NACCHO
National Association of County & City Health Officials
The National Connection for Local Public Health

25-01

STATEMENT OF POLICY

Data Strategy: Standardization, Governance & Confidentiality

Policy

The National Association of County and City Health Officials (NACCHO) strongly supports the development of data strategies that include standardization of public health data elements, alignment with nationally recognized data standards, and comprehensive data governance, defined as the framework of roles, responsibilities, policies, and procedures for managing and using data effectively and ethically, and data confidentiality practices across all levels of public health and healthcare infrastructure.

NACCHO advocates for the establishment of common data standards, strengthened interoperability, robust data leadership roles, and a culture of data ethics within local health departments. These practices are critical for ensuring data quality, safeguarding data confidentiality and privacy, and enhancing the effectiveness of public health programs nationwide.

General Recommendations

To implement effective data governance, confidentiality, and standardization, NACCHO recommends local health departments:

1. Adopt standardized data elements and definitions across systems, aligning with federal and state guidance where applicable.
2. Establish formal data governance roles, including a data governance lead and Data Governance Council.
3. Develop a comprehensive data strategy aligned with local and state priorities.
4. Invest in secure, modern IT infrastructure to support interoperability.
5. Provide ongoing workforce training in data ethics, privacy, and confidentiality practices.
6. Apply structured, ethical review processes for data sharing.
7. Enforce a Small Numbers Policy to protect privacy in small populations.
8. Monitor and evaluate data practices to ensure continuous improvement.
9. Engage national, state, and local stakeholders and communities to promote transparency and build trust.

By standardizing data elements, implementing robust data governance practices, and safeguarding confidentiality, local health departments can ensure that data serves as a powerful tool for advancing public health. These efforts will build stronger, more resilient communities,

foster trust among stakeholders, and empower timely, equitable responses to public health challenges.

Justification

Accurate, timely, and standardized data is the foundation of effective public health action. Local health departments rely on high-quality data to monitor health trends, manage outbreaks, allocate resources, and guide interventions. However, inconsistent data elements and a lack of structured governance can hinder this work, compromising local, state, and national public health goals.

Standardization of Data Elements

Standardization of data elements is essential to ensure consistency, accuracy, and interoperability across public health programs and systems. NACCHO supports alignment with nationally recognized standards such as USCDI/USCDI+ and PHIN, as well as the use of HL7 and FHIR standards to enable seamless data exchange between local, state, and federal systems.

These practices enable public health systems to respond more effectively during emergencies, support equitable service delivery, and strengthen public health's ability to protect and promote the health of communities at both jurisdictional and national levels. It allows for greater efficiency and collaboration within the public health sector as local health departments can share resources and best practices more easily when data are standardized.

Implementing clear data standards enhances data transparency by ensuring information is collected, reported, and interpreted consistently across systems and sources. This consistency allows public health professionals to confidently explain differences between datasets such as those from local, state, and federal levels based on methodology, definitions, or timing. When data users understand why numbers differ and how data are defined, it builds credibility and reinforces public trust. Standardized data not only supports accurate analysis and decision-making but also fosters openness and accountability.

By clearly defining and uniformly applying data fields such as date values (onset, report, specimen collection, event), geographic identifiers (jurisdiction, residence, death location), and classification types (vital statistics versus infectious disease), local health departments can improve data quality, reduce reporting errors, and streamline analysis.

Data Governance

Data governance provides the framework to manage public health data responsibly and effectively. It supports:

- Data quality: Ensures accuracy, consistency, and completeness of data collected and reported.
- Privacy and compliance: Protects sensitive health information and ensures adherence to ethical and legal standards.
- Operational efficiency: Reduces redundancy and streamlines data management and sharing processes.
- Trust and transparency: Strengthens partnerships with stakeholders and communities by promoting accountability in data use.
- Strategic alignment: Ensures data are available, usable, and aligned with public health priorities and objectives to plan interventions, manage outbreaks, and monitor health trends.

Key Data Governance Recommendations for Local Health Departments
To effectively implement data standardization and governance, NACCHO encourages local health departments to take the following steps:

1. **Establish Data Leadership Roles**
   Create formal roles and structures to oversee data governance. This may include appointing a designated data governance lead, establishing a Data Governance Council or Board, and designating data stewards within each program. These groups should include, at minimum:
   - A designated data governance lead
   - Program-specific data stewards
   - Information Technology (IT) staff
   - Legal and compliance officers
   - Data analysts and epidemiologists

   These roles should be scaled to the size and capacity of each department to ensure accountability, coordination, and consistent application of data standards and governance policies.

2. **Develop a Comprehensive Data Strategy**
   Data strategies can be broad encompassing all stages of the data life cycle, as well as components of governance, standardization, and compliance. Local health department authority over various stages and components of the data lifecycle can vary due to health department location, size, and governance structure. At minimum, a data strategy should provide a clear roadmap for data collection, use, and evaluation. This strategy can be integrated into the organization's broader strategic plan and informed by State or Community Health Needs Assessments and Improvement Plans. Alignment with CDC's Public Health Data Strategy, where applicable, can assist with data sharing with and interoperability with state and federal partners. It should define what data will be collected, how it will be used, and what outcomes are expected.

3. **Define Roles and Responsibilities**
   Local health departments should outline proper data use roles that can be assigned at the database or program level. Suggested roles include:
   - Data Architect: Designs and manages the local health department's data infrastructure.
   - Data Custodian: Manages technical control and access to the data, including its storage, security, and backups.
   - Data Owner: Holds accountability for a dataset and has the authority to make decisions regarding how the data is collected, shared, and used.
   - Data Steward: Oversees the quality and integrity of data and metadata over time, ensuring compliance with governance standards.
   - Data User: Accesses and utilizes data for analysis, reporting, research, or decision-making.

Some roles may be combined or held by the same person and terms may be used interchangeably.

4. **Implement Common Data Standards**
   Standardizing data fields, such as case dates, geographic identifiers, and classification categories ensures consistency across systems and jurisdictions. Use of common data standards facilitates trend analysis, reduces misclassification, and improves data sharing with partners such as hospitals, state agencies, and federal entities.

5. **Enhance Interoperability**
   Ensure that systems can securely and efficiently exchange data across platforms and partners. This may involve building or upgrading databases, developing shared data platforms, or using secure file transfer protocols to enable seamless integration of data from diverse sources.

6. **Bolster IT Infrastructure**
   Modern, secure infrastructure is necessary for electronic data exchange and cloud-based platforms. Continuous investments in software, hardware, and network systems are essential to support the safe and efficient handling of sensitive public health data.

7. **Foster a Culture of Data Ethics**
   Promote ethical data use through regular training and clear policies. Local health department staff should be trained in how to handle sensitive data with care, ensure privacy and confidentiality, and consider equity and transparency in all data activities. Training programs may include those developed by IRB, HIPAA, or other related certifications as per state and local policies.

8. **Apply Structured Decision-Making for Data Sharing**
   Establish a standardized review process to assess public and partner data requests. This may include a data request committee comprising governance leads and legal advisors. Consider the following when evaluating a request to share data:
   - Routine vs. non-routine requests
   - Alignment with public health goals
   - Departmental authority and capacity
   - IRB or Data Use Agreement requirements
   - Re-identification risks due to small numbers or identifiable information

Data Confidentiality

Protecting the confidentiality and security of public health data is a fundamental responsibility of local health departments. As public health agencies collect, store, and share sensitive information, it is essential to have clear policies and practices in place to safeguard personal privacy and maintain public trust.

Identifiers and De-Identified Data
To maintain data confidentiality, it is essential to recognize and appropriately handle identifying variables that can directly or indirectly reveal an individual's identity. The U.S. Department of Health and Human Services (HHS) defines 18 specific identifiers[1] that must be removed under the HIPAA Privacy Rule to achieve de-identification.

Direct identifiers include names, social security numbers, and full-face photographs, while indirect identifiers when combined can also compromise confidentiality. Examples include dates (birth, admission, discharge), geographic locations smaller than a state, or unique physical characteristics. All team members handling data must be trained to recognize both types of identifiers and apply safeguards.

De-identification is a process by which identifying information is removed or altered to reduce the risk of subject re-identification. To be compliant in de-identification, all 18 identifiers listed under the HIPAA Privacy Rule must be removed from the data set, consistent with established guidance on data confidentiality and privacy.[1,2] This may involve removing direct identifiers, aggregating categories, masking or truncating dates, and generalizing geographic data. Statistical techniques, such as data perturbation or k-anonymity, may also be applied. All de-identified data must be reviewed for compliance with privacy laws and only shared once the risk of re-identification is deemed acceptably low by the data governance body. Shared data must follow both the policies of the partner organization and the local health department.

Protected Health Information (PHI) and Personally Identifiable Information (PII)
Protected Health Information (PHI) refers to individually identifiable health information transmitted or maintained in any medium. PII includes data that can directly or indirectly identify an individual, even if it is not health related. Local health departments must handle both PHI and PII with the highest security and confidentiality, ensuring compliance with federal and state laws. Access should be limited to personnel with a legitimate need to know.
Local health departments face ongoing security threats due to the sensitive nature of the data they collect and maintain. The HIPAA Security Rule, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, requires covered entities, including local health departments, to maintain reasonable and appropriate administrative, physical, and technical safeguards for the security and integrity of PHI and PII against reasonably anticipated threats or hazards.[3] Local health departments must implement HIPAA and HITECH-compliant safeguards and ensure staff compliance with this rule. Additional security measures may be necessary for local health departments to mitigate specific risks and comply with additional local or state laws and regulations.

Small Numbers Policy
To further protect confidentiality, especially in small communities or specific subpopulations, health departments should follow a Small Numbers Policy when releasing data. This policy restricts public release when the number of cases, events, or individuals is so small that it could lead to identification. Local health departments' policies may vary based on the size of the population served and per condition based on prevalence and risk to the community or a specific subpopulation.

General guidelines for small number include:

- Suppressing data counts of fewer than 5 individuals in public reports or presentations, consistent with national recommendations on small numbers suppression.[4]
- Considering suppression of counts between 5 and 10 if re-identification risk is heightened due to small geographic areas or other potentially identifiable information.[4,5] This threshold is supported by standards from organizations such as the CDC's National Center for Health Statistics and the Agency for Healthcare Research and Quality, which recommend suppressing or masking small numbers in public data releases.[4,5]
- Applying suppression to totals or subtotals if back calculation from other cells could reveal suppressed numbers.

This policy maintains community trust, protects individual privacy, and ensures compliance with ethical and legal obligations.

References

1. Koo, D., & Wetterhall, S. F. (2011). Using data confidentiality in public health: Experience from the CDC. PLOS ONE, 6(12), e28071. Retrieved June 30, 2025, from https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0028071
2. National Center for Health Statistics. (n.d.). How NCHS Protects Your Privacy. Retrieved June 30, 2025, from https://www.cdc.gov/nchs/policy/how-nchs-protects-your-privacy.html
3. U.S. Department of Health and Human Services (2024). Summary of the HIPAA Security Rule, from: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
4. Centers for Disease Control and Prevention. (2022). Cautionary Notes Regarding Use of United States Cancer Statistics Public Use Database. Retrieved June 30, 2025, from https://www.cdc.gov/united-states-cancer-statistics/public-use/cautionary-notes.html
5. National Cancer Institute, SEER Program. (2022). Small Denominator Guidelines for Protecting Privacy in Public Data Release. Retrieved June 30, 2025, from https://healthcaredelivery.cancer.gov/poc/POC_Small-Denominator-Guidlines_2022-08-22.pdf

Record of Action

Proposed by NACCHO Epidemiology Workgroup and Informatics Workgroup Summer 2025
Approved by NACCHO Board of Directors September 2025