NASTAD

HIV Data Privacy and Confidentiality

Legal & Ethical Considerations for Health Department Data Sharing

A Ten State Analysis

JUNE 2018

Introduction

Use of health information technology to improve efficiency and coordination in the healthcare system continues to accelerate. At the same time, evidence-based and innovative public health data-use and data-sharing practices have emerged that allow health departments to more effectively leverage both public health and healthcare systems data to inform action. Governmental public health programs are using a range of program data, claims data, and encounter data to:

- Better assess HIV prevalence, health outcomes, and care coordination in their jurisdictions by querying claims and encounter data from payers and providers
- Clean data and address syndemics via matching with vital records and other public health databases
- Assess and address gaps in utilization and retention in care, through data-to-care activities
- Assess and respond to outbreaks using viral genetic sequencing data ("molecular HIV surveillance")

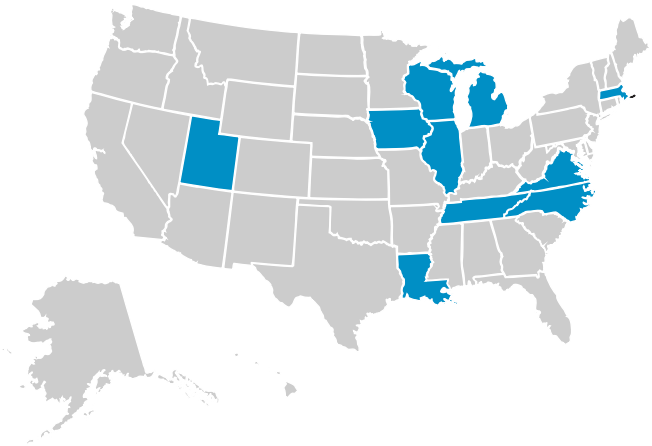
However, these emerging data-use and data-sharing activities raise questions about data privacy and confidentiality protections and the ethical uses and sharing of personally identifiable data.[1] The fact that HIV surveillance data is, by and large, collected without explicit patient consent for enumerated data uses triggers additional ethical considerations for how health departments use and share this data. Data-sharing protections and limitations are important not only to inform emerging public health data-sharing activities, but also to restrict data sharing for non-public health purposes, such as criminal HIV exposure and transmission prosecutions. To better assess how state-level legal and regulatory protections that govern HIV privacy and confidentiality apply to a range of data-sharing activities, NASTAD undertook a research project to assess the following:

1. What is the extent to which state laws and regulations permit or compel health departments to share personally identifiable HIV data with various entities?
    - With whom can health departments share this data (e.g., other health department programs, state agencies, providers, law enforcement, or researchers)?
    - For what purposes can this data be shared?
    - What are the limitations on the scope of data that can be shared?
2. What are the health department gatekeeper functions for release of patient data (e.g., written policies, internal checks, patient consent requirements)?
3. How are communities engaged in the discussion around emerging data-use and sharing activities?

This paper outlines NASTAD's findings and includes recommendations for how health departments can balance patient privacy considerations as data-sharing activities become more complex. For questions, please contact Amy Killelea or Dori Molozanov.

Methodology

NASTAD focused our research on the ten states below (Illinois, Iowa, Louisiana, Massachusetts, Michigan, North Carolina, Tennessee, Virginia, Wisconsin and Utah).



These states were chosen to reflect geographic diversity as well as variation in the types of health department data-sharing activities occurring.

NASTAD conducted research for this project in three phases.

Phase one consisted of a review of the statutes and regulations governing HIV data privacy in the ten focus states.[2] NASTAD used a commercial legal database to conduct this research, assessing both HIV-specific statutes and regulations as well as statutes and regulations pertaining to communicable diseases more broadly as they are applied to HIV.[3]

Phase two consisted of collection and review of health department written policies governing HIV data sharing and privacy and confidentiality, including published guidelines and data-sharing agreements.

Phase three consisted of stakeholder interviews with relevant health department staff to discuss interpretation of statutes and regulations and how data-sharing activities were operationalized. Health department staff participants included the designated NASTAD Member (formerly referred to as the AIDS director), surveillance coordinators, Ryan White Part B directors, AIDS Drug Assistance Program (ADAP) coordinators, prevention coordinators, and legal counsel.

A **database** of NASTAD's legal research is available, including the state laws and regulations on which we based the findings included in this paper.

Key Findings

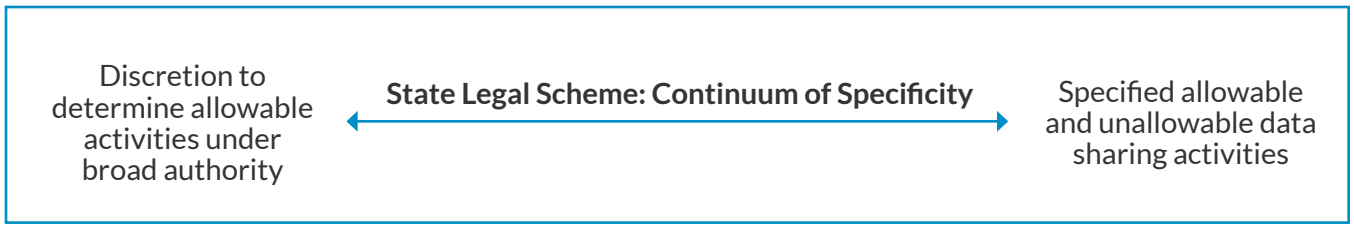
A number of themes emerged from our research that may inform how health departments, federal partners, policy makers, and other stakeholders approach these new and complex data-sharing activities in ways that safeguard patient privacy. These findings are discussed in detail below.

Internal Health Department Policies and Procedures Are Critical to Safeguarding Privacy

Provisions governing health department HIV data sharing were primarily found in HIV-specific statutes and regulations. We included analysis of statutes and regulations applicable to communicable diseases more broadly when there was no relevant HIV specific statute or regulation. In general, statutes provided health departments with authority to disclose personally identifiable HIV data without consent for the following general purposes:

- Surveillance, investigation, or control of communicable disease
- Treatment, payment, research, or healthcare operations
- Justifiable public health need

Within this broad statutory authority, a few states enumerated specific allowable and unallowable health department HIV data-sharing activities (particularly for data sharing related to law enforcement and research). However, the vast majority of statutory schemes used more general language giving discretion to health departments and their legal counsel to act under fairly broad authority as long as the statute's purposes were met. This lack of specificity in state laws places great importance on health department internal data-sharing policies and gatekeeping functions.



Health departments indicated that they relied heavily on the Centers for Disease Control and Prevention (CDC) 2011 guidance, *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs* to inform data privacy and security standards.[4] Several health departments had also adopted their own guidelines applicable to HIV data. Health department policies regarding privacy and confidentiality include the following:

- Reference to any relevant state and federal legal HIV data confidentiality protections
- Guiding principles for data use and protection across HIV surveillance, care, prevention, and STD programs
- Staff roles and responsibilities for safeguarding data privacy and confidentiality, including standards for minimum necessary access
- Circumstances and processes under which personally identifiable data may be released
- Data storage and security requirements
- Guidance and principles to inform health department practice when statutory authority for data collection is vague or broad
- How to handle inadvertent data breaches

Pursuant to the federal CDC data privacy guidance as well as state-specific guidance and procedures, all health department staff accessing sensitive HIV data undergo comprehensive data privacy and confidentiality training before accessing sensitive data.

In addition, when legal and statutory provisions leave flexibility for interpretation, legal counsel working directly with public health programs play a pivotal role in reviewing many proposed data sharing activities.

Health Department Approaches to Emerging Data-Use and Data-Sharing Activities Vary

The combination of broad statutory and regulatory authority and the variation in health department interpretation has meant that data-sharing activities vary depending on the jurisdiction. The following section discusses the different ways that state legal schemes address emerging data-sharing activities and the different ways states have approached these activities. Our focus is on the circumstances under which health departments may share personally identifiable HIV data (primarily HIV surveillance data) without a person's consent.

DATA-TO-CARE ACTIVITIES

Data to Care is a relatively new public health intervention using HIV surveillance data to identify individuals in need of HIV medical care or other services and facilitating linkage to those services. Because the intervention turns on using and sharing HIV surveillance data across HIV health department programs (e.g., between surveillance and Ryan White care programs) and with providers outside of the health department, implementation of data-to-care activities have necessarily involved data privacy and confidentiality considerations.

While there was some variation in how the ten focus states implemented data-to-care activities, we were able to identify some common themes:

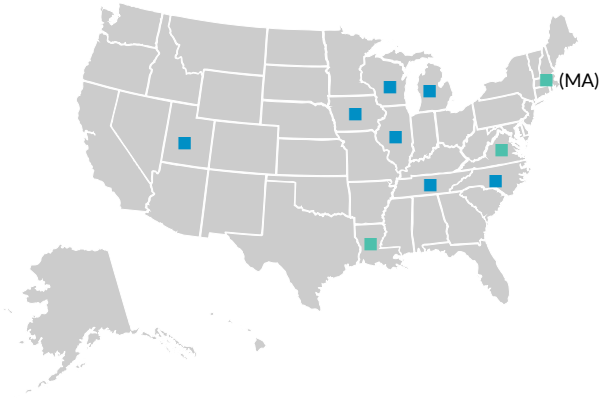
- Data sharing between HIV surveillance and Ryan White care programs or local health departments to better identify individuals who were out of care is a key aspect of data-to-care programs. In the vast majority of states, this type of intra-health department data sharing is occurring as part of regular health department public health activities without the need for a formal data sharing agreement. Only one state, Iowa, had executed a data sharing agreement between its surveillance and Ryan White care programs. Legal authority allowing this type of data sharing across health department HIV

programs is generally derived from broad authority to share data to operate a public health program, except in three states (IA, MI, and UT) where there is specific statutory authority to share data across programs within the health department.

- Data sharing with entities outside of the health department is more complex to navigate and varies among states based on the specificity of state statutes and regulations as well as health department data gatekeeping functions (see figure 1).
- The CDC data sharing privacy and security guidelines discussed above as well as health department internal policies and staff training have been important to ensure policies and procedures are in place to protect sensitive data.

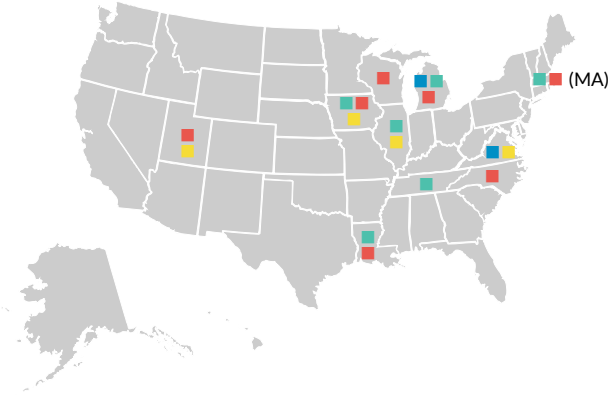
FIGURE 1: Relationship of Statutory/Regulatory Data Sharing Provisions to Health Department Surveillance Data Sharing with Providers for Data-to-Care

Statutory/Regulatory Schemes



- Explicitly permits sharing data with providers for treatment purposes
- Does not explicitly permit sharing data with providers (sharing may still be authorized under other laws)

Health Department Privacy Practices Limiting Who Uses Surveillance Data for Linkage Activities



- Share surveillance data (including viral load and CD4 count) with treating medical providers
- Match provider out-of-care patient list with surveillance data and share limited information back to the authorized provider (e.g., "need for follow-up" or "no need for follow-up")
- Share surveillance data with health department staff, "designees," or "agents" (including, in some cases, DIS located at local health departments)
- Share surveillance data with clinical and non-clinical based organizations with whom the health department has a contractual relationship as long as data security protections are followed

MEDICAID DATA-SHARING ACTIVITIES

Increasingly sophisticated data-use and data-sharing abilities, combined with the Affordable Care Act's Medicaid expansion, have made data sharing with state Medicaid programs an important public health intervention. Several states (IA, LA, NC, VA, MI, and WI) had executed some form of data-sharing agreement with Medicaid at the time of our research, but the extent to which personally identifiable information is shared varied state to state. The states noted above executed data-sharing agreements with their state Medicaid programs to receive Medicaid beneficiary data (either the entire Medicaid file or only those with "HIV markers" determined by diagnosis and CPT codes), match that data with HIV surveillance program data, and provide aggregate information (and in one case, client-level data) back to Medicaid, such as the proportion of Medicaid beneficiaries who are virally suppressed.

In each state sharing any data with Medicaid, a formal data-sharing or data-use agreement has been required. These types of bi-directional data-sharing arrangements must clear two legal hurdles: the first are the privacy requirements that attach to HIV data held by the health department and the second are the privacy requirements that attach to data held by the Medicaid agency.

- Of the states with data-sharing agreements with Medicaid in which data is being shared with Medicaid, half have justified this data sharing under specific provisions in their legal schemes allowing for sharing of confidential data with other state agencies outside of public health to support prevention, care, and surveillance activities related to HIV (IA, LA, NC, and VA). Other health departments rely on broader legal authority to share data to protect the health of the individual, prevent further transmission, or diagnose and care for the patient, with no reference to other state agencies (WI) or with limited reference to other state agencies that do not include Medicaid (MI).
- State Medicaid programs are subject to both federal data privacy laws (including the Health Insurance Portability and Accountability Act) as well as state laws and regulations governing data privacy and security. Medicaid programs have typically justified sharing beneficiary information with the health department by citing quality improvement and a specific assurance that the sharing of this data benefits individuals receiving services under the Medicaid program. In one state (MI), the Medicaid program required Institutional Review Board (IRB) approval before Medicaid data could be shared. Importantly, even in states where the health department lacks the legal authority to share HIV data with Medicaid agencies, the health department may still be able to receive data from Medicaid because of the different legal authorities involved.

When the data-sharing agreement involves sharing any health department data with Medicaid, the security of HIV surveillance data is protected in several ways. First, many states choose to only share aggregate data with Medicaid. In addition, no state allowed external access to the HIV surveillance database, but instead provided limited data back to the Medicaid program after internal data matching and analysis. Finally, one state – North Carolina – has created an integrated data hub that includes data from HIV surveillance, ADAP/Ryan White, and Medicaid. The hub allows the health department to conduct internal data matching and analysis and limit the data shared back to reporting entities, including Medicaid.

At the time of our research for this report, only one state – Louisiana – was sharing personally identifiable surveillance data back to Medicaid Managed Care Organizations (MCOs) as part of a data-sharing arrangement and HIV quality improvement initiative with the Medicaid program (though several other states had determined legal authority existed for this type of data sharing and were considering implementation). Medicaid MCOs in Louisiana provide the health department with their beneficiary data files and the health department matches this data with HIV surveillance data. The health department then provides individual-level data on viral suppression back to each MCO for their enrollees only. This enables the MCO to develop targeted linkage and care coordination approaches to improve patient outcomes. The same legal justification that has allowed Louisiana to build its data-to-care program also provides the basis for this type of Medicaid data-sharing.

LAW ENFORCEMENT DATA-SHARING ACTIVITIES

Public health practitioners have a strong desire to reduce stigma against people living with HIV and promote community trust by limiting public health disclosures to law enforcement.[5] However, limited data is required to be shared via subpoena or court order for events like court-ordered testing, sexual assault or abuse, and criminal transmission or exposure prosecutions. All health departments have strong policies and procedures to reduce data shared with law enforcement to minimum necessary standards.

Every state except for Massachusetts provided explicit legal/regulatory authority for sharing health department HIV data for law enforcement purposes (Massachusetts is also the only state in our research group without an explicit HIV criminal transmission statute).[6] Since a key element of many of the HIV criminalization statutes that can trigger a request for health department data is that the accused individual knowingly transmitted HIV without disclosing his/her status, health department surveillance data is usually requested to prove that the person was diagnosed

with HIV as of a certain date.[7] Some states have modernized their criminal transmission statutes to take into account that someone who is virally suppressed cannot transmit the virus to others (for instance, Iowa and North Carolina have recently updated their laws). In states where a detectable viral load is an element of criminal transmission, health department viral load data may become more relevant for prosecutions. Data are requested from health departments via two mechanisms, a subpoena or court order. The distinction between a subpoena and a court order is important, with a court order carrying the extra requirement that it be issued by a judge or tribunal:

- **Subpoena:** A subpoena is a document issued by one of the attorneys involved in the case, a clerk of the court, or the judge presiding over a case and can be used to compel the production of medical records or other documents.
- **Court order:** A court order must be issued by a judge or tribunal, unlike a subpoena which can be issued by a third party. A court order can also be used to compel the production of medical records or other documents.

As described in the chart below, states vary on whether a subpoena or court order is required for the production of HIV data from a health department. Some states include the extra protection that any HIV-related information produced as a result of a subpoena or court order be reviewed, in camera, by a judge to weigh its probative value against the privacy considerations of the patient. The limitations on the types of data that can be shared by a health department in response to a subpoena or court order varied, as did the procedural requirements for determining if the justification meets the legal requirements (see figure 2).

The statutes and regulations governing health department data sharing for law enforcement purposes still leave a great deal of discretion when evaluating individual requests. Every health department that has fielded these types of court orders and subpoenas works closely with the health department's legal counsel before any data are disclosed. Legal counsel reviews the request to ensure it is made pursuant to state laws and regulations, and if a request is granted, ensures that disclosure is made pursuant to state laws and regulations, and that only a narrow subset of data is provided.

States that limit the data that may be provided to an "HIV test" or "HIV-related test" have relied on this statutory language to further limit disclosure to only data related to HIV diagnosis. However, even in states with broader statutory language around the types of data that can be shared, health department staff reported that releases are structured narrowly based on health department and legal counsel policies and procedures. These types of statutory distinctions in scope of data that may be released may become more relevant as the field of molecular HIV surveillance advances, particularly in creating specific restrictions on the ability to share any data outside of an HIV diagnosis, including any subsequent phylogenetic testing data. At the time of research, no state had yet discussed making any statutory, regulatory, or procedural changes related to law enforcement-related requests for health department HIV data, but many acknowledged this may be a consideration moving forward. It is important to note that the health department staff we spoke with for this project indicated that they receive very few requests to release data pursuant to a criminal prosecution.

FIGURE 2: Data Sharing for Law Enforcement Purposes

	Statute/ regulation?	Limitations on what data can be shared
IL	Yes	Pursuant to court order or subpoena, "information and records" related to HIV may be shared for prosecution under the Illinois HIV criminal transmission statute or to enforce Illinois Sexually Transmissible Disease Control Act (410 Illinois Compiled Statutes 325)
IA	Yes	Pursuant to court order, "HIV-related test"* may be shared following in camera proceedings. Pleadings must substitute a pseudonym for the test subject's true name (Iowa Code § 141A.9)
LA	Yes	Pursuant to court order, "HIV test result"‡ may be shared following in camera proceedings (Louisiana Revised Statutes § 40:1171.4)
MA	No	N/A
MI	Yes	Pursuant to court order or subpoena, "all reports, records, and data pertaining to testing, care, treatment, reporting, research, and [partner notification]" may be shared (Michigan Compiled Laws 333.5131)
NC	Yes	Pursuant to court order or subpoena, "all records and information" related to HIV may be shared; health department may surrender the requested records to the court, for in camera review, if necessary to make determination (NC General Statutes § 130A-143)
TN	Yes	Pursuant to court order, "all records and information" related to HIV may be shared (Tennessee Code § 68-10-113)
VA	Yes	Pursuant to any federal or state law (Virginia Code § 32.1-36.1)°
WI	Yes	Pursuant to a court order "HIV test"¶ results may be shared (Wisconsin Statutes § 252.15(3m)(d)(9))
UT	Yes	Pursuant to a court order or subpoena, "medical or epidemiological information" collected by the department may be shared with the courts for the purposes of enforcing the Utah Communicable Disease Control Act, which includes a criminal transmission provision (Utah Code § 26-6-27)

* *"HIV-related test" means a diagnostic test conducted by a laboratory approved pursuant to the federal Clinical Laboratory Improvement Amendments for determining the presence of HIV or antibodies to HIV. (Iowa Code § 141A.1)*

‡ *"HIV test result" is the original document, or copy thereof, transmitted to the medical record from the laboratory or other testing site the result of an HIV-related test, which is a test performed solely to diagnose HIV infection. The term "HIV test result" shall not include any other note, notation, diagnosis, report, or other writing or document. (Louisiana Revised Statutes § 40:1171.2)*

° *Where a state's statutes and regulations were silent as to whether a court order or subpoena is required before the health department may release data, we made the assumption that either of these mechanisms will suffice, pursuant to due process protections*

¶ *"HIV test" means a test for the presence of HIV or an antibody to HIV. (Wisconsin Statutes § 252.02(2m))*

DATA SHARING WITH RESEARCHERS

Deidentified dataset	A dataset that is stripped of all data elements that can identify an individual.
Identifiable dataset	A dataset that contains data elements that either alone or in combination with other data can identify an individual.
Partially identifiable or limited dataset	A dataset that has been stripped of most identifiable elements, but may include dates, geographic information, or ages.

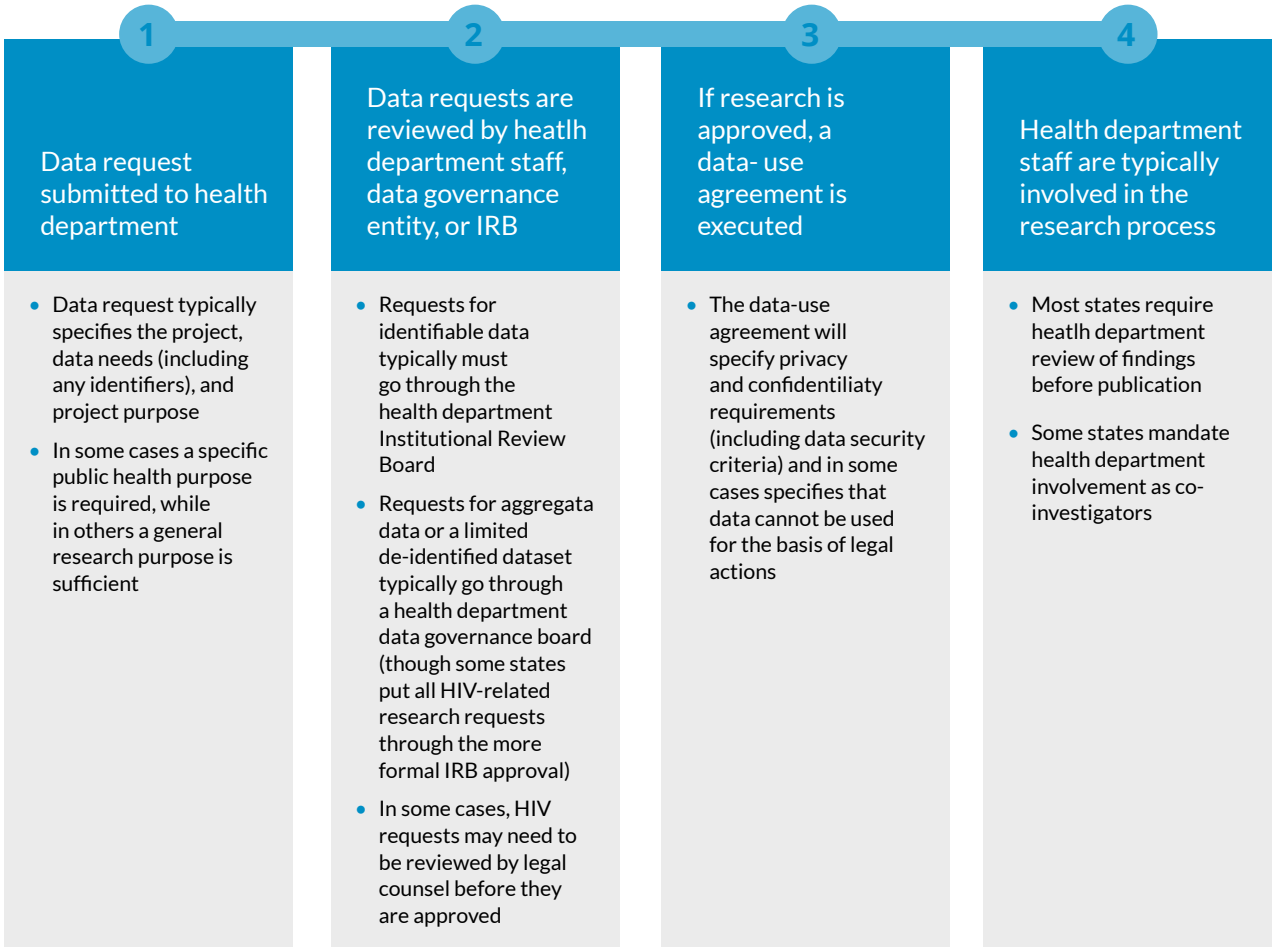
Collaborations between researchers and health departments have yielded important contributions to the HIV research field and the majority of the health departments featured in this paper reported excellent relationships and a long history of sharing de-identified data with local academic institutions and Centers for AIDS Research (CFARs). The legal authority to share data for research purposes varied, with states falling into the following categories:

- Only de-identified datasets may be shared for research purposes (IL, IA)
- Identifiable datasets may be shared for research purposes, but the publication must only include de-identified data (VA, WI)
- Identifiable datasets may be shared for research purposes (NC)
- Statute is silent as to sharing HIV data for research purposes (LA, MA, MI, TN, UT)

In states without explicit laws with regard to sharing data with researchers, the broader privacy laws governing HIV data sharing govern this situation. For instance, strict protections may preclude sharing of any identifiable data outside of the health department, including with researchers. Even in states whose statutes may allow sharing of identifiable data or are silent as to data sharing with researchers, in practice, health department internal policies often require that the data is de-identified. In North Carolina, for instance, even though identifiable data is allowed to be shared for research purposes under the statute, the health department has extensive procedures in place to ensure that these identifiers do not leave the custody of the health department (meaning any matching is done by researchers on health department servers, and only deidentified data are captured for analysis).

The processes that researchers must follow to request health department HIV data and assure that privacy and confidentiality protections will be strictly followed are detailed below in figure 3. While the process in each state is similar, there are some variations, including additional review and data security protections for requests involving HIV data. For instance, Iowa requires a separate level of review from health department legal counsel before any data is released for research purposes. Virginia includes a specific clause in its data-use agreement prohibiting data released for research purposes to be used for legal actions. This type of clause mirrors the National Institutes of Health (NIH) Certificate of Confidentiality (CoC) process, which prohibits disclosure of identifiable, sensitive information for any purpose not related to human subjects research.[8] Though not required, researchers not funded by NIH or another Department of Health and Human Services (HHS) agency may also request a CoC, and this may be advisable for research projects using particularly sensitive data, including molecular HIV surveillance data.

FIGURE 3: Health Department Data Research Requests Process



In addition to the procedures discussed above, in most jurisdictions, anyone using sensitive data for research purposes must undergo an accredited training program on privacy protections. Programs are often available online and include an overview of HIPAA protections as well as key provisions of the "Common Rule," the federal regulation governing human subjects research.

Community Engagement Considerations

In addition to our analysis of state laws, regulations, and internal health department policies, we also asked health departments to describe how they engaged and communicated emerging data-use and data-sharing activities with the communities they serve.[9] Every health department described meaningful community engagement as a critical component of both emerging data-use activities as well as overall administration of public health programs. The activities around data use and data sharing described by health department staff included the following:

- Provide communication and opportunity for feedback and discussion on data-to-care and other data-related activities through the state's community planning group
- Include data-related sections in the state HIV plan, commissioning a mix of community members and health department staff to discuss and develop this section

- Include emerging data-use and data-sharing considerations in community discussions surrounding state "ending the epidemic" initiatives
- Provide regular reports from the health department to community about data for public health action activities as well as opportunity for questions and discussion
- Include data updates and discussion at statewide HIV/hepatitis/STD meeting or other state and regional conferences convening individuals living with and affected by HIV as well as providers and other public health stakeholders
- Engage community advisory boards of large infectious disease clinics in data-use and data-sharing discussions
- Convene statewide task force, including consumers, to examine patient privacy issues
- Sponsor community engagement events with key informants and community advocates specifically seeking their input and help in encouraging community buy-in and trust

This list of activities is not exhaustive, and many health department staff we spoke with as part of our research indicated the need to increase meaningful community engagement opportunities in direct response to emerging molecular HIV surveillance activities.

Health Department Considerations

Because the speed at which HIV science and data technology are advancing far outpaces the speed at which laws and regulations are reviewed and updated, health departments play a critical role in continuously balancing data innovation with patient privacy and confidentiality concerns. The following are considerations for health departments as they tackle these complex legal, ethical, and programmatic data issues:

1. Health departments and other public health stakeholders should review their state's legal and regulatory scheme to determine what level of protections exist for HIV data, particularly with regard to sharing data with external entities, including providers, Medicaid and other payers, law enforcement, and researchers.
2. Health departments should be encouraged to develop or update internal guidelines and staff training for data sharing, data security, and patient privacy addressing emerging data sharing practices and privacy concerns (e.g., molecular HIV surveillance).
3. Health department HIV program staff should engage their legal counsel in conversations about legal and regulatory considerations for emerging data-sharing practices, including the legal protections for sharing viral load and molecular HIV surveillance data.
4. Most health departments already have robust policies and procedures in place to protect patient privacy when surveillance data is shared for research purposes. As molecular HIV surveillance data activities increase, health department staff may need to engage IRBs and other data governance boards to ensure they are aware of scientific advances and the ethical considerations for data-use and sharing activities involving genetic sequencing data.
5. Emerging data-use activities often involve balancing patient privacy and confidentiality with the goals of better improving public health activities and ultimately health outcomes for people living with HIV. Health departments may want to consider new ways to engage their community partners and stakeholders in conversations about the best way to balance competing priorities. This community engagement is particularly important in the context of molecular HIV surveillance, where the potential risks of disclosure of this type of data are not fully known.

Acknowledgments

This document was developed by Amy Killelea, Director, Health Systems Integration and Dori Molozanov, Manager, Health Systems Integration at NASTAD. NASTAD represents the chief governmental public health agency staff who have programmatic responsibility for administering HIV and hepatitis health care, prevention, education and support service programs funded by state and federal governments.

NASTAD would like to thank the individuals at the ten health departments highlighted in our research who generously gave their time and content expertise for the development of this report.

Murray C. Penner, Executive Director
Jacquelyn Clymore, North Carolina, Chair
June 2018

ENDNOTES

1. Fairchild, Amy L. et al. "Public Goods, Private Data: HIV and the History, Ethics, and Uses of Identifiable Public Health Information." Public Health Reports 122.Suppl 1 (2007): 7-15.
2. A database of NASTAD's legal research can be found here: https://www.nastad.org/sites/default/files/Uploads/2018/nastad-surveillance-laws-spreadsheet.xlsx.
3. We focused our research on state laws and regulations and considered analysis of federal laws, like the Health Insurance Portability and Accountability Act (HIPAA) and 42 CFR Part 2 (the federal regulation governing substance use data protections) to be outside the scope of this project. While all of the HIV surveillance programs we surveyed were in fact HIPAA exempt, both HIPAA and 42 CFR Part 2 were relevant for bi-directional data sharing, where the health department program was receiving personally identifiable data from another source (e.g., Medicaid). The following resource may be useful to determine when HIPAA compliance is necessary and the intersection of HIPAA and public health data: Centers for Disease Control and Prevention (CDC), "FAQs About HIPAA Privacy Rule," available at https://www.cdc.gov/nhsn/hipaa/index.html.
4. CDC, "Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action" (2011), available at https://www.cdc.gov/nchhstp/programintegration/docs/pcsidatasecurityguidelines.pdf.
5. NASTAD, "Understanding State Departments of Health and Corrections Collaboration" (2011) available at https://www.nastad.org/sites/default/files/resources/docs/decriminalization_findings_.pdf.
6. CDC, "State HIV Laws," available at https://www.cdc.gov/hiv/policies/law/states/index.html.
7. ProPublica has compiled an extensive database of HIV-related prosecutions. See ProPublica "How we Built Our HIV Crime Database" (2013), available at https://www.propublica.org/article/how-we-built-our-hiv-crime-data-set. See also Center for HIV Law and Policy, "HIV Criminalization in the United States: A Sourcebook on State and Federal HIV Criminal Law and Practice (2017), available at https://www.hivlawandpolicy.org/sourcebook.
8. National Institutes of Health, "Certificate of Confidentiality," available at https://humansubjects.nih.gov/coc/index.
9. The extensive work done by Project Inform and others to document community engagement best practices for data-to-care implementation is relevant to this discussion. See Project Inform, "Using Surveillance and Other Data to Improve HIV Care, Linkage, and Retention: A Report from a Think Tank Convened by Project Inform" (2012), available at https://www.projectinform.org/pdf/surveillance_0313.pdf.