (eHARS) databases is invaluable for ensuring accuracy in HIV surveillance data. Up-to-date surveillance data facilitate cluster detection and promote efficient data-to-care and cluster response strategies.

Kentucky, Ohio, and West Virginia participate in Routine Interstate Duplicate Review (RIDR), a standard HIV surveillance practice used to identify duplicate case data between jurisdictions and exchange information about individuals diagnosed with HIV who are documented in eHARS databases maintained by multiple jurisdictions. RIDR is conducted semi-annually based on reports generated from deidentified eHARS data in 59 jurisdictions and distributed by CDC. RIDR operates with an estimated 12-month time lag between case reporting and duplicate resolution due to the extensive manual follow-up needed to deduplicate records.[2] Due to the time lag, this form of data-sharing and deduplication has limited utility in emergent cluster response. However, it is currently the only routine data exchange in place. Additionally, there is no similar or standardized nationwide process for the deduplication of viral hepatitis surveillance data.

Regional data-sharing relationships between jurisdictions with shared borders may supplement RIDR in areas with significant population movement, where residents frequently travel or relocate across borders. Additional data exchange beyond standard RIDR may be particularly useful for neighboring jurisdictions vulnerable to HIV outbreaks. Such outbreaks often include individuals who reside or seek care in different jurisdictions and are therefore likely included in multiple eHARS systems.

---

[2] Joanne Michelle Ocampo, et al., *Improving HIV Surveillance Data by Using the ATra Black Box System to Assist Regional Deduplication Activities*, JOURNAL OF ACQUIRED IMMUNE DEFICIENCY SYNDROMES: Vol. 82, Supp., S13 (Sept. 2019), https://journals.lww.com/jaids/Fulltext/2019/09011/Improving_HIV_Surveillance_Data_by_Using_the_ATra.3.aspx.

Maryland, Virginia, and Washington, D.C. have established a local "Black Box" data exchange process to deduplicate HIV data on a quarterly basis through sharing personally identifiable information, exchanging laboratory data to assess the HIV care continuum, and enabling accurate estimates of the HIV burden in their jurisdictions.[3] The Black Box, which began as a 2014 pilot program, is an automated process that uses encrypted technology to receive surveillance data from the three health departments and securely report likely matches back to the jurisdictions.[4]

This quarterly exchange occurs more frequently than the semi-annual RIDR process. More frequent data exchanges are beneficial to jurisdictions like Maryland, Virginia, and Washington, D.C. This is mainly due to the frequency with which people in this area traverse borders to work, socialize, seek healthcare, and change residence. High rates of cross-jurisdictional migration and care-seeking within a metropolitan area can pose challenges to maintaining accurate surveillance estimates absent an efficient process for deduplicating and consolidating case data.[5] The Black Box process used by Maryland, Virginia, and Washington, D.C. is more accurate than the standard RIDR method because duplicate cases can be identified using information such as Social Security Number and last name, which is not available at the national level.[6]

This automated process increases efficiency and accuracy of deduplication efforts while maintaining data privacy because duplicate cases can be identified using a larger set of data points, but health department staff do not need to view or store any personally identifiable information used in the matching process.[7] The Black Box process has also significantly reduced the number of manual RIDR processes needed—after beginning regular data exchanges in 2017, the volume of HIV cases needing RIDR decreased by 74% between Washington, D.C. and Maryland, and 81% between Washington, D.C. and Virginia.[8] This is consistent with findings that implementation of a Black Box system with a larger number of jurisdictions resulted in significantly increased accuracy and time efficiency compared to standard RIDR.[9]

Virginia also participates in a Black Box system that includes a larger number of jurisdictions but reported several advantages to a smaller, three-jurisdiction system, such as the ability to modify agreements easily when needed; the ability to include other types of data, such as care-related information, in data-sharing agreements; and flexibility to test innovative approaches to data-sharing.

Efficient HIV surveillance data sharing across jurisdictions can also support data-to-care activities. Data-to-care efforts use HIV surveillance data to identify and re-engage people who have been diagnosed with HIV but are not in care. Jurisdictions expend significant public health resources on locating individuals who appear to be out-of-care based on clinical and surveillance data. In Maryland, Virginia,

---

[3] Auntre D. Hamp, et al., *Cross-Jurisdictional Data Exchange Impact on the Estimation of the HIV Population Living in the District of Columbia: Evaluation Study*, JOURNAL OF MEDICAL INTERNET RESEARCH: PUBLIC HEALTH AND SURVEILLANCE: Vol. 82, Iss. 3, 21 (2018), https://publichealth.jmir.org/2018/3/e62/.

[4] *Id.*

[5] *Id.*

[6] Centers for Disease Control and Prevention, "National HIV Surveillance System (NHSS), Attachment 4c: Duplicate Review Technical Guidance," Feb. 2018 (accessed Apr. 26, 2021), https://www.reginfo.gov/public/do/DownloadDocument?objectID=92803101.

[7] Ocampo, et al., *supra* note 2.

[8] Hamp, et al., *supra* note 3.

[9] Ocampo, et al., *supra* note 2.

and Washington, D.C., individuals who appear to be out-of-care based on surveillance data may, in fact, have relocated their residence or accessed services in a nearby jurisdiction. The Black Box system enabled these jurisdictions to reduce the number of people appearing to require re-engagement by increasing accuracy of patient location and laboratory data, saving public health resources that would otherwise have been spent searching for individuals with incomplete surveillance data.

Kentucky, Ohio, and West Virginia reported interest in expanding interstate data sharing of HIV surveillance data beyond the standard RIDR process to improve overall accuracy and facilitate cluster detection and response activities near their shared borders.

Case Study: Innovative Models for Cross-Jurisdiction HIV Data Sharing

Maryland, Virginia, and Washington, D.C. have established a local "Black Box" data exchange process to deduplicate HIV data on a quarterly basis through sharing personally identifiable information, exchanging laboratory data to assess the HIV care continuum, and enabling accurate estimates of the HIV burden within their jurisdictions.[1] The Black Box, which began as a 2014 pilot program, is an automated process that uses encrypted technology to receive surveillance data from the three health departments and securely report likely matches back to the jurisdictions.[1]

Viral Hepatitis Surveillance Data

There is no nationwide process for deduplication of viral hepatitis surveillance data, though jurisdictions that have responded to hepatitis A outbreaks may have some system in place for data sharing related to vaccine-preventable diseases. Kentucky, Ohio, and West Virginia reported little-to-no interstate data-sharing of viral hepatitis surveillance data. While these states may share some hepatitis surveillance data with neighboring states, this data-sharing is not conducted on a routine basis and is typically limited to informal data exchange, such as by responding to individual requests by phone or secure email. No states reported having any existing mechanisms in place for consistent deduplication of viral hepatitis surveillance data.

HIV Care and Case Management Data

Sharing HIV surveillance data across borders enables jurisdictions to maintain up-to-date, non-duplicative surveillance records and supports data-to-care activities. However, sharing care- and case management-related data with neighboring jurisdictions can further improve cluster response efforts.

West Virginia reported that it exchanges care-related data, distinct from cluster surveillance data, with Ohio and Kentucky to maintain accurate records for Ohio and Kentucky residents identified within a West Virginia cluster. However, this data-sharing is informal and conducted by phone on an as-needed basis.

Virginia has built upon existing data-sharing relationships with Maryland and Washington, D.C. through the Black Box project to execute formal data-sharing agreements allowing the exchange of care and case management data, such as information related to linkage to care, referral, and partner services. This

enables the states to identify more cluster members, maintain comprehensive information related to clusters, link people to care, and take public health action to limit transmission within a cluster, including identifying and providing wraparound services

STEP 2: ASSESS JURISIDICTIONAL LEGAL AUTHORITY AND BARRIERS TO CROSS-JURISDICTIONAL DATA-SHARING.

All states provide some statutory authority for state and/or local health officers to implement measures for control, prevention, and treatment of communicable diseases. These statutes and any implementing regulations typically include privacy and confidentiality provisions, which authorize sharing of personally identifiable information as needed for health departments to effectively carry out their public health functions. While some state statutes specifically delineate the scope of authorized activities, other states define the parameters of statutory public health authority through administrative regulations. However, most state statutes and regulations give health departments and their legal counsel discretion to act under fairly broad authority. As a result, many health departments use their own discretion to develop data-sharing policies and written data-sharing agreements with other state health departments.

Statutes and regulations establishing data privacy and confidentiality for communicable disease data provide a framework for determining the extent to which states may share data with other states for cluster detection and response purposes. State laws addressing communicable disease data privacy may be specific to HIV data or apply broadly to some or all reportable communicable diseases. While some state laws and regulations specify the types of data that can be shared and the circumstances under which data-sharing is permissible, most jurisdictions give health departments broad discretion to make data-sharing decisions. Most statutes and regulations do not explicitly address emerging data-sharing practices, such as data-to-care and use of data in cluster detection and response activities. Further interpretation and analysis from department legal counsel, as well as collaboration between legal counsel and programmatic staff, may present new opportunities for data-sharing across borders.

West Virginia

West Virginia provides broad statutory authority for local health officers to investigate cases of communicable diseases within their jurisdiction, ascertain the sources and spread of communicable diseases, and institute measures to prevent transmission.[10] The parameters are further defined through state health agency rules authorizing local health officers to collaborate with public health officials in other states when investigating an outbreak or cluster involving residents of that state.[11] Such investigation may include "systematic collection of demographic, clinical, laboratory and epidemiological information on the cases" and "ongoing surveillance to establish that the outbreak is over."[12]

Despite this clear legal authority for local health officers to collaborate with other states to detect and respond to disease outbreaks and clusters, the West Virginia Department of Health and Human Resources has not implemented routine cluster response data-sharing processes with neighboring states or with local health authorities. West Virginia health department staff reported that, while they can routinely share surveillance with neighboring states for deduplication purposes, collaboration with other states for detecting and responding to clusters is conducted on an ad hoc basis. When West Virginia identifies cluster members in Ohio or Kentucky through a Soundex search, and the person is not

[10] W. Va. Code Ann. § 16-4-2.
[11] W. Va. Code R. 64-7-7.3.
[12] W. Va. Code R. 64-7-7.4.

included in the RIDR report provided by CDC, health department staff notify the other state's health department that their resident was involved in a West Virginia outbreak.

However, Ohio and Kentucky do not similarly request cluster detection data from West Virginia outside of standard deduplication processes such as RIDR. West Virginia health department staff also request care data about Ohio and Kentucky residents who receive care in West Virginia, and similarly shares care information with Ohio and Kentucky upon request. West Virginia expressed interest in executing written data-sharing agreements with neighboring states to share data more systematically through a routine, standardized process that does not require individual follow-up for every person identified in a cluster. Health department staff in West Virginia, Kentucky, and Ohio all indicated that informal data-sharing processes rely upon existing relationships with state and local health departments in other states and are therefore vulnerable to change in health department personnel absent formal written agreements and established internal policies.

Ohio

Ohio's statutes generally give the state health officer broad authority to investigate the cause of contagious and infectious disease and to take prompt action to control and suppress the spread of disease.[13] Information collected pursuant to such investigation is generally confidential, but the health director has discretion to execute written agreements to facilitate exchange of information related to ongoing public health investigations with "government entities."[14] The statutes provide additional protections when the release includes "protected health information." In general, protected health information may be released without patient consent for the purposes of providing treatment or ensuring accuracy of information, only pursuant to a written agreement requiring the recipient to comply with Ohio's confidentiality requirements, or in response to a search warrant or subpoena from a grand jury or prosecutor.[15]

However, the law gives the health officer discretion to release protected health information without a written agreement if the health officer determines that release is necessary to avert or mitigate a clear threat to individual or public health, provided the release is made only to persons or entities necessary to control, prevent, or mitigate disease.[16] Staff at the Ohio Department of Health reported that the statute is intentionally broad, placing guardrails around permissible data-sharing without limiting the health department's ability to share data with external stakeholders in circumstances that legislators may not have contemplated when drafting a narrower statute. In evaluating whether data release is appropriate in each instance, the health department considers the totality of circumstances to determine whether the statutory requirements are met. Release serves a necessary public health purpose and is limited to only those individuals who have a need for the information in furtherance of that objective.

Staff at the Ohio Department of Health reported no legal barriers to interstate HIV surveillance data sharing, indicating that it may share protected health information with other states. However, bi-directional interstate data-sharing has been limited due to legal and technological limitations in other states. Health department staff therefore indicated that it might be useful to formally outline data-sharing processes and identify potential barriers to sharing data across state lines, but that it would take

[13] Ohio Rev. Code Ann. § 3701.14(A).
[14] Ohio Rev. Code Ann. § 3701.14(B)(2).
[15] Ohio Rev. Code Ann. § 3701.17(B).
[16] Ohio Rev. Code Ann. § 3701.17(B)(4).

health department leadership and buy-in to ensure data sharing was consistently practiced. Like West Virginia and Kentucky, Ohio reported that successful data sharing without formal written agreements often relies upon existing relationships with health department colleagues in other states, making these relationships vulnerable to staff turnover.

Ohio HIV surveillance program staff utilize the Council for State and Territorial Epidemiologists HIV contact board to identify state-specific HIV surveillance program contacts to ensure securing exchange of sensitive information during case record searches and RIDR investigations. The health department considers written data-sharing agreements with other states that set expectations and parameters for data exchange to be a good practice, even though such agreements are neither legally required nor legally binding. When evaluating whether a given data-sharing platform or mechanism is secure, the health department consults with the Ohio Department of Health (ODH) Office of Management Information Systems (OMIS) and the Ohio Department of Administrative Services (ODAS) Office of Information Technology to ensure compliance with minimum standards under the Health Insurance Portability and Accountability Act (HIPAA). The establishment of a system such as the Maryland, Virginia, and Washington, D.C. Black Box would require collaboration between ODH legal counsel, OMIS and ODAS, agency HIPAA privacy and security officers, and database administrators.

The Ohio Department of Health also has a mechanism in place for sharing STI/HIV partner services information with other states. CDC's Division of STD Prevention and Control refers to this long-standing practice as Out-of-Jurisdiction or "OOJ" investigations. More recently, the Council for State and Territorial Epidemiologists STD subcommittee developed a contact board similar to the HIV contact board previously mentioned. States are responsible for maintaining their STD contact list on the site. In Ohio, the STI surveillance program serves as the OOJ contacts.

Kentucky

Kentucky's HIV reporting statute broadly authorizes health department HIV surveillance staff to match information from the state's HIV reporting system to other public health databases to limit duplication and better quantify the extent of the state's HIV epidemic.[17] Personally identifiable information may only be released to entities outside the health department in compliance with federal law or in consultation with other state surveillance and reporting sources.[18]

Staff at the Kentucky Department for Public Health reported that their experiences sharing data across state lines have been limited. While they have engaged in some successful data-sharing with Ohio, this was a one-time, limited exchange in response to a specific cluster at the states' shared border. Kentucky health department staff echoed concerns raised by Ohio and West Virginia that informal, reactive data-sharing in the event of a cluster relies upon individual relationships between staff working in different health departments and is therefore vulnerable to change. The Kentucky Department for Public Health is currently working on developing a written data-sharing agreement with Ohio, consistent with its cluster outbreak and response plan submitted to CDC and indicated that preemptively executing data-sharing agreements with neighboring states would enable Kentucky to prepare for cluster response and detection activities in the future. While Kentucky does not have a cluster response plan for viral hepatitis, a data-sharing agreement may be helpful and would assist in hepatitis C elimination planning.

[17] Ky. Rev. Stat. Ann. § 214.645(3)(a).
[18] Ky. Rev. Stat. Ann. § 214.645(3)(j).

Other Considerations

In some states, interstate data sharing may require explicit statutory authorization. For example, Iowa amended its HIV confidentiality statute in 2012 to explicitly permit data sharing with other states and federal agencies that have a need for the information for activities related to HIV prevention, disease surveillance, or care.[19] Prior to the 2012 legislation, the health department lacked legal authority to share data with other state agencies, even for duplication review, and was unable to report data to CDC. The change allowed the Iowa health department to engage in interstate data sharing for data-to-care efforts and other purposes.

Maryland, Virginia, and Washington, D.C. have implemented comprehensive cross-jurisdictional data-sharing activities pursuant to broad statutory authority. Maryland's laws and regulations pertaining to HIV data confidentiality include broad authority for sharing HIV surveillance data with "other governmental agencies" if the secretary of health determines that the agency receiving the data will maintain its confidentiality.[20] Virginia's regulations broadly require the state health department Office of Epidemiology notify other jurisdictional health departments of reported illnesses in their residents.[21] Washington, D.C.'s regulations broadly authorize sharing of HIV-related data for public health and surveillance purposes.[22] These jurisdictions relied upon these broad legal authorities in developing a local "Black Box" data exchange process and other written data-sharing agreements to deduplicate HIV data on a quarterly basis and obtain updated surveillance, care, and case management-related information for out-of-jurisdiction residents identified in a cluster.

STEP 3: ASSESS ETHICAL CONSIDERATIONS FOR CROSS-JURISDICTIONAL DATA SHARING, PARTICULARLY FOR PEOPLE WHO USE DRUGS.

Given the heightened stigma related to drug use, particularly injection drug use, HIV transmission, and their intersection, there is a need to evaluate potential ethical considerations related to data sharing when developing cross-jurisdictional guidelines. This is especially true for smaller, rural jurisdictions where identification of an individual who has acquired or been exposed to HIV related to their drug use behavior or network may make that individual subject to harmful privacy infringements, increased community stigma, and potential interference or surveillance from law enforcement entities. Throughout our research with Kentucky, Ohio, and West Virginia, individual privacy, especially in smaller communities, was raised as a major concern.

One major consideration is the extent to which data shared across states, or even across jurisdictions within a state, includes personally identifiable information. Even where legal authority for data sharing is broad, legal counsel may advise and health departments may operate under a principle of "limited release," releasing only what is necessary for specified surveillance or cluster response activities. For example, cross-jurisdictional data sharing of aggregate HIV or viral hepatitis surveillance data would be useful for awareness and increased need for communications related to the identification of emergent clusters and triggering cross-jurisdictional outbreak response teams and communications. On the other hand, sharing client-level identifiable or de-identified data with neighboring jurisdictions might be particularly useful for disease intervention specialists (DIS) and cluster response activities. Data-sharing

[19] 2012 Ia. Legis. Serv. Ch. 1113 (H.F. 2464) (amending Iowa Code Ann. § 141A.9).
[20] Md. Code Ann., Health-Gen. § 18-207(b)(3); Md. Code Regs. 10.18.02.09(C)(3).
[21] 12 Va. Admin. Code 5-90-90(E).
[22] D.C. Mun. Regs. tit. 22-B, § 206.5.

agreements with other jurisdictions and internal health department data-sharing policies should consider the public health activities that data exchange is intended to support, and the types of data needed for those activities, and delineate mechanisms for sharing data and maintaining confidentiality.

The data-sharing agreements and structures described in this resource are limited to HIV and viral hepatitis data, and do not include any extension to data pertaining to mental health, substance use, or behavioral health. Information related to these areas may be protected by additional state or federal laws that require written patient consent before release. While there are potential benefits to connecting systems of care that extend beyond infectious disease, this type of client-level care coordination should only be approached after a client is engaged in HIV or viral hepatitis care and gives informed consent for more comprehensive case management.

Also, it is imperative to create meaningful privacy protections and internal processes for sharing data related to HIV and viral hepatitis status and drug use with law enforcement entities.

Ensuring these protections are clearly stated and outlined in data-sharing agreements, and having a clear internal health department process for navigating requests for data from law enforcement or non-public health entities, will help jurisdictions avoid the disclosure of data that could result in the arrest and prosecution of individuals identified in an outbreak response or cluster investigation.

For example, in jurisdictions where statutory authority for data-sharing with law enforcement and courts does not explicitly limit the types of data that can be shared, health department staff that receive such data requests typically structure releases of data narrowly based on health department and legal counsel policies and procedures. Data release in the law enforcement context may be subject to additional layers of review within the health department, either by surveillance staff or legal counsel, prior to release, and requests are typically evaluated on a case-by-case basis.

STEP 4: ENGAGE LEGAL COUNSEL ABOUT LEGAL AND REGULATORY CONSIDERATIONS FOR EMERGING DATA-SHARING ACTIVITIES.

Partnerships between health department programs and public health legal counsel can be instrumental in facilitating data exchange between jurisdictions. Legal counsel can interpret jurisdictional legal authorities for, and limitations on, cross-jurisdictional data sharing, as well as work with health department staff to develop policies and procedures for ethical data sharing that supports cluster detection and response within the parameters of the law. Health department staff, in turn, can identify educational opportunities with public health legal counsel who may not be aware of the nuances of HIV surveillance technology and data.

In a state such as Kentucky, where the law broadly authorizes release of identifying information for the purposes of “consultation with state surveillance programs,” health department legal counsel can play an important role in reviewing proposed data-sharing activities. Legal counsel and health department staff can work together to develop workable standards and internal policies for data release that satisfy applicable state legal requirements and data privacy best practices, including federal guidelines such as

CDC's *Guiding Principles for Data Collection, Storage, Sharing, and Use to Ensure Security and Confidentiality*.[23]

Legal counsel can also support health departments in written agreements related to data sharing and use. Written agreements with other jurisdictions can address, among other things, the types of data to be shared, procedures for data exchange, data security standards, and the frequency and manner of data exchange activities. In jurisdictions where legal authorities for data sharing are broad and non-specific, written agreements can establish parameters on permissible data sharing and promote best practices. However, even where the legal authorities for data sharing are fairly narrow, health departments may still be able to execute written agreements to facilitate cross-jurisdictional data sharing. Specific data sharing and/or use agreements that include explicit terms, processes, and expectations for data exchange and confidentiality can allow health departments to engage in meaningful data-sharing activities while remaining consistent with state law and privacy best practices.

Kentucky, Ohio, and West Virginia reported relying on informal data exchange relationships with neighboring states, but health department staff in all states expressed interest in executing formal data-sharing agreements to establish standardized, routinized processes. All states reported that, absent formal written agreements, data-sharing relationships between health departments in different states may be vulnerable to changes in health department personnel. Other reported drawbacks to informal data exchange included lack of coordination between health department staff and supervisors, lack of consistency in data-sharing processes and outcomes, and overall lack of efficiency in non-standardized processes that tend to be labor-intensive and conducted on an ad hoc, case-by-case basis. At least one state's viral hepatitis program reported an inability to do any routine data exchange absent a written agreement, relying instead on secure email and phone calls to respond to occasional data requests. One state also expressed interest in using data-sharing agreements to coordinate HIV and viral hepatitis data exchange across state lines.

Formal, written agreements may lay a foundation for expanded data-sharing in the future. For example, prior to establishing the Black Box, Maryland, Virginia, and Washington, D.C. agreed to share surveillance data and entered into data-sharing agreements specifying the types of data to be shared, frequency of data sharing, security measures, and the format in which data would be transmitted. [24] Support from legal counsel was critical in executing these agreements, which were the precursor to eventual implementation of the successful Black Box system. Following execution of data-sharing agreements to facilitate the Black Box system, each jurisdictions' surveillance division provided nuanced input to plan for implementation.[25] The jurisdictions then established a Washington, D.C., Maryland, and Virginia (DMV) HIV Surveillance Group that included leadership of the three jurisdictions' HIV surveillance units, epidemiologists, eHARS data managers, and case surveillance coordinators, and scheduled monthly calls to plan and review progress.[26] A subcommittee of epidemiologists from each jurisdiction also met to develop specific procedures for data exchange, including data elements to be shared, the frequency of exchanges, and the validation of results.[27] Maryland, Virginia, and Washington,

---

[23] U.S. Centers for Disease Control and Prevention, *Ten Guiding Principles for Data Collection, Storage, Sharing, and Use to Ensure Security and Confidentiality* (last accessed: Apr. 26, 2021), https://www.cdc.gov/nchhstp/programintegration/tenguidingprinciples.htm.

[24] Hamp, et al., *supra* note 3.

[25] *Id.*

[26] *Id*.

[27] *Id*.

D.C. have since expanded their data-sharing agreements to include other types of data, such as HIV care and case management data. Additionally, these jurisdictions are exploring enhancing their existing data-sharing agreements to include data related to other infectious diseases.

The lack of specificity in most state data privacy laws additionally necessitates health department internal data-sharing policies and gatekeeping functions, which can be developed in consultation with public health legal counsel. Such internal policies may include reference to relevant state and federal data confidentiality protections, guiding principles for data use and prevention across health department HIV and STD programs, staff roles and responsibilities for safeguarding data privacy, circumstances and processes under which identifiable information may be released, data storage and security requirements, responding to inadvertent data breaches, and guidance and principles to inform health department practice when statutory authority for data-sharing is vague or broad.[28]

The partnership between health department programs and legal counsel should remain an ongoing, dynamic process. Policies and procedures should be revisited and adjusted to account for emerging community concerns about data privacy and use of surveillance data, advances in HIV surveillance technology, and changes in state laws or regulations.

STEP 5: IDENTIFY DATA PLATFORMS AND PROCESSES THAT ALLOW FOR SECURE DATA TRANSMISSION.

A formal agreement that defines a secure data platform is essential to successfully share infectious disease data related to routine HIV/viral hepatitis care coordination and cluster response. All parties should review and agree to the security measures in place for their respective data platforms (i.e., REDCap, MAVEN, or others).

In the case of the Maryland, Virginia, and Washington, D.C. Black Box data sharing arrangement, the jurisdictions consulted with their respective legal counsel and agreed on the security elements that would need to be present for a data platform to be considered adequately secure to house personal identified information, including HIV data. Surveillance staff, eHARS data managers, and other health department stakeholders in each jurisdiction then worked together to plan for implementation, which included identification of data platforms to which all jurisdictions would have access that met agreed-upon privacy and confidentiality standards.

Written data-sharing agreements between the jurisdictions included provisions related to processes using specified platforms and technology, the types of data to be shared, and guidelines and expectations on joint data entry. This example offers a tangible model and roadmap for other jurisdictions to replicate, and would have utility for jurisdictions experiencing, or at risk for, HIV outbreaks involving residents in multiple jurisdictions, including but not limited to outbreaks related to people who inject drugs. Depending on the jurisdiction, establishment of a system such as the Black Box may require collaboration between several stakeholders, including legal counsel, the health

[28] NASTAD, *supra* note 1.

department's office of information technology, HIPAA privacy and security officers, and database administrators.

STEP 6: MONITOR DATA-SHARING ACTIVITIES FOR PRIVACY COMPLIANCE, ASSESSMENT OF EMERGING ISSUES, AND POTENTIAL NEED FOR MODIFICATIONS IN DATA-SHARING PROTOCOLS.

As with any public health system, program, or protocol, it is important to consider sustainability from the outset. Below are several distinct categories of considerations for public health staff to evaluate and incorporate as they plan to increase cross-jurisdictional data-sharing. In addition, routine monitoring and evaluation of data-sharing activities and protocols should be conducted to ensure they are still accomplishing intended purposes of promoting care engagement and dialogue between jurisdictions on emergent or timely issues.

Legal and Ethical Considerations

Legal authorities related to data privacy and confidentiality in general, and cross-jurisdictional data-sharing in particular, are subject to change. Legislatures may add, expand, or limit data-sharing authorities through new legislation, and public health regulations may be altered through administrative rulemaking. Even if statutes and regulations do not materially change, public health legal counsel interpretation of legal authorities may change over time. Health departments should monitor the evolving legal landscape in their jurisdictions and work closely with public health legal counsel to ensure written internal policies and data-sharing agreements account for emerging community concerns about data privacy and use of surveillance data, advances in HIV surveillance technology, and evolving public health practice.

Health departments have a duty to ensure that data-sharing activities are not only legal, but also ethical. Strategies and legal interpretations related to data release must balance maximizing community trust with ensuring that the data shared is meaningful and significant enough to promote public health. A narrow statute authorizing data release only in limited enumerated circumstances may facilitate ethical data-sharing by reducing uncertainty about legally permissible activities. Explicit, specific data protections codified in state law can also strengthen community trust by promoting transparency about how personally identifiable data is collected and shared. However, overly narrow statutes may be too inflexible to account for disease surveillance advances, emerging community concerns about data privacy, and development of innovative public health strategies for disease control and prevention.

Broad statutory authorities are, on the one hand, more adaptable to advances in technology and public health practice. Health departments may adopt a more dynamic interpretation of legal data-sharing authorities that evolves over time and is informed by agency expertise and community input. On the other hand, overly broad or ambiguous statutes may deter data-sharing absent administrative regulations, sub-regulatory guidance, and/or health department internal policies setting forth clear standards, requirements, and ethical considerations. Additionally, while community engagement should be an essential component of all efforts to expand communicable disease surveillance and data-sharing, broad statutory approaches may exacerbate existing community concerns that personally identifiable surveillance data is not adequately protected and require a heightened level of community engagement.

Infrastructure Considerations

All health department staff interviewed or consulted for this project identified data systems and infrastructure as key considerations in engaging in meaningful cross-jurisdictional data-sharing. Health department staff can work with legal counsel to identify data-sharing platforms and modes of communication that meet applicable privacy and security standards in their jurisdiction, and incorporate use of such platforms and modes of communication into written data-sharing agreements. Health departments may also consider which stakeholders beyond legal counsel, such as HIPAA privacy and security officers, would need to participate in evaluating proposed data-sharing activities and ensuring any technology used meets all applicable state and federal privacy requirements. Data-sharing agreements can also address which jurisdictions will house and maintain the agreed-upon platforms, if needed.

Evaluation of current data-sharing infrastructure that exists within the health department, and evaluation of any additional infrastructure needs and resources available to support it, is critical to long-term sustainability and maintenance of cross-jurisdictional data-sharing activities. Within this evaluation, it might be useful to examine data systems and platforms already in place within the health department, such as systems used by DIS, partner services, or viral hepatitis programs. Alignment of these systems might allow for increased and streamlined data-sharing for several different health services and public health functions. While data-sharing for these other comorbidities were outside the scope of this project, all jurisdictions interviewed indicated that increased ability to share multiple types of data across borders would be extremely useful.

Staffing Considerations

Creating and maintaining a sustainable staffing structure for routine or ongoing interstate data-sharing activities was a common concern among health department staff interviewed for this project. Sustainable staffing structure is important not only for data-sharing in general and cluster response in particular, but also for other day-to-day program operations. Health department staff consistently identified staff turnover and internal transitions in staff roles and responsibilities as significant challenges to enhancing data-sharing efforts, especially given the more informal phone and secure-email based data-sharing states currently rely upon for outbreak and cluster response. All states reported that, absent formal written agreements, their interstate data-sharing activities primarily rely on existing relationships with individual staff in state and local health departments and are therefore vulnerable to staffing changes.

Jurisdictions considering increasing data-sharing activities can establish clearly defined roles, responsibilities, and protocols in internal health department policies and data-sharing agreements. Jurisdictions can determine appropriate health department points of contact for cross-jurisdictional data-sharing activities based on staff positions instead of relying on specific individuals to fulfill this role, and further consider having multiple points of contact.

Establishing such documented policies and protocols, and ensuring consistent adherence to them, relies on mutual staff and leadership buy-in at all levels of the health department structure. Staff may therefore need to advocate internally for adequate allocation of health department resources towards these efforts. Maintenance and monitoring plans for review of data-sharing protocols, staffing, and infrastructure, both between jurisdictions and internally, is essential to ensure long-term sustainability, ability to respond to emerging data-sharing activities, and program readiness for urgent data-sharing needs during an active cross-jurisdictional outbreak or cluster investigation.

CONCLUSION

In response to ongoing and emergent HIV clusters and outbreaks, as well as routine surveillance activities for HIV and other communicable diseases, there has been a growing need for increased data sharing between public health systems of neighboring jurisdictions. During the interviews conducted with health department staff, participants emphasized that informal data-sharing processes rely on existing relationships with state and local health departments in other states and are therefore vulnerable to change in health department personnel absent formal written agreements and established internal policies.

This resource outlines legal, practical, and ethical considerations to support the creation and adoption of sustainable, streamlined, and effective mechanisms for cross-jurisdictional data-sharing. While this resource was informed primarily by current data-sharing efforts in several jurisdictions that have recently experienced HIV clusters near state borders among networks of people who inject drugs, a broader analysis of cross-jurisdictional data-sharing models, promising practices, and lessons learned is included as well. This broader perspective provides considerations for jurisdictions seeking to improve their outbreak detection, response, and preparedness measures.