



Information sharing is the ability to conduct multijurisdictional, multidisciplinary exchange of health-related information and situational awareness data among federal, state, local, territorial, and tribal levels of government, and the private sector. This capability includes the routine sharing of information as well as issuing of public health alerts⁷⁶ to federal, state, local, territorial, and tribal levels of government and the private sector in preparation for, and in response to, events⁷⁷ or incidents⁷⁸ of public health significance.⁷⁹

This capability consists of the ability to perform the following functions:

Function 1: Identify stakeholders to be incorporated into information flow

Function 2: Identify and develop rules and data elements for sharing

Function 3: Exchange information to determine a common operating picture

Function 1: Identify stakeholders to be incorporated into information flow

Identify stakeholders within the jurisdiction across public health, medical, law enforcement, and other disciplines that should be included in information exchange, and identify inter-jurisdictional public health stakeholders that should be included in information exchange. Determine the levels of security clearance needed for information access across and between these stakeholders.

Tasks

This function consists of the ability to perform the following tasks:

Task 1: Prior to and as necessary during an incident, identify intra-jurisdictional stakeholders across public health, public safety, private sector, law enforcement, and other disciplines to determine information-sharing needs.

Task 2: Prior to and as necessary during an incident, identify inter-jurisdictional public health stakeholders to determine information sharing needs.

Task 3: Prior to and as necessary during an incident, work with elected officials, identified stakeholders (both inter- and intra-jurisdictional) and private sector leadership to promote and ensure continual connection (e.g., ongoing standing meetings, webinars, and teleconferences) and use continuous quality improvement process to define and redefine information-sharing needs.

Performance Measure(s)

At present there are no CDC-defined performance measures for this function.

Resource Elements

*Note: Jurisdictions must have or have access to the resource elements designated as **Priority**.*

P1: (Priority) Written plans should include processes to engage stakeholders that may include the following: ^{80,81}

- Law enforcement
- Fire
- Emergency Medical Services
- Private healthcare organizations (e.g., hospitals, clinics, large corporate medical provider organizations and urgent care centers)
- Fusion centers
- For states: local health departments, tribes and territories
- Individuals who have or may need a security clearance, based on functional role

Suggested resources

- FBI-CDC Criminal and Epidemiological Investigation Handbook:
<http://www2a.cdc.gov/phlp/docs/crimepihandbook2006.pdf>

Function 1: Identify stakeholders to be incorporated into information flow

Resource Elements *(continued)*

PLANNING (P)	<ul style="list-style-type: none"> - Joint Public Health Law Enforcement Investigations: Model Memorandum of Understanding, created by Public Health and Law Enforcement Emergency Preparedness Workgroup, CDC and Bureau of Justice Assistance: http://www.nasemso.org/Projects/DomesticPreparedness/documents/JIMOUFinal.pdf <p>P2: (Priority) Written plans should include a role-based public health directory that will be used for public health alert messaging. The directory profile of each user includes the following elements:⁸²</p> <ul style="list-style-type: none"> - Assigned roles - Multiple device contact information - Organizational affiliation <p>Suggested resource</p> <ul style="list-style-type: none"> - CDC’s Public Health Information Network: www.cdc.gov/phinf <p>P3: Written plans should include processes for stakeholder communication, including frequency of standing meetings and method for requesting additional meetings.</p>
EQUIPMENT AND TECHNOLOGY (E)	<p>E1: Have or have access to a database of public health department contact information updated quarterly.⁸³ The database may be paper-based or electronic.</p> <p>E2: Have or have access to equipment that may be needed to access information when clearances are required.</p>

Function 2: Identify and develop rules and data elements for sharing

Define minimum requirements for information sharing for the purpose of developing and maintaining situational awareness. Minimum requirements include the following elements:

- When data should be shared
- Who is authorized to receive data
- Who is authorized to share data
- What types of data can be shared
- Data use and re-release parameters
- What data protections are sufficient
- Legal, statutory, privacy, and intellectual property considerations

Function 2: Identify and develop rules and data elements for sharing
Tasks

This function consists of the ability to perform the following tasks:

- Task 1:** Prior to and as necessary during an incident, identify, through public health agency legal counsel (and counsel to other agencies and jurisdictions as appropriate), current jurisdictional and federal regulatory, statutory, privacy-related and other provisions, laws, and policies that authorize and limit sharing of information relevant to emergency situational awareness. Such laws and policies may include Health Insurance Portability and Accountability Act (HIPAA), Office of the National Coordinator Health IT Information Technology Policy, HHS Information Management Policy, and specific requirements of current memoranda of understanding and memoranda of agreements; these laws may address privacy, civil liberties, intellectual property, and other substantive issues.
- Task 2:** Prior to and as necessary during an incident, identify routine or incident-specific data requirements for each stakeholder.
- Task 3:** Prior to and as necessary during an incident, identify public health events and incidents that, when observed, will necessitate information exchange. *(For additional or supporting detail, see Capability 3: Emergency Operations Coordination)*
- Task 4:** Prior to, during, and after an incident, utilize continuous quality improvement or have a processes and a corrective action system to identify and correct unintended legal and policy barriers to sharing of situational awareness information that are within the jurisdictional public health agency's control (e.g., legal and policy barriers, opportunities to shorten the amount of time to share data).

Performance Measure(s)

At present there are no CDC-defined performance measures for this function.

Resource Elements

*Note: Jurisdictions must have or have access to the resource elements designated as **Priority**.*

PLANNING (P)

- P1: (Priority)** Written plans should include a listing of data-exchange requirements for each stakeholder (including the use of common terminology, definitions, and lexicon by all stakeholders) that adhere to available national standards for data elements to be sent and data elements to be received.
- P2: (Priority)** Written plans should include health information exchange protocols for each stakeholder that identify determinants for exchange and which may include the following elements:
- Unusual cluster(s) or illness that threaten closure of institutional settings (e.g., illness among healthcare workers or prisoners)
 - High burden of illness or a cluster of illness confined to a specific population (e.g., racial or ethnic group, or vulnerable populations)
 - Illness burden that is expected to overwhelm local medical or public health resources
 - A public health laboratory finding of interest (e.g., a novel virus identified by lab) that is not picked up clinically or through other surveillance
 - Large numbers of patients with similar and unusual symptoms
 - Large number of unexplained deaths
 - Higher than expected morbidity and mortality associated with common symptoms and/or failure of patients to respond to traditional therapy
 - Simultaneous clusters of similar illness in noncontiguous areas
 - Received threats or intelligence
 - Incidents in other jurisdictions that raise possible risk in home jurisdiction (e.g., elevation of pandemic influenza alert level)
- P3:** Written plans should include communications processes and protocols to communicate with identified stakeholders (e.g., intra-jurisdictional public health, inter-jurisdictional public health, medical, mental/behavioral health, and law enforcement).

Function 2: Identify and develop rules and data elements for sharing

Resource Elements *(continued)*

PLANNING (P)	<p>P4: Written plans should include memoranda of understanding or letters of agreement with agencies and stakeholders for participation and information sharing.</p> <p>P5: Written plans should include processes to ensure that the jurisdiction adheres to applicable state and federal constitutional and statutory privacy and civil liberties provisions (e.g., Information Control or Collection Plan).</p> <p>P6: Written plans should include processes and procedures for exchanging information when security clearances apply (e.g., when sharing information with the Federal Bureau of Investigation or state bureau of investigation).</p> <p>P7: Written plans should include documentation where and if state laws and regulations prohibit sharing of information to the federal level and inter-jurisdictionally.</p> <p>P8: Written plans should include processes and frequency for data exchange in both routine and incident-specific settings, including requirements for data exchange with CDC at a frequency as determined by the type of incident and phase of the incident, as well as jurisdictional standards.</p>
SKILLS AND TRAINING (S)	<p>S1: All public health personnel should receive awareness-level training in the pertinent laws and policies regarding information sharing and in procedures to assure adherence to them (e.g., transport of data and use of personal identifiable information).</p>
EQUIPMENT AND TECHNOLOGY (E)	<p>E1: Information systems should follow industry or national system-independent data standards as identified by CDC</p> <p>E2: Written conversions to convert non-standard formats or terminologies into federally accepted standards for communication</p> <p>Suggested resource</p> <ul style="list-style-type: none"> – CDC’s Public Health Information Network: www.cdc.gov/phin

Function 3: Exchange information to determine a common operating picture

Share information (both send and receive) within the public health agency, with other identified intra-jurisdictional stakeholders, and with identified inter-jurisdictional stakeholders, following available national standards⁸⁴ for data vocabulary, storage, transport, security, and accessibility.

Function 3: Exchange information to determine a common operating picture

Tasks

This function consists of the ability to perform the following tasks:

- Task 1:** Prior to and during an incident, collaborate with and participate in jurisdictional health information exchange (e.g., fusion centers, health alert system, or equivalent). *(For additional or supporting detail, see Capability 3: Emergency Operations Coordination)*
- Task 2:** Prior to and during an incident, maintain data repositories that are able to support data exchange with other regional and federal public health entities. Store data according to jurisdictional and/or federal standards for formatting, vocabulary, and encryption. *(State and local jurisdictions)*
- Task 3:** Prior to and during an incident, request, send, and receive data and information using encryption that meets jurisdictional and/or federal standards. *(State and local jurisdictions)*
- Task 4:** Verify authenticity with message sender or information requestor.
- Task 5:** Prior to and during an incident, if necessitated by the situation, acknowledge receipt of information or public health alert.

Performance Measure(s)

At present there are no CDC-defined performance measures for this function.

Resource Elements

*Note: Jurisdictions must have or have access to the resource elements designated as **Priority**.*

PLANNING (P)

- P1: (Priority)** Written plans should include a protocol for the development of public health alert messages that include the following elements:⁸⁵
- Time sensitivity of the information
 - Relevance to public health
 - Target audience
 - Security level or sensitivity
 - The need for action may include
 - Awareness
 - Request a response back
 - Request that specific actions be taken
- P2:** Written plans should include a process for information system development and maintenance⁸⁶ that take into account the following elements:
- Controls and safeguards for data access levels
 - Data structure definitions and specification of databases (structured/unstructured data). Structured healthcare data should utilize the latest applicable federal standards.
 - Ownership of the data
 - Data quality and data reliability
 - Security and privacy of patient health information as applicable
 - Consent, security, and privacy procedures
 - Access permissions, including data release and reuse agreements
 - Additional protections against data theft such as encryption, data loss, and back-up storage
 - Authentication service to authenticate requestors and data submissions from various locations
- P3:** Written plans for jurisdictions considering participation in an information exchange process such as a fusion center should address the following elements:
- Clearly defined intelligence requirements that prioritize and guide planning, collection, analysis, and dissemination efforts
 - Clear delineation of roles, responsibilities, and requirements of each level and sector of government involved in the fusion process

Function 3: Exchange information to determine a common operating picture
Resource Elements *(continued)*

Suggested resources

- Health Security Intelligence Enterprise Strategy: <https://cs.hsin.gov/HPH/default.aspx>
- Public Health and Medical Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers: <http://it.ojp.gov/documents/baselinecapabilitiesa.pdf>
- Integrating Health Security Capabilities into Fusion Centers: <https://cs.hsin.gov/HPH/default.aspx>

P4: Written plans should include processes that indicate how healthcare providers in the jurisdiction shall be able to exchange information with electronic public health case-reporting systems, syndromic surveillance systems, or immunization registries according to the Centers for Medicare and Medicaid Services (CMS) Electronic Health Record Incentive Program rules and any additional applicable federal standards.⁸⁷ This electronic sharing includes but is not limited to the following elements:

- Electronic sharing of laboratory test results
- Immunization registries
- Syndromic surveillance data

Suggested resources

- The Office of the National Coordinator for Health Information Technology: <http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3006&PageID=20401>
- CDC’s Public Health Information Network: www.cdc.gov/phin

P5: Written plans should include a process for verifying that received messages are from a trusted source.

P6: Written plans should include a process to acknowledge receipt of information and to be able to accept acknowledgement from stakeholders.

P7: Written plans should include a procedure in place that ensures that public health alert messages are received by multiple people, at least one of whom has responsibility to process the message 24/7/365.

P8: Written plans should include a public health alerting message template that includes the following elements:⁸⁸

- Subject or title
- Description
- Background
- Request or recommendations (action requested)
- Who to contact
- Where to go for more information
- Who it went to (e.g., specific roles)
- Different templates for every level of alert with different criteria for each
- Distribution method

P9: Written plans should include a template for Information Sharing Access Agreements via a memorandum of understanding, memorandum of agreement, or other letter of agreement with data-sharing partners, which should consider the following:

- Breach notification procedures, particularly if data is not stored in an encrypted state
- Maintenance of Health Insurance Portability and Accountability (HIPAA) Security Rule compliance, when potential Personally Identifiable Information must be shared

P10: Written plans should include a process for standardized electronic data exchange with partners according to information exchange standards established by Public Health Information Network.

Suggested resource

- CDC’s Public Health Information Network: www.cdc.gov/phin

Function 3: Exchange information to determine a common operating picture
Resource Elements *(continued)*
SKILLS AND TRAINING (S)

S1: Identify staff that meets jurisdictionally defined competencies for a Public Health Informatician as defined in Competencies for Public Health Informaticians -2009⁸⁹ (or updated versions of this document) to participate in health information exchange.⁹⁰

EQUIPMENT AND TECHNOLOGY (E)

E1: Have or have access to electronic systems capable of handling routine day-to-day information data transmission as well as emergency notification and situational awareness. When conveying personal health information or syndromic surveillance information the system should meet the following standards:⁹¹

- Federal standards and specifications, (e.g., messaging guides) when applicable⁹²
(For additional or supporting detail, see Capability 13: Public Health Surveillance and Epidemiological Investigation)
- Applicable patient privacy-related laws and standards, including state or territorial laws, and Health Insurance Portability and Accountability, Health Information Technology for Economic and Clinical Health, National Institute of Standards and Technology, and the Office of the National Coordinator standards such as:
 - Data must be encrypted during transit according to jurisdictional and, if available, national standards^{93,94}
 - Data protections based on the types of data shared such as:
 - All data exchanges should abide by the National Institute of Standards and Technology/Federal Information Security Management Act requirements for the integrity, confidentiality and availability appropriate for the data sensitivity level (e.g., low, medium, and high).
 - All communication containing health data (personally identifiable information and non-personally identifiable information) should take place over transport layer security/secure socket layers using authentication appropriate for the data sensitivity level (e.g., userid/ password, and secureID)
 - For more sensitive data, public key infrastructure should be used to authenticate all parties and to encrypt the data (e.g., mutual authentication SSL, XMLEncryption, NIST FIPS 140-1-compliant encryption scheme)
 - Software storing data must have the ability to encrypt and, based on data exchange packages, some exchanges may require data to be encrypted while at rest^{95,96}
 - Data storage and retrieval must be compliant with the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information⁹⁷
 - Should be able to generate an audit log for a user-specified time period
- Recipient systems be patched and maintained with recent security controls (e.g., strong system administrator password policies and anti-malware patches)
(State and local jurisdictions)

E2: Have or have access to secondary systems for information sharing and public health alerting in the event that the primary system is unavailable *(State and local jurisdictions)*

E3: Have or have access to a communication and alerting system that can handle both public health alert messaging and non-urgent messaging *(State and local jurisdictions)*