Information Governance for Public Health

February 2019

Public Health
Informatics Institute

Table of Contents

Introduction and purpose

As you identify your priorities and strategies for building an informatics-savvy health department, a critical area to develop or enhance is information governance. If an overall purpose of being informatics-savvy is to improve your health department's or program's use of information and information technology, then how you thoughtfully make decisions about the collection, management, uses, exchange and release of information is critical. That is what information governance is largely about, and why it belongs as a component of your informatics strategy roadmap.

The American Health Information Management Association (AHIMA) defines information governance as "an organization-wide framework for managing information throughout its lifecycle and supporting the organization's strategy, operations, regulatory, legal risk and environmental requirements." Information governance is thus an organizational-level approach to managing information that includes both legal and operational processes.

Information governance principles

In 2014, AHIMA published the *Information Governance Principles for Healthcare* which identified key principles for information governance for healthcare organizations. This guidance that follows "translates" and describes those principles in terms of governmental public health. Although healthcare and public health share many of the same values and imperatives when it comes to information, governmental public health agencies have unique legal and operational needs and obligations that are addressed in this document.

The principles as adapted for health departments are:

- ***The principle of accountability-*** An accountable member of senior leadership oversees the information governance program and delegates responsibilities for information management.
-

- ***The principle of*** transparency - The health department's processes and activities related to information governance are documented in an open and verifiable manner.
- ***The principle of integrity*** - The information governance program is constructed so the information generated by, managed for, and provided to the organization has a reasonable and suitable guarantee of authenticity and reliability.
- ***The principle of protection*** - The information governance program ensures that appropriate levels of protection from breach, corruption and loss are provided for information that is private, confidential, secret, classified, essential to business continuity or otherwise requires protection.
- ***The principle of compliance*** - The information governance program is constructed to comply with applicable laws, regulations, standards and organizational policies.
- ***The principle of availability*** - The health department has the ability to identify, locate and retrieve the information required to support its ongoing activities.
- ***The principle of retention*** – The health department maintains its information for an appropriate time, taking into account its legal, regulatory, fiscal, operational, risk and historical requirements.
-
- ***The principle of*** disposition – The health department provides secure and appropriate disposition for information no longer required to be maintained by applicable laws and the organization's policies.

Are data governance and information governance different?

Data governance is typically an IT responsibility and focuses on information storage and movement, and usually includes data security, data lineage, service levels, master data management and data loss prevention. Information governance focuses on maximizing the value of information to the organization while minimizing risks. Information governance presumes effective governance of data, since data are the building blocks of information. Information cannot be reliable and of organizational value if the data are not reliable.

The principle of accountability

The principle of accountability establishes who is accountable for the adoption and oversight of information governance practices, policies and procedures, and where responsibilities reside.

A member of the senior leadership team is ideally appointed to have overall accountability for information governance. But, as a practical matter, it makes sense to appoint a qualified and accountable staff person to oversee and coordinate the myriad operational details of developing and maintaining an information governance program. The information governance coordinator would report directly to the designated senior leader on the information governance activities.

Key activities and considerations

- Appoint a member of the senior leadership team to have overall accountability for information governance.
- Appoint an information governance coordinator to oversee and coordinate the development, implementation and evaluation of an information governance plan.
- The responsibilities of the coordinator might include:
  - Developing and maintaining the information governance strategy and related documentation.

    - Ensuring there is awareness of and support for information governance resources and implementation among senior leadership and management.
    - Establishing and documenting the principles and processes that will govern the program.
    - Providing direction and support for developing, implementing and promoting information governance policies.
    - Establishing working groups as needed to coordinate the activities of staff given information governance responsibilities and progress initiatives.
    - Ensuring annual assessments of information governance policies and activities that are completed, documented and reported to senior leadership.
- Information governance should be established throughout the health department, using a collaborative approach, with clearly defined roles and responsibilities (and training) for all staff who manage information at any level.

The principle of transparency

The principle of transparency establishes that organizational processes and activities related to information governance are documented and available for sharing/verification within legal or regulatory limits.

Documentation on how information is managed and governed should be accessible to health department staff and other interested parties while adhering to legal and administrative restrictions. It should include definitions of appropriate uses of information based upon their classification in statute, e.g., private, public, non-public, etc. The documentation should address the structure (how it is organized) and processes and practices (how things are done) of the information governance program.

The information governance records may be of interest to clients, elected officials, auditors, litigants and the general public. Although the records may vary in complexity depending on the health department, it is still important that the records are understandable and available to interested parties if requested.

Key activities and considerations

- Explore your state's data practices law and rules for those aspects that relate to information governance. While you may be most familiar with aspects related to confidentiality and allowable uses, other provisions likely relate to record retention, allowable charges for access to data, management of back-ups and other provisions.
- This and other principles assume you know what data sets and information is held by the health department. This may require an inventory to identify the data sets, data stewards, etc. See www.phii.org/PHI-Toolkit for one approach to conducting such an inventory.
- Likely roles for an information governance coordinator include:
  - Documenting the structure, principles, relevant laws and rules, processes and practices that govern the program.
  - Accurately and completely recording the activities undertaken to implement the program.
  - Being available to interested parties in a timely and reasonable manner.

The principle of integrity

An information governance program ensures that the information generated by, managed for, and provided to it has a reasonable and suitable guarantee of authenticity and reliability. The principle of integrity speaks to the health department's obligation to provide *authentic, timely, accurate* and *complete* information to internal and external stakeholders.

Integrity of information would likely include elements such as adhering to health department policy and procedures, workforce training on information management and governance, defined attributes of reliable information, acceptable audit trails, reliability of systems that control information, and clear, well-established business processes to provide data to interested parties.

Health departments need to also determine their responsibilities for receiving, managing and sharing information received from other sources. This almost certainly involves establishing data sharing agreements but also having defined and documented business processes for acting on information requests from interested parties that protect privacy and are compliant with all state and federal relevant laws.

Key activities and considerations

- Apply information governance practices throughout the information lifecycle to ensure that information is managed as a routine course of business and to ensure integrity and compliance with accepted data quality standards.
- Establish processes for monitoring information systems for reliability of performance and risk management. This must be done by the health department even if a central IT office also has it as a responsibility.
- Likely roles for an information governance coordinator include:
  - Assembling and documenting the data quality processes and standards across programs in the department while looking for ways to standardize as much as possible.
  - Establishing appropriate/minimum audit trails and quality assurance processes to ensure the reliability of information.
  - Reviewing and updating as needed audit trail capabilities in the department's systems.
  - Determining IT's role in monitoring system performance reliability and determining what processes the department should put in place to ensure its satisfaction that risks to data quality are minimal.
  - Reviewing change control processes across the department's programs and their information systems, ensuring they adhere to project management best practices and minimize risk of data corruption, loss or poor quality.
  - Reviewing programs' use of health data standards to ensure data can be exchanged internally or externally and convey/retain its meaning with the receiving system. \

The principle of protection

Protection of data is likely the aspect of information governance that is most developed and mature in your health department. Certainly, long-standing traditions of protecting sensitive and confidential information is a hallmark of public health, while breaches of healthcare data have pushed information governance to the forefront for healthcare organizations.

The principle of protection applies from the moment a health department creates or obtains a piece of information, regardless of medium, until it is appropriately dispositioned at the end of its retention period. Given that most data and information in a health department is now digital, this means that every information system must be managed and governed with data protection in mind. This includes several dimensions:

- Access/login controls to software that houses confidential information, including rescinding or otherwise changing access privileges when staff transition to new duties or leave employment.
- Processes to ensure continued operation of information systems during period of disruption from natural or human causes.
- Policies and processes for final disposition of records/information, particularly of protected health information as defined by state statute or HIPAA.
- An audit program to ensure the policies and processes for protecting information are effective and are being adhered to.

Key activities and considerations

- The information governance framework should identify a senior lead for data protection, including compliance with data protection and privacy laws. This may or may not be a chief security officer or chief privacy officer.
- Data protection should be supported by staff skills, knowledge and experience across the health department.
- Likely roles for an information governance coordinator include developing and documenting the list of activities above.

The principle of compliance

Information governance must describe and ensure that internal controls are in place to ensure compliance with laws, rules, regulations, policies and program requirements. This is especially critical for protected health information on individuals, whether governed by federal or state law or both. Among the state and federal laws to include are those related to birth, death and adoption records; communicable diseases, with the special requirements for protecting HIV-related data; inspections; immunizations; and WIC, among many others.

The duty of compliance impacts information management and governance in that:

- Information management systems and processes should reflect that the health department's activities are conducted in an ethical, credible and lawful manner, adhering to all legal and regulatory requirements.
- The information management systems themselves need to adhere to legal and regulatory requirements, including security standards, use of health data standards, audit logs, etc.

Key activities and considerations

- Ensure policies adequately address the legal, regulatory or other requirements related to data entry, maintenance, use, sharing and disposition.
    - Ensure all programs that manage information, regardless of size, have such policies, preferably that mirror health department-wide policies.
- Assess data management risks in programs/information systems and develop risk mitigation strategies.
- Include security and other requirements into requests for proposal and contracts for commercial-off-the-shelf or other software systems.
- Develop staff training plans and content to ensure staff understand the legal and other requirements, and what constitutes compliance.

The principle of availability

This principle requires health departments to be able to retrieve data in a timely, accurate and efficient manner. This applies whether the information is for administrative/operational or programmatic/ population health purposes, and whether for internal or external uses. Timely information retrieval is more critical than ever, given the growing pressures for timely information for decision making and the trend toward "liberating" government-held information and "open government" policies. Being able to respond quickly and credibly to, for example, legislative or media requests is increasingly expected.

Given the growing volumes and variety of information held by a health department, accessing that information in the format needed may require retrieval across multiple electronic and paper-based systems, some of which may be external to the health department location or working with and through one or more vendors or central IT offices.

> ***"Metadata are the structured information that describe, explain, locate or otherwise make it easier to retrieve, use, audit, and manage information."***
>
> ***-AHIMA***

Key activities and considerations

- To facilitate availability, the health department could use metadata to index data across systems.
- Data should also be backed up routinely to reduce the impact of a disaster, system malfunction or data corruption. Data created with legacy hardware or software should also be reviewed to confirm the data can be accessed with current systems.
- Information should be backed up routinely to mitigate the effects of a disaster, system malfunction or data corruption. Practice restorations from back-ups should be performed at least annually, something which is seldom done.
- Information created with legacy hardware and software systems must be reviewed periodically to confirm that the information can be accessed with current systems.
- When systems are ready to be decommissioned, information with organizational value should be migrated to currently supported hardware and/or converted into a readable format for archival purposes.
- Given the sheer volume of data held by health departments, policies and processes should be in place to ensure obsolete data sets or information are appropriately dispositioned based on records retention requirements. This will help the remaining data to be more identifiable and accessible.

The principle of retention

A health department should have an information retention schedule (one likely already exists within your jurisdiction, but perhaps not specific to your health department and its information) that states what information must be retained and for what length of time. Retention decisions should align with the retention schedule established in statute or federal regulation, and the schedule should be reviewed and updated regularly.

Key activities and considerations

- Work with your privacy and/or security officer to research existing local, state and federal requirements for retention of information, including any minimum and maximum time specifications.
- Different classes of information can fall under different requirements, so ensure the retention schedule is being specifically applied to the various data sets/information being maintained, including financial and HR data.

- Periodic risk assessments should be conducted to evaluate the appropriate retention period for each information type, and the findings should be incorporated into the retention schedule.
- There may be operational value in retaining information beyond what the retention schedule requires. Such value is likely best determined by interviewing staff who are most likely to use/need the information.
- Retention laws or rules written during an age of all paper records should be carefully reviewed to understand how to comply with the requirements in an age of on-site and “cloud” digital storage.

The principle of disposition

A health department must provide secure and appropriate disposition for information no longer required to be maintained by the jurisdiction’s retention schedule or other requirements (see the previous principle). Disposition includes destruction or permanent changes in custody of data such as reorganization of programmatic responsibilities within or across agencies (including to central IT). Disposition may occur at the end of a retention period or when information is converted or migrated to a new system. In all instances, a health department should ensure that all versions and copies are accounted for during the disposition process, and the process should be documented.

Key activities and considerations

- Determine how data being migrated to a new system will be accounted for and appropriately dispositioned from the legacy system/media.
- Are there particular disposition requirements for birth and death registration data, particularly around adoptions? Given how birth records in particular can be used across a health department, how will birth record data related to a person’s birth mother be expunged from registries and other systems, including their backup systems?
- Determine how you will verify that data have been destroyed appropriately. If you contract for such disposition, ask how the company certifies that the data have been disposed of as you directed.