AHIMA
American Health Information Management Association®

AHIMA Policy Statement on Public Health

AHIMA's Position:

AHIMA supports the use of policy to ensure the soundest, most reliable, and responsible use of health information for public health. Health information (HI) professionals have extensive knowledge and expertise to contribute in developing these policies. To ensure public health is bolstered while protecting the privacy, confidentiality, and security of a patient's health information, AHIMA believes that public policy must:

1. **Encourage standards to ensure accurate and timely data are used for public health responses and initiatives.** As public health surveillance systems increasingly pull data from electronic health records (EHRs), policy must work to ensure that the health information in those records is accurate and timely to address public health needs. Surveillance systems must also ensure they have timely health data from a number of sources, including hospitals and health systems that participate in syndromic surveillance. The value of coded data should be acknowledged for public health initiatives, and accurate coded data must be prioritized to address public health needs.

2. **Fund public health infrastructure to improve interoperability and sharing of public health data.** Public health surveillance systems must be funded at an adequate level to ensure data is available in a timely manner to permitted public health agencies.

3. **Adopt modern technical standards and requirements to enhance interoperability, decrease unnecessary reporting duplication, and ensure data is consistent, comparable, and meaningful across the US and internationally.** Public health surveillance systems must encourage the adoption and implementation of modern standards, such as Fast Healthcare Interoperability Resources (FHIR), and deploy application programming interfaces (APIs) to strengthen interoperability and reduce duplicative work faced by healthcare organizations, which are often required to report the same data in different formats based on local, state, and federal requirements. Standards for data collection and reporting processes are needed to ensure data is consistent, comparable, and meaningful. Policy should also support the flow of public health information across borders to ensure robust and targeted public health responses.

4. **Enhance communication and transparency with patients.** Leveraging modern standards and new technologies may increasingly lead to public-private partnerships to conduct public health surveillance. Policy must ensure that data holders clearly and conspicuously communicate what information will be collected, maintained, and analyzed. They must also make clear how the data may be processed, disclosed, and shared, and whether the information will be de-identified.

5. **Protect patient privacy and security.** Policy must safeguard patient privacy, including the de-identification of data whenever possible; prohibit attempts at re-identification of de-identified public health data; encourage strong security, privacy, and confidentiality standards within any public health institutions or system; promote privacy protections for contact tracing initiatives; and offer methods to engage and inform patients on the use of

their patient health information. Policy should also promote appropriate data minimization and retention policies.

Background:

Public health response and planning in the US relies on accurate, standardized, timely, and accessible health information that can be used to protect the health of populations. Public health surveillance systems today are often viewed as antiquated and suffer from underfunded and outdated systems that delay responses to public health threats. Under-functioning public health systems put the public at risk of disease outbreaks, such as measles, pandemics, COVID-19, and chronic threats, such as the opioid epidemic.

One concern is the lack of standardization and incompatibility of public health data collected across different surveillance systems; across local, regional, and federal agencies; and across geographic borders. During the COVID-19 pandemic, data collected and reported across the US has been found to be inconsistent and incomplete, hampering health officials' ability to understand factors that place certain populations and communities at increased risk.[1]

While it is necessary to have a well-functioning, fully funded public health system, patient privacy must be protected and safeguarded. Current methods used by American public health departments to produce de-identified data sets are not always successful in preventing patient re-identification.[2] The CDC states that systems need to be modernized to ensure systems and data are secure.[3] Public health and patient privacy are compatible goals that can be met through clear policy guidance.

Key Points:

An improved public health surveillance system could result in considerable benefits, including:

- Improved health of populations throughout the US and globally including more rapid interventions and deployment of resources to "hot spots," and improved environmental and occupational health;

- Increased interoperability between systems, including between EHRs and public health surveillance systems;

- Faster federal, state, local, tribal, and territorial response to disease outbreaks and pandemics;

- Improved public trust in public health systems;

- Fewer inefficiencies that come from outdated and inefficient surveillance systems; and

- Improved patient privacy.

To realize the benefits of an improved public health system that relies on health information, certain challenges must be addressed, including:

[1] https://popcouncilcovid19research.org/us-equity-data
[2] https://www.emerald.com/insight/content/doi/10.1108/IJHG-11-2017-0058/full/html
[3] https://www.cdc.gov/csels/dhis/blogs/yoon-201611.html

- **Inaccurate and incomplete patient data in EHRs**. This includes patient misidentification due to the lack of a national strategy around patient identification. The rise in patient-generated health data is an additional challenge that must be addressed to ensure accurate and complete data in EHRs.

- **Inconsistent and duplicative data reporting requirements at the state and federal level.** Hospitals and other health organizations often face varying reporting requirements from local, state, and federal public health authorities, resulting in duplicative work and wasted resources.

- **Outdated and antiquated public health surveillance systems.** Lack of consistent and adequate federal funding across a number of public health surveillance systems, including the National Notifiable Disease Surveillance System (NNDSS), Electronic Case Reporting (eCR), Syndromic surveillance, the Electronic Vital Records System, and Laboratory Information Systems (LIMS) has created a system that is not timely, secure, or sufficiently expansive. This decreases the capacity of such surveillance systems to perform research and accurately respond to public health threats. Lack of sustained funding for public health surveillance systems has also left these systems less secure than they should be.[4]

- **Inadequate patient privacy and security protections in an increasingly digitized healthcare ecosystem.** The rise in artificial intelligence, including sophisticated algorithms and use of machine learning, has increased the risk that de-identified data stripped of identifiable demographic and health information could be re-identified.[5]

- **Inadequate and inconsistent data collection to address health inequities at the population level.** More complete, timely, and accurate public health data will provide policymakers with the opportunity to promote health equity in ways that are culturally respectful.

Current Situation:

A strong public health surveillance system is vital to protect communities across the US and internationally. Various systems at the state and federal level in the US track infectious diseases, non-infectious health conditions, risk factors, and exposures for public health threats. Without adequate support of these interconnected systems, response to public health threats are lacking and patient privacy protections may be insufficient.

In recent years, surveillance systems have become increasingly complex due to the adoption of electronic health records and digitization of health information. Expectations for near real-time data have added pressures to public health surveillance systems used by the federal, state, local, tribal, and territorial governments; however, funding for and upgrades to these systems have not kept pace with the needs and expectations of these systems.

In 2014, a push began to modernize the public health surveillance systems used in the US, specifically at the Centers for Disease Control and Prevention (CDC). Since 2014, there have been a number of advancements, including enhancements to cloud-based platforms; faster reporting of vital statistics data on influenza-related deaths; use of new electronic messaging in

[4] https://www.hhs.gov/cto/blog/2016/11/30/modernizing-our-public-health-surveillance-systems.html
[5] https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2719130

several states to simplify disease reporting to the CDC; an enhanced focus on data reporting for the opioid epidemic; and solicitations from stakeholders to inform new public health data strategies.

In 2016, a CDC initiative called Digital Bridge was founded to represent stakeholders from public health, the healthcare delivery system, and EHR vendors. This initiative created a forum for stakeholders to discuss challenges and find solutions on information sharing and the use of electronic health data, with a commitment to bidirectional information exchange between healthcare and public health. Digital Bridge was successful in creating a technical approach to electronic case reporting (eCR) that leverages existing EHRs to flag reportable disease cases and create a case report, which alleviates burdensome processes for healthcare professionals. As COVID-19 became a pandemic, the CDC responded with eCR Now, which allows for the rapid adoption and implementation of eCR for COVID-19.

In addition, Congress passed the Coronavirus Aid, Relief, and Economic Security (CARES) Act, a package to address the pandemic that included $500 million for the Data Modernization Initiative at the CDC. This funding is slated to be used to modernize public health infrastructure in the US.

While improvements have been made, investments are still needed to support public health in the US. Though reporting has increased in recent years, many system improvements are still lacking. For instance, only 63 percent of mortality records are collected electronically from states within 10 days. Only 60 percent of emergency department visits are reported electronically to health departments.[6] The CDC Health Information Innovation Consortium has noted that privacy and security are among its priority areas, but many awarded projects are still in their infancy and have not been integrated across all systems. Without strong and increased investments in these areas, our public health systems will continue to be overburdened and be unable to respond quickly and seamlessly to public health threats while protecting patient privacy.

AHIMA stands ready to contribute to the conversation around public health data and the modernization of our public health infrastructure.

[6] https://www.cdc.gov/surveillance/pdfs/Surveillance-Series-Bookleth.pdf