Public Health Emergency Preparedness and Response Capabilities

National Standards for State, Local, Tribal, and Territorial Public Health

Capability 6: Information Sharing

October 2018
Updated January 2019

For the full 508 compliant document, please visit https://www.cdc.gov/cpr/readiness/00_docs/CDC_PreparednessResponseCapabilities_October2018_Final_508.pdf
**Capability 6: Information Sharing**

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

**Functions:** This capability consists of the ability to perform the functions listed below.

- **Function 1:** Identify stakeholders that should be incorporated into information flow and define information sharing needs
- **Function 2:** Identify and develop guidance, standards, and systems for information exchange
- **Function 3:** Exchange information to determine a common operating picture

**Summary of Changes:** The updates align content with new national standards, updated science, and current public health priorities and strategies. Listed below are specific changes made to this capability.

- Increases alignment to public health surveillance and data strategies
- Emphasizes the need to implement data security and cybersecurity
- Emphasizes the need to decrease reporting time and increase collaboration by expanding use of electronic information systems, such as electronic death registration (EDR), electronic laboratory reporting (ELR), and syndromic surveillance systems

**For the purposes of Capability 6, partners and stakeholders may include the following:**

- clinical and other professional organizations
- critical infrastructure services
- emergency management agencies
- emergency response organizations
- environmental health agencies
- federal, state, local, tribal, and territorial agencies
- food safety and agricultural representatives
- fusion centers
- hazardous material regulators and responders
- health care coalitions
- health care organizations
- health care providers
- health information exchanges
- immunization programs
- medical examiner or coroner offices
- mental/behavioral health agencies
- pharmacies
- private sector organizations
- public health agencies
- tribes and native-serving organizations

---

2 For example, water and electrical utilities
3 For example, law enforcement, fire departments, and emergency medical services (EMS)
**Function 1: Identify stakeholders that should be incorporated into information flow and define information sharing needs**

**Function Definition:** Identify intra- and inter-jurisdictional stakeholders to participate in information exchange, and determine and periodically reassess stakeholders’ needs for bi-directional information sharing.

**Tasks**

**Task 1:** Identify intra- and inter-jurisdictional stakeholders to incorporate into information flow.

Identify intra- and inter-jurisdictional stakeholders to incorporate into information flow, and determine the information sharing needs for each stakeholder.

**Task 2:** Update and refine information sharing needs.

Engage identified stakeholders regularly, and use quality improvement processes to continuously update and refine information sharing needs and capabilities.

**Preparedness Resource Elements**

**P1:** (Priority) Roster of identified stakeholders to engage for bi-directional information exchange across jurisdictional public health agencies and other partners and stakeholders.

**P2:** (Priority) Procedures in place to review and update the role-based public health directory that supports public health alert messaging. Recommended directory categories may include

- Organizational affiliation
- Assigned role(s) and notification tier
- Multiple sources of contact information, as available

*(See Capability 4: Emergency Public Information and Warning)*

**P3:** Established channels for stakeholder communications, such as standing meetings, electronic messaging, e-mailed communications, and web conferencing.

*(See Capability 3: Emergency Operations Coordination and Capability 4: Emergency Public Information and Warning)*

**Equipment and Technology Resource Elements**

**E/T1:** Information system(s) updated regularly and with appropriate backup to store and retrieve stakeholder contact information in a timely manner.

**E/T2:** System credentials and security clearances to access restricted information and systems, such as Epi-X, Homeland Security Information Network (HSIN), and the jurisdictional health alert network (HAN).
Function 2: Identify and develop guidance, standards, and systems for information exchange

Function Definition: Define procedures and establish systems for information governance, management, and sharing.

Tasks

Task 1: Identify relevant data regulations, policies, and standards. Identify current jurisdictional and federal laws and policies that authorize, limit, or protect the exchange of information relevant to emergency situational awareness.

Task 2: Identify stakeholder data requirements. Coordinate with identified stakeholders to determine routine and incident-specific essential elements of information (EEI) for each stakeholder.

Task 3: Determine the conditions for information exchange. Identify when and to what extent information and data exchange is necessary for public health events and incidents.

Task 4: Develop systems for data storage and exchange. Identify and develop systems, such as electronic or non-electronic solutions to store, protect, control, and exchange data.

Task 5: Identify and mitigate barriers to information exchange. Use continuous quality improvement processes and corrective action systems to identify and mitigate procedural, legal, and policy-related barriers.

Preparedness Resource Elements

P1: (Priority) Procedures in place for information exchange that adhere to available national standards for health information exchange. Recommended standards and considerations may include

- Information exchange standards
  - Security levels, such as sensitive, but unclassified or confidential
  - Personnel authorized to share and receive information
  - Timeline and frequency
  - Data format, such as text or numeric and structure to ensure proper consumption in electronic health records (EHRs) and clinical decision support (CDS) systems
  - Data use and release parameters
  - Metadata needs
  - Data privacy and cybersecurity
  - Legal, statutory, and intellectual property regulations
- Other relevant considerations
  - Inventory Data Exchange (IDE) dependent upon medical countermeasure type
  - Electronic laboratory reporting (ELR), electronic case reporting (eCR), electronic death reporting (EDR), syndromic surveillance reporting, electronic laboratory test order and reporting (ETOR), immunization information systems (IIS), exchange of data among health jurisdictions, and data for other registries
Capability 6: Information Sharing

- Environmental exposures data including hazardous material releases, air monitoring, water quality samples, food contamination, and radiation detection. Monitoring of individuals in isolation or quarantine and monitoring of populations for contamination.
- Dissemination of clinical guidance for diagnostic evaluation and care.
- Situational awareness briefings.


P2: (Priority) Stakeholder-specific procedures, determinants, trigger events or other applicable criteria for health information exchange. Determinants may include:

- Epidemiology/Surveillance
  - Unusual cluster(s) of illness that threaten closure of institutional settings, such as illness among health care workers or prisoners.
  - Large numbers of patients with similar and unusual symptoms.
  - Large number of unexplained deaths.
  - High burden of illness or a cluster of illness confined to a specific population.
  - Simultaneous clusters of similar illness in noncontiguous areas for example, because of travel to affected areas.
  - Higher than expected morbidity and mortality associated with common symptoms or failure of patients to respond to traditional therapies.
  - Incidents in other jurisdictions that raise possible risk in an individual’s home jurisdiction including elevation of the pandemic influenza alert level.
  - World Health Organization’s (WHO’s) Public Health Emergency of International Concern (PHEIC).
  - Laboratory
  - Diagnosis or clinical, laboratory, environmental, or pathology finding of public health concern.
  - Public health laboratory findings not identified by clinical, surveillance, or epidemiological investigations, such as a novel virus.
- Other
  - Illness or injury burden expected to overwhelm local health care or public health resources.
  - Received threats or intelligence.
  - Mass casualty incident due to a catastrophic event, such as flood, earthquake, terrorism, or industrial release.


P3: Procedures in place for data exchange in both routine and incident-specific settings, including agreed upon systems for data storage and exchange and data exchange frequency with CDC and other stakeholders, in accordance with jurisdictional standards.

P4: Strategies for collaboration and system integration to improve intra- and inter-jurisdictional information sharing for situational awareness during routine operations and public health events or incidents. Consider collaborative strategies and activities, which may include:

- Increasing information system interoperability to support disease and syndromic surveillance, public health registries, outbreak management, exposure assessment, and other activities.
- Extending data availability with dashboards and other information sharing tools.
P5: **(Priority)** Written agreements, such as contracts or memoranda of understanding (MOUs) with relevant agencies and other stakeholders to define participation, security or access levels, and procedures for information exchange.

P6: **(Priority)** Procedures in place to account for laws, provisions, and policies addressing privacy, security including cybersecurity, civil liberties, intellectual property, information sharing limitations, and other substantive issues. Relevant laws and policies may include:

- Emergency powers for public health data collection and sharing
- Health Insurance Portability and Accountability Act (HIPAA)
- Office of the National Coordinator for Health Information Technology Policy
- U.S. Department of Health and Human Services (HHS) Information Management Policy
- State laws and regulations prohibiting information sharing to federal or inter-jurisdictional entities

P7: Guidelines for information exchange that requires security clearances, such as information exchange with the Federal Bureau of Investigation (FBI), state bureau of investigation, fusion centers, or agents with a “need to know.”

**Skills and Training Resource Elements**

S/T1: Personnel with awareness-level training in pertinent laws and policies for information sharing procedures including transport of data and use of personally identifiable information (PII).

S/T2: Personnel trained in informatics and information technology project management, as necessary, to implement public health informatics systems.

**Equipment and Technology Resource Elements**

E/T1: Information systems that meet national data standards for interoperability as identified by CDC, other federal agencies, such as the Office of the National Coordinator for Health Information Technology, or other standards development organizations (SDOs). Recommended information system capabilities may include:

- Receiving and transmitting data electronically using standards-based messaging
- Converting non-standard formats or terminologies into federally accepted standards for communication
- Receiving, using, and transmitting messages that adhere to certified EHR technologies or standards under Meaningful Use guidelines
- Transmitting and receiving data from non-electronic data sources, only if electronic capabilities are unavailable
- Gathering EEI or data from cross-disciplinary stakeholders and transmitting data into a public health situational awareness system
**Capability 6: Information Sharing**

**Function 3: Exchange information to determine a common operating picture**

**Function Definition:** Share information across public health agencies and intra- and inter-jurisdictional stakeholders using available national standards, such as data vocabulary, storage, transport, security, and accessibility standards.

**Tasks**

**Task 1: Exchange health information.** Exchange meaning request, send, and receive relevant data and information with identified cross-disciplinary stakeholders using procedures and systems that meet jurisdictional or federal standards.

**Task 2: Maintain accessible data repositories.** Support information exchange among cross-disciplinary stakeholders using accessible data repositories that adhere to jurisdictional or federal standards.

**Task 3: Apply data security protocols.** Request, send, and receive information using security protocols that meet jurisdictional or federal standards.

**Task 4: Verify data authenticity.** Confirm data authenticity with message sender or information requestor.

**Task 5: Acknowledge receipt of information.** Confirm the successful transmission and receipt of information, as appropriate, for the incident.

**Preparedness Resource Elements**

**P1: (Priority)** Procedures in place to develop information and public health alert messages. Procedures may include:

- Time sensitivity of information
- Relevance to public health
- Target audience
- Security level or sensitivity of information
- Actions required following the receipt of information, such as sending a response

*(See Capability 4: Emergency Public Information and Warning)*

**P2: (Priority)** Procedures in place for information exchange with fusion centers and other intelligence entities. Procedures may include:

- Defined intelligence requirements that prioritize and guide planning, collection, analysis, and information dissemination efforts
- Delineated roles, responsibilities, and requirements for each level and sector of government

**P3: (Priority)** Procedures in place for information exchange among jurisdictional health care entities using electronic public health case-reporting systems, syndromic surveillance systems, notifiable disease surveillance systems, electronic death registration systems, immunization information systems, or other specialized registries. Data should be shared using electronic systems when available or as possible. Electronic information sharing may include:

- Sharing reportable diagnoses and related information from a health information exchange (HIE) or an EHR system to state and local public health agencies
Capability 6: Information Sharing

- Sharing laboratory test results from commercial, public health, hospital, and other laboratories’ laboratory information management system (LIMS) to state and local public health agencies
- Sharing laboratory test orders and results between a public health laboratory and another laboratory or a clinical setting
- Sharing immunization information between an HIE or EHR system and public health immunization registries, public health syndromic surveillance systems, such as CDC’s National Syndromic Surveillance Program BioSense Platform, or other public health registries
- Sharing notifiable disease data among public health agencies and between public health agencies and CDC
- Sharing information regarding individuals undergoing health monitoring or in isolation and quarantine

**P4:** Procedures in place to acknowledge receipt by trusted sources and send verification of information to intended audience(s).

**P5:** Templates for public health alert messages and procedures including distribution methods to ensure messages reach intended individuals 24/7 year-round. Public health alert message templates may include
  - Subject or title
  - Description
  - Background
  - Request or recommendations (if action requested)
  - Recipient(s)
  - Point of contact to address additional questions
  - Links to additional information

*(See Capability 4: Emergency Public Information and Warning)*

**P6:** Information Sharing and Access Agreements (ISAA) or similar agreements with data sharing partners. Recommended elements for ISAAs may include
  - Breach notification procedures, particularly if data is not stored in an encrypted state
  - Maintenance of HIPAA Security Rule compliance, when potential PII must be shared

**Skills and Training Resource Elements**

**S/T1:** Personnel, such as informaticians trained on public health information systems to develop, sustain, coordinate, and oversee public health informatics.

**S/T2:** Information system support personnel trained, as necessary, to maintain or enhance the functionality and capacity of public health information systems, perform public health information specialist and informatics roles, and use data standards and facilitate interoperability across allied disciplines, including the Open Geospatial Consortium.
Capability 6: Information Sharing

**Equipment and Technology Resource Elements**

**E/T1: (Priority)** Electronic systems for routine information transmission, emergency notification, and situational awareness between health care and public health systems and between jurisdiction-based surveillance systems and CDC that meet applicable national and jurisdictional standards. Standards may include

- Data format and structure
- System interoperability
- Data quality and reliability
- Consent, security, and privacy for protected health information and other sensitive information, as applicable, such as protections against data breaches using encryption
- Data governance or ownership and rules or agreements for data use, reuse, release, and publication
- Controls and safeguards for data storage and access that may include
  - Authentication service for data requests and submissions from various locations
  - System administrator password policies
  - Updated security patches
  - Encryption, as required


**E/T2:** Systems that automate transmission of information from the clinical setting, such as an EHR system, to the public health agency in compliance with jurisdiction-specific reporting regulations to support overall public health surveillance, improve the timeliness and accuracy of data submitted to state and local public health agencies, and enable subsequent information sharing with CDC.

**E/T3: (Priority)** Secondary systems for information sharing and public health alerting in the event that the primary system is unavailable.

*(See Capability 4: Emergency Public Information and Warning)*

**E/T4:** Data visualization tools, such as analytic dashboards and geographic information systems (GIS) for effective presentation and dissemination of data for situational awareness in routine and response situations.