Homeland Security and Public Health: A Critical Integration

Jeremy G. Carter, Ph.D.[1]
Indiana University – Purdue University Indianapolis

Michael Rip, Ph.D.
Michigan State University

Abstract
In the wake of a series of tragic events impacting public health in the United States, the Department of Health and Human Services Centers for Disease Control and Prevention and the Department of Homeland Security have attempted to facilitate information sharing across public health and homeland security organizations. Data collected as part of a national assessment of law enforcement and homeland security information sharing, funded by the National Institute of Justice, indicate such efforts to date have been helpful in establishing a foundation for information sharing, yet fall short of creating mechanisms by which tangible information sharing can occur. Recent initiatives to remedy this shortcoming are presented and recommendations for further success are discussed.

Keywords: preparedness, homeland security, public health, prevention, information sharing

Carter, J. G. & Rip, M. (2013). Homeland security and public health: A critical integration. *Criminal Justice Policy Review*, 24(5), 573-600.

[1]Author Correspondence: 801 W. Michigan Street, Indianapolis, IN 46202, P: (317) 274-4170, carterjg@iupui.edu

Homeland Security and Public Health: A Critical Integration

Terminology such as homeland security, intelligence-led policing, preparedness, and risk management have become consistent in the criminal justice lexicon in the wake of the attacks of September 11, 2001. As these policy applications continue to be conceptualized in the academic literature as well as in practice, the integration of the public health sector has just recently begun to emerge as the next supporting pillar in the preparedness structure. Recent initiatives primarily driven by the Department of Homeland Security and the Centers for Disease Control and Prevention have begun to outline the need to establish two-way communication channels and integrated policy initiatives between law enforcement and public health organizations in order to enhance threat prevention and preparedness efforts. Such initiatives have been absent from discussions in the criminal justice discipline. Indeed, policy and regulatory initiatives are being developed with virtually no research (or theoretical) foundation.

Mechanisms for gathering and sharing information[1] have been operationalized within both homeland security and public health. Despite such mechanisms being in place, there remains an information sharing disconnect between homeland security and public health. This paper seeks to provide an analysis of these initiatives, in order to assess and provide guidance to integrate public health and homeland security policies and capabilities. Data from a recent National Institute of Justice study on fusion center information sharing across the U.S. is presented here and illustrates an existence of such collaborations among stakeholders yet also a lack of tangible information sharing. This paper will provide an analysis of the types of information gathered for both homeland security and public health and how this information can be integrated together using the information fusion center approach.

Statement of Purpose

Since September 11, 2011 a significant amount of progress has been made to improve information collection and sharing in both the public health and homeland security sectors in their own rights. Approximately five years ago, both sectors recognized the importance of creating an information sharing capability that would connect one to the other. To date, there have been substantial efforts to successfully integrate public health information into homeland security prevention and preparedness efforts. In short, these efforts have established an operating environment in which both public health and homeland security have begun to develop working relationships, yet a lack of tangible information sharing remains. It is argued that efforts to improve information sharing under the guidance of the U.S. Department of Health and Human Services, which has a different operational view of information sharing, have not be successful in integrating homeland security efforts. Recently, efforts guided by the U.S. Department of Homeland Security have provided actionable steps to integrate public health information. The present paper provides a legislative, regulatory and policy discussion followed by a national empirical assessment to illustrate the present information sharing environment among public health and homeland security. Recommendations for further operational success are provided. Areas for academic evaluation are identified.

A Note on Homeland Security

For purposes of this paper, the term "homeland security" refers to the capabilities of state and local law enforcement agencies, capabilities of state and major urban area fusion centers, as well as the integrated initiatives from the Department of Homeland Security (DHS) as their prevention and preparedness missions are related to public health threats. Specifically, the

present DHS mission is centered on five core areas. Two of these areas pertain specifically to preventing terrorism and enhancing security as well as ensuring resilience to disasters (U.S. Department of Homeland Security, 2011a). It is within these two core mission areas which the importance of integrating public health information becomes critical to the success of DHS in accomplishing its mission. Methods of terrorist attack go beyond explosives to include biological agents and the natural spread of E.Coli is just one example of a public health disaster. In order to successfully integrate this information into the homeland security decision making process, fusion centers will play a pivotal role.

While the DHS and state and local law enforcement are familiar to most in the criminal justice discipline, fusion centers are not as well understood. As it will be discussed, fusion centers are the focal point of current efforts to enhance public health prevention and preparedness (U.S. Department of Justice, 2011). At the time of this paper, there are 72 officially recognized fusion centers in the United States (U.S. Department of Homeland Security, 2011c). In brief, fusion centers operate as the information sharing lynchpin among all levels of law enforcement as well as the private and public sectors. Such a collaborative effort facilitates the sharing of threat-related information to law enforcement and client organizations (Cooney *et al*., 2011). Masse and Rollins (2007) note that fusion centers represent a vital part of the nation's homeland security and are essential to fuse a broad range of data, including nontraditional sources of data, to create a more comprehensive threat picture for the prevention of terrorism. This threat picture has broadened, largely a result of measures initiated by the *Intelligence Reform and Terrorism Prevention Act* (2004) which expanded fusion center missions from terrorism to include "all threats, all hazards" (Carter & Carter, 2009a). Specifically, the Homeland Security Advisory Council (2005, p.2) observed,

> "Although the primary emphasis of intelligence/information fusion is to identify, deter, and respond to emerging terrorism-related threats and risks, a collateral benefit to state, tribal and local entities is that it will support ongoing efforts to address non-terrorism related issues by . . . allowing state and local entities to better identify and forecast emerging crime, public health, and quality-of-life trends . . . supporting targeted law enforcement and other multidisciplinary, proactive, risk-based and community-focused, problem-solving activities; and . . .improving the delivery of emergency and nonemergency services".

Using a medical metaphor, fusion centers are the heart of the prevention and preparedness body for public safety. The public health sector represents a critical vein for moving epidemiological information to the fusion center where it can then be pumped back out to the prevention and preparedness limbs that are state and local law enforcement, critical infrastructure and public health organizations. The discussion to follow will expand on the types of information collected by fusion centers and public health and how this information can be fused together.

A Review of Homeland Security and Public Health Integration

The Department of Homeland Security and Public Health

The role of public health in homeland security has recently evolved. Immediately following the events of 9/11, public health's primary role in homeland security was to assist in the detection of and preparedness for bio-terrorism attacks as set forth by President G. W. Bush's *Biodefense for the 21st Century* (2004). While these efforts have had measurable successes

(Alexander, Larkin, & Wydia, 2006; Nelson, Lurie, & Wasserman, 2007) and shortcomings (Spranger *et al*., 2007; Koh *et al*., 2008), they established a foundation for *Homeland Security Presidential Directive (HSPD) 21 National Strategy for Public Health and Medical Preparedness*. HSPD 21 outlines a national policy for proactive preparedness for incidents impacting public health. This directive asserts such an approach is achievable by utilizing mechanisms of active information sharing across public health, public safety, and private business sectors. The effectiveness of this approach relies on the ability to translate best practices currently established in the arena of "all threats, all hazards" homeland security law enforcement to the operations of those in the public health discipline (The White House, 2007). In sum, HSPD 21 formally established the need to have different methods of "biosurveillance" and "epidemiologic surveillance" as a means to maintain an active situational awareness of current public health trends and potential threats. The process of biosurveillance integrates active data gathering with analysis and interpretation of biosphere[2] data that might relate to disease activity and threats to human or animal health – whether infectious, toxic, metabolic, or otherwise, and regardless of intentional or natural origin – in order to achieve early warning of health threats (Wagner *et al*., 2007). Epidemiologic surveillance is the process of actively gathering and analyzing data related to human health and disease in a population in order to obtain early warning of human health events, rapid characterization of human disease events, and overall situational awareness of disease activity in the human population (Watkins *et al*., 2011).

As the lead agency responsible for the prevention of and response to chemical, biological, radiological, nuclear, and explosive (CBRNE) attacks, the Department of Homeland Security (DHS) acknowledged the need to not only have a system in place for responding to such public health-related tragedies, but also a means by which all public health-related threats could be

monitored. As such, the Office of Health Affairs (OHA) was created to serve as the DHS' principal authority for all medical and health issues (Department of Homeland Security, 2011c). The operational arm with respect to monitoring public health threats and trends is the National Biosurveillance Integration Center (NBIC). Created as part of the *Implementing Recommendations of the 9/11 Commission Act* of 2007, DHS was to ensure the NBIC has the ability to rapidly identify, characterize, localize and track a biological event of national concern with the goal being real time or near real time (U.S Department of Health and Human Services, 2010) as well as enhance the nation's capability to integrate biosurveillance efforts as most of the organizations maintaining these capabilities are relatively uncoordinated (Castillo-Salgado, 2010). The bioterrorism threat presents a risk to the population, economy or infrastructure of the United States. Section 1011 of this Act required the NBIC to operate by integrating and analyzing data relating to human health, animal, plant, food and environmental monitoring systems and that it must be fully operational by September 30, 2008 (U.S. House of Representatives, 2011). While the NBIC is presently "up and running", it has yet to effectively demonstrate its ability to integrate disparate pieces of health threat information (U.S. Government Accountability Office, 2009).

While DHS may be the lead agency responsible for CBRNE incidents, HSPD 21 established the U.S. Department of Health and Human Services (HHS) as the authority over the response to health emergencies and to establish a system that creates a network which allows for two way information flow between and among federal, state and local government, public health authorities, and clinical health care providers. To this end, the Centers for Disease Control and Prevention (CDC) within HHS created a surveillance mechanism known as BioSense 2.0 which is currently the only nation-wide all-hazards emergency public health surveillance system

(Centers for Disease Control and Prevention, 2011a). In short, BioSense 2.0 is designed to facilitate the interchange of information that can be used to coordinate responses and monitor health-related outcomes on a routine as well as event basis. An evolution from bioterrorism and biosurveillance to epidemiological surveillance and "all threats, all hazards" has resulted in the term "biopreparedness" – the ability to proactively prevent or mitigate public health threats – being introduced to the homeland security lexicon. An epidemiological surveillance capability is the capacity to rapidly conduct epidemiological assessments in real-time. It includes deliberate (e.g. bioterrorism) and naturally occurring (e.g. disease) threat detection, rapid implementation of active surveillance, analysis, communication with partners and liaison about case definitions, risk assessments, mitigation, and recommendations for the implementation of control measures. Desired outcomes of such a capability include a threat being identified rapidly as well as a means to contain the spread of the event and reduce number of cases.

Efforts on behalf of both public health and homeland security have mirrored one another – both a positive and negative as these efforts progress. It is positive as both sides recognize and formally agree that information sharing for preparedness and prevention should exist between public health and homeland security. The negative impact of both sectors repeatedly agreeing that they should share information is that no progress is made towards actually achieving the desired outcomes. Actionable steps must be identified as a means to reach desired ends. Identification of such steps remains difficult as initiatives to bridge public health and homeland security are plagued by a lack of systematic evaluation. While assessments of progress have been reported towards these goals have been reported (U.S. Department of Homeland Security, 2011c; U.S. Government Accountability Office, 2011), there has been no empirical evaluation of success or return on investment.

State and Local Law Enforcement and Public Health

State and local law enforcement's role in public health has largely pertained to emergency response. While law enforcement has long served the role of "first-responder", their role in the current health threat environment can be traced to the anthrax incidents shortly after 9/11 (Butler *et al*., 2002; McHugh, Staiti & Feeland, 2004), the 2003 spread of the Severe Acute Respiratory Syndrome (Sarpy *et al*., 2005), and more recently the H1N1 flu pandemic of 2009 (Macario *et al*., 2009). Following the *National Response Framework* published by the Department of Homeland Security (2008), in the event of an emergency incident, local law enforcement serves as the initial response mechanism in a multi-layered response approach. More specifically in event of a public health emergency, law enforcement is responsible for to quickly coordinate its response with public health and medical officials and, depending on the threat, enforce public health orders (e.g., quarantines or travel restrictions), secure the perimeter of contaminated areas, securing health care facilities, and investigating scenes of suspected biological terrorism (Richards *et al*., 2006). In a large-scale incident, such as a pandemic, law enforcement resources are likely to become exhausted and law enforcement officials will have to balance their resources and efforts between these new responsibilities and everyday service demands. Moreover, within this multi-faceted responsibility of being first-responders to public health emergencies, it is plausible for law enforcement to be in a situation with a greatly diminished workforce, as officers and their families may become infected and ill, and some personnel may determine that the risk of continuing to report to work is just too great to themselves or their families (Richards *et al*., 2006) – such as in the aftermath of Hurricane Katrina when officers of New Orleans Police Department did not report to work for a variety of

reasons. A department's ability to respond effectively to any emergency - public health or otherwise - greatly depends on its preparedness which relies on the law enforcement agency's strategic planning and its partnerships. Strategic planning is achieved through successful information sharing and analysis.

The emphasis on strategic planning and partnerships is the dimension of law enforcement's role in public health that has recently begun to evolve. Rather than operationalizing planning and partnerships as a means to solely improve first-responding, law enforcement has begun efforts to identify proactive measures via these components. For example, rather than having partnerships in place with local health organizations for purposes of knowing who to contact and where to go in the event of an emergency, law enforcement attempts to establish a two-way open dialogue among both public health organizations and the community in an attempt to share threat-related information. The Police Executive Research Forum (PERF) published a series of reports to help improve the law enforcement response to public health emergencies. In short, these reports emphasized the importance of law enforcement communication with public health organizations, other public safety agencies, and the community (Brito, Luna, & Sandberg, 2009a) and strategic planning for the prevention and mitigation of public health events such a pandemic flu (Brito, Luna, & Sandberg, 2009b; Sandberg *et al*., 2010). Such communication is achieved through partnerships and liaison officer programs. Local law enforcement serves as a force-multiplier with respect to information collection. Primarily through community policing, police officers are able to gather raw information and recognize indicators and warnings of threats (Carter & Carter, 2009b) – a somewhat "grass-roots" level of epidemiological surveillance. This micro-level information is

critical to identifying accurate threat pictures and is relied upon by fusion centers and thus public health organizations as well.

An example of this approach can be found in Los Angeles, California where the Terrorism Early Warning Group (TEWG) serves as the focal point for analyzing the strategic and operational information needed to respond to a range of threats. The TWEG has two primary functions; 1) responsible for information sharing and intelligence fusion, and 2) performs net assessments to aid mission planning, decision-making, and allocation of resources in support of incident command during actual events (Sullivan, 2005). More specifically, the TEWG…

> "…includes analysts from local, state and federal agencies to produce a range of intelligence products at all phases of response specifically tailored to the user's operational role and requirements…As part of this process, the TEWG seeks to identify emerging threats and provide early warning by integrating inputs and analysis from a multidisciplinary, interagency team. Toward this end, the TEWG has developed a local network of Terrorism Liaison Officers at law enforcement, fire, and health agencies, formed partnerships with the private sector to understand threats to critical infrastructure, and has developed and refined processes to analyze and synthesize threat data to support its client agencies" (Sullivan, 2005, p.1).

Progress of Homeland Security and Public Health Integration since September 11, 2001

To begin, it is necessary to acknowledge the re-socialization process facing homeland security. This re-socialization impact is centered largely on state and local law enforcement. As contingency theorists would argue, September 11, 2001 created a dramatic shift of the environment in which law enforcement functions on a daily basis. This shift is primarily

exhibited in the additional focus of law enforcement, which was traditionally limited to responding to incidents and calls for service, to - put it simply - create a level of situational awareness of potential threats in their jurisdictions (Burress, Giblin, & Schafer, 2010). This shift in operational responsibilities, coupled with an emerging prevention and preparedness lexicon, has created a substantial learning curve for most state and local agencies.

Two recent reports have assessed the DHS' progress of implementing mechanisms to be preventative and prepared for a variety of threats in the 10 years since the attacks of 9/11. Included in these reports are findings related to public health. The first report, *Implementing 9/11 Commission Recommendations: Progress Report 2011* published by the Department of Homeland Security (2011a) noted that in order to improve state and local biopreparedness, DHS established the first formalized sharing of public health and intelligence information with state and local health partners in 2009. In 2010, DHS developed and conducted a series of information sharing and response exercises involving more than 1,000 state and local officials (U.S. Department of Homeland Security, 2011c, p.33). Despite anecdotal success – such as efforts to acquire data from its partners, obtain analytical expertise from other agencies, establish governance bodies to develop and oversee the community of partners, and provide information technologies to support data efforts - these pilot exercises identified disconnects of information sharing among stakeholders involved.

The second progress report, *The Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11* published by the U.S. Government Accountability Office (2011), documented similar findings with respect to CBRNE information sharing noting that "the National Biosurveillance Integration Center lacks resources necessary for operations, such as data and personnel from its partner agencies" (U. S.

Government Accountability Office, 2011, p.20). More specifically, this report noted interviews with NBIC partner agencies found "widespread confusion, uncertainty, and skepticism about the value of participation in the NBIC, as well as the mission and purpose of the NBIC within its community of federal partners" (U.S. Government Accountability Office, 2011, p.69). This report went on to discuss that for the NBIC to obtain the resources it needs to meet its mission, it must

> "effectively employ collaborative practices, and we recommended that the NBIC work with its interagency advisory body to develop a strategy for addressing barriers to collaboration, such as the lack of clear mission, roles, and procedures, and to develop accountability mechanisms to monitor these efforts" (United States Government Accountability Office, 2011, p.69). In summation, while the NBIC appears to have organizational partners willing to share information, these partner agencies lack a common understanding of information sharing practices as well as the infrastructure to physically share information.

In sum, these reports have identified functional gaps of successfully sharing information between public health and homeland security. In response to these findings, both public health and homeland security must identify mechanisms that serve as information sharing conduits. Systems for disseminating and receiving intelligence products must be created and public health must identify a means by which information can actively flow to and from public health organizations and incorporate a system by which this information is integrated into an analytic process.

Public Health Information Gathering and Sharing

Within the public health arena, biosurveillance describes the monitoring of characteristics (e.g. symptoms, lab results, or deaths within a population) for changes that could indicate an emerging threat - natural or deliberate. To date, most surveillance has not been in real time. Rather, patient or community information is submitted to local health departments which are then reported in aggregate to state or federal health agencies. Such reporting techniques create detached information silos where information is typically stored vertically in disease-specified categories (e.g. H1N1 or HIV/AIDS) and those go largely unconnected (horizontal) to other, often inter-related, diseases or problems (Merrill *et al*., 2008). These information silos are virtually the same that were experienced by both law enforcement intelligence and the intelligence community. Fusion centers are intended to be the remedy for sharing threat information – the same processes which must be applied to share public health threat information across sectors. Public health officials need to recognize this type of vertical organization hinders the ability of epidemiologists or analysts to fully assess the impact of diseases and conditions that affect public health. Moreover, the multiple public health surveillance systems that conduct surveillance are rarely capable of the data analysis needed to understand complex multidimensional problems. In short, these systems lack horizontal movement and simply "cannot talk to each other" (Danos & Hancock, 2009).

In an effort to remedy this lack of horizontal communication among systems, new informatics solutions are emerging that reduce or eliminate these challenges by establishing effective silo system interoperability. A critical component of these new tools is a master person index that is used to link individuals across many disconnected data silo systems (Centers for Disease Control and Prevention, 2011d) – essentially an established information liaison officer for each system. A legal complexity of this approach – one that remains a constant for this entire

discussion – is the sharing of patient information with law enforcement that may include individual identifying information. There are two legal frameworks guiding the sharing of this information.

The first is that according to the *Program Manager's Information Sharing Environment Privacy Guidelines* (2006a) published by the Office of the Director of National Intelligence, law enforcement organizations must articulate a criminal nexus connected to information which identifies an individual. Secondly, under the *Health Insurance Portability and Accountability Act* (HIPAA), patient information[3] is only available to law enforcement organizations if the individual seeking the information has been verified as law enforcement personnel, that the law enforcement personnel clearly articulates the justification for the patient information[4], and that the custodian of the patient information only provides the minimum amount of information necessary for the articulated purpose (The University of Chicago, 2007). Given these two most salient legal provisions regarding the sharing of public health related information with law enforcement, law enforcement must not only have established a criminal nexus related to the desired information, but also have articulated a justification for requiring such information. While this approach may delay "real-time" sharing of certain information, it is well within the grasp of the law enforcement function. However, such an approach may prove to be difficult for personnel working for public health organizations as these individuals will likely lack the knowledge (or access to classified information) to establish either a criminal nexus or an articulable justification for sharing patient information with law enforcement in a proactive manner that is usually necessary to remain cognizant of natural and man-made threats.

Once again in the wake of the anthrax attacks of 2001, SARS in 2003, and H1N1 in 2009, rather than waiting for cases to appear, it became clear that identifying trends (or precursors) to

these events would allow for earlier recognition of a possible epidemic or bioterrorism event. It became evident the system of surveillance was antiquated and slow; it wasn't capable of identifying the health risks until well after an attack had taken place (Centers of Disease Control and Prevention, 2011b). It was felt that public safety and public health data should be monitored on the local level as well as sent to a centralized repository for aggregation into larger geographic areas to detect a multi-site concurrent attack instead of the current silo mentality of looking at singular locals.

Public health utilized a case-counting method of information collection. Dimensions typically include who, what, where, when, how, and why. This case-counting process may be active or passive. Active processes are when cases are reported by health officials on a real-time basis – as they are identified. Passive processes are when health officials report case information on a scheduled basis – perhaps once a month. With respect to identifying threats, active processes are necessary as information pertinent to the threat must be identified in order to properly respond and/or prevent on-going threats. At present, passive surveillance is the predominant way case information is reported to public health officials. This is a hindrance to threat prevention and preparedness as this information may be shared too late to identify appropriate responses. The quality of this passive method of reporting depends on the actions of physicians, hospitals, and laboratories to identify and promptly report a case of importance or a positive laboratory result that suggests the presence of an important case (e.g. disease) – also referred to as notifiable diseases.

A host of laws and regulations dictate which diseases are notifiable to public health agencies, the method of submitting these reports, and the information required in the report. Further complicating this information sharing effort is that these laws lack uniformity and vary

among cities, regions, states, and countries (Centers for Disease Control and Prevention, 2011c). Compliance with these reporting requirements also varies, but is frequently inadequate to meet the disease surveillance requirements facing today's public health leaders. This is because the current, paper-based passive reporting systems rely on a person (physician, nurse, administrator, laboratory technician, etc.) to submit the reports to public health officials. Unfortunately, public health reporting is too often delayed, incomplete, or even forgotten because of the competing priorities facing today's healthcare workforce (Barr *et al*., 2011).

In contrast, active surveillance differs from passive surveillance by the methods used by health officials to identify new cases rather than predetermined notifiable diseases. This is typically achieved by assigning public health staff to medical facilities to review medical files to identify new cases (Olson, 2007). Unlike passive surveillance systems, active surveillance reporting is typically timely, complete, and inclusive; however the majority of public health agencies lack the resources to conduct comprehensive active surveillance of health-related threats (Morrow & Novick, 2005). Making widespread adoption of active surveillance of health-related threats a tangible reality is the *Health Information Technology for Economic and Clinical Health Act* (HITECH) of 2009 which established the present movement for health records to be maintained electronically by 2014. Though the HITECH Act facilitates this electronic information sharing initiative, it also contains safeguards against any privacy and security violations associated with the electronic transmission of health information through several provisions that strengthen the civil and criminal enforcement of the HIPAA regulations (U.S. House of Representatives, 2009). Similar safeguards have also been established with respect to law enforcement's information sharing efforts, typically in the form of a USC 42 Section 1983 deprivation of civil rights lawsuit resulting in law enforcement's failure to establish a criminal

predicate for maintaining criminal intelligence files consistent with 28 Code of Federal Regulation Part 23[5].

Effectiveness of active surveillance systems are determined based upon their sensitivity and specificity. A high sensitivity surveillance system is one that rapidly identifies all cases and all potential cases of a disease whereas a high specificity system is one that correctly and uniquely identify cases of disease under surveillance. Accuracy of case reports in highly specific surveillance systems sacrifice speed of reporting while sensitive systems report faster, but lack accuracy. A specific and passive surveillance system may provide a useful estimate of the burden of a disease in a population over time, yet such a system is likely to be inadequate in its ability to predictor current disease trends, especially when trend changes occur rapidly (Barr *et al*., 2011). The 2009 H1N1 influenza pandemic illustrated the shortcomings of traditional passive surveillance systems as health organizations struggled to identify cases in real-time so that prevention measures could be implemented in an efficient manner to reduce the impact of disease in the community (Barr *et al*., 2011). This shortcoming is commonly attributed to delays in reporting on behalf of medical personnel and a failure to report all cases of a given threat. With the implementation of new technologies and the movement towards electronic medical records, is appears to be likely that public health surveillance system automation will transform data collection, data analysis, and data reporting - thus resulting in dramatic increases in surveillance system sensitivity and specificity (Danos & Hancock, 2009). Such automation is likely to increase system sensitivity by rapidly identifying all potential cases that are entered into an electronic medical records system and then securely transmitting these cases to the appropriate public health agency. Simultaneously, specificity should increase with the adoption

of person-matching and database analysis software tools that prevent duplication and false-positive reports (Danos & Hancock, 2009).

The *Pandemic and Public Health Information Fusion for Situation Awareness All-Hazards Preparedness Act* (PAHPA) of 2006, established a demand to increase collaboration with state, local, and tribal public officials through a near real-time electronic nationwide public health situational awareness capability. Increases in the sensitivity and specificity of surveillance systems are designed to create a situational awareness system. Conceptually, situational awareness systems are designed to better understand when a public health threat is growing or decreasing, whether it is expanding into different geographic areas, and whether the threat is becoming more or less serious to the community or population (Hsu *et al.*, 2010). This situational awareness information is the critical type of public health threat information that needs to be shared with the homeland security sector. However as it will be illustrated and discussed in subsequent sections, this is not occurring.

Situational awareness is utilized to inform decision makers in the event of a looming threat to public health. Such decisions could include from deployment of additional resources to respond to the threat, implementing plans to provide mass vaccinations or treatments, and determinations of the movement of people within a community (e.g. school closings or quarantine areas). The key to successful situational awareness is the integration of disparate information sources. As it has been discussed, traditional information has included case-counting and medical chart reading. Situational awareness is most comprehensive when non-traditional sources of data are included to better inform the threat picture. For example a school liaison information officer may provide information on an unusual number of children absent. This information can be integrated with local hospital/clinic information, pharmaceutical sales,

or children absenteeism from a neighboring school. Lastly, disparate sources of information should be disseminated using standardized, or common, terminology. As a variety of medical-related threats are likely to have scientific or medical terminology not commonly understood by stakeholders involved, the use of common terminology is likely to increase successful communication and accurate integration of the information into the analytic process (Centers for Disease Control and Prevention, 2004).

Current mechanisms by which the Department of Homeland Security and the Department of Health and Human Services are generating a situational awareness capability are through the BioWatch Generation 3.0 and BioSense2.0 detection systems. The function of the BioWatch technology is to detect the release of pathogens into the air, providing early warning to government and public health officials of a potential bioterror event. This program operates by employing aerosol samplers mounted on preexisting Environmental Protection Agency air quality monitoring stations to collect and sample air passing through the filters on an hourly basis (U.S. Department of Homeland Security, 2010). BioSense2.0 is a program of the Centers for Disease Control and Prevention that monitors health problems as they evolve and provides public health officials with data on emerging illnesses and health trends to allow for early detection and rapid assessment of potential bioterrorism-related illness. This program provides health officials a means to monitor syndromic[6] activity within and beyond their jurisdictions in a basic, qualitative level (e.g. person, place, and time) (Centers for Disease Control and Prevention, 2011a).

A National Snapshot of Information Sharing among Public Health and Homeland Security

The present study utilizes a unique national data set funded by the National Institute of Justice to "take the pulse" of current public health and homeland security information sharing. No statistical inferences are made from the data. The intent of this paper is to illustrate the current public health and homeland security threat preparedness and prevention environment in the wake of initiatives to this point. As such, the data to follow will illustrate proportions of the state, local, and tribal law enforcement agencies and fusion centers sampled from across the United Sates and their information sharing relationships with members of the public health community. Such efforts are still in the infant stages of becoming operational; both public health and homeland security are "finding their way" in attempts to become interoperable with one another. An empirical evaluation of such efforts would simply be premature. The data presented here provides a snapshot of current information sharing among public health and both law enforcement and fusion center personnel.

Methods

Data for the present study were collected as part of the *Understanding the Intelligence Practices of State, Local, and Tribal Law Enforcement Agencies* grant funded by the National Institute of Justice[7]. The survey, a self-administered questionnaire completed through a web-designed survey provider and targeted two groups of key informants through a purposive sample. The first group included individuals who had attended training programs designed and delivered by the School of Criminal Justice at Michigan State University, and funded by the Department of Homeland Security. This sampling strategy, which includes personnel from significantly

different sized police agencies in all geographic regions of the country, was chosen for two reasons. First, this sample included law enforcement personnel who have a working understanding of key issues tied to developing an intelligence capacity and thus have unique knowledge of the key concepts. Second, their awareness of the intelligence structures, requirements, and formal communication networks increased the likelihood that they will have direct knowledge about the strengths and weaknesses of these issues. The sample represents a diversity of agencies and personnel consistent with all types of agencies from all levels of these organizations – thus ensuring the sample includes personnel that will have crucial information for understanding key issues related to information sharing.

The second group consisted of all persons who had attended the 2007 and 2008 National Fusion Center Conferences[8] (NFCC). The NFCC is sponsored by the leading law enforcement intelligence organizations and is considered to be the prominent gathering of key personnel from every fusion center in the United States. Attendees of the NFCC included fusion center directors, operational personnel, and intelligence analysts. This compilation of personnel that attended the NFCCs provides the most comprehensive population of persons with specific knowledge regarding the information sharing practices of state and regional fusion centers in the United States. Given the infancy and ever-evolving nature of fusion centers in the U.S., such specialized knowledge of key concepts is critical to the issues discussed in the present study.

In early June 2009 an email was sent to each addressee outlining the purpose of the study and inviting them to complete a self-administered, online questionnaire. Data collection began at the end of June 2009. Replies in both the form of automated server notifications alerting addresses were invalid (313 in the law enforcement sample and 52 in the fusion center sample) and formal refusals (57 in the law enforcement sample and 31 in the fusion center sample) were

recorded in order to correct the sampling frame by removing individuals who could not be contacted in addition to those who declined to participate. During the law enforcement sampling process, 2882 invitations and 2395 follow-up emails were transmitted. During the fusion center sampling process, 872 invitations and 772 follow-up emails were transmitted. As email replies and survey submissions were received, the sampling frames were readjusted so subsequent requests targeted only those who had not communicated. Further follow-up emails were issued a second, third, and fourth time at approximately monthly intervals; the fifth and final reminders were sent at the end of March 2010 and the collection window closed one month later. This sample includes 414 responses from state, local, and tribal law enforcement and 88 responses from regional and state fusion center personnel. Using the formula of valid responses divided by first phase invitation minus undelivered invitations minus declined invitations, the response rate for the law enforcement sample was 16% (414 / (2882-313-57)) fusion center sample was 11% (88 / (872-52-31)).

These low response rates were surprising. In order to clarify why the response rate was not higher, follow up telephone interviews were conducted with 100 randomly selected participants. Comments these individual provided, along with comments addressees emailed when they declined to participate, cited the following reasons when they chose not to respond:

1. Job responsibilities. Some individuals questioned whether their responses would be valid since they did not believe intelligence work was their primary role. This issue was also exacerbated by staff that previously served as intelligence workers, but had switched positions and no longer felt qualified to speak about intelligence issues.
2. The survey length. In order to fully explore the nature of and challenges to law enforcement intelligence work the survey instrument included 125 questions. Feedback

suggests individuals were uncomfortable committing to this task, especially when they were at work. As one informant remarked, "Thirty minutes is too long, there's no way I have time to take a survey for half an hour – we're under massive pressure as it is."

3. One response per agency. Several individuals declined because they knew a colleague from the same agency had already responded. One person even indicated his work group had instituted an informal policy whereby they only respond to one survey per week and this task is rotated around the group. While it is possible to control for a limited number of responses when departments are small, it becomes problematic in the case of larger organizations and fusion centers.
4. Security. A handful of individuals were concerned about the security implications of sharing information about intelligence activities outside of the law enforcement community. This was a surprising finding since the study aims to inform public policy by identifying general, not agency specific, trends about law enforcement intelligence work. However, even with the backing of the U.S. Department of Justice, there was skepticism about the legitimacy of the data collection exercise.

Despite a somewhat low response rate and given the reasons listed above, the data remains very unique and at the time of this paper, is the only national quantitative survey of fusion centers. To date, there has been little research on fusion centers in general and of the available research, the methodologies employed consist largely of personnel interview data (Fresenko, 2010; Graphia-Joyal, 2010, Ratcliffe & Walden, 2010), analysis of government or public reports (Harper, 2009; Saari, 2010), interviews of non-fusion center law enforcement (MacGregor, 2010), and quantitative analyses of information sharing practices of a single state fusion center (Nennema, 2008; Cooney, Rojek, and Kaminski, 2011).

Sample Demographics

National dispersion of responses was based on the 10 Federal Protective Service Homeland Security Regions[9]. It is suspected that due to federal involvement in information sharing initiatives, respondents working for fusion centers based in Region 3[10] provided the most (21.6%) responses followed by Region 9[11] (20.4%). The fewest responses (3.4%) came from Region 1[12]. Most fusion center personnel (48.0%) had held their position for between one and three years, in marked contrast to law enforcement workers (21.8%) who tended remain in the same role for more than ten years. Lastly, most of the respondents from both the fusion center sample (57.5%) and law enforcement sample (30.3%) indicated serving an administrative role. Supervisors also consisted of a large portion (29.3%) of the law enforcement respondents.

Results

As working relationships among agencies and the sharing of analytic products has been found to be predictive of successful information sharing practices among state and local law enforcement (Carter, 2011), the two critical areas to explore with respect to the current discussion are working relationships and the sharing of intelligence products among key stakeholders. Public health stakeholders include hospitals, public health agencies, public health officials, and state health departments. Results of the two data samples are provided consistent with this approach. Table 1 illustrates working relationships among public health stakeholders and different personnel in both the law enforcement and fusion center samples.

[Table 1 approximately here]

The sharing of actionable intelligence – the desired outcome of the information sharing initiatives described throughout this paper – rely largely on the efforts of intelligence analysts. As can be seen in Table 1, the majority of analysts in both fusion centers and law enforcement believe their working relationships with public health stakeholders is at best somewhat close and in much of the case, distant or non-existent. Intuitively, analysts are not very satisfied with these relationships. On the whole, fusion center personnel reported overall more positive working relationships with public health compared to law enforcement personnel. Again this is intuitive (and a good sign) as fusion centers are the primary entities tasked with the responsibility of developing and maintaining active relationships with the public health community. While clearly relationships among public health and law enforcement do exist, they are a far cry from being as close as one would expect to facilitate successful information sharing.

More direct indicators of the extent to which public health and homeland security are engaged in information sharing is the frequency by which they share information with one another, conduct sector-specific analysis, and have access to sector-specific information. Table 2 illustrates these indicators. On average, both law enforcement (78.2%) and fusion center (79.8%) personnel indicated they either infrequently or very infrequently provide intelligence to hospitals in their jurisdiction. These percentages are consistent with law enforcement's (78.7%) infrequently or very infrequently sharing of actionable intelligence to public health agencies and the state health department (79.8%) in their jurisdictions. An increase in the sharing of actionable intelligence with both public health agencies and state health departments was indicated by fusion center personnel as compared to the frequencies reported with respect to hospitals.

[Table 2 approximately here]

With regard to information access, only 18.8% of law enforcement agencies that employed either a full- or part-time intelligence analyst indicated their analyst had access to public health information as compared to 41.7% of fusion center personnel indicated analysts had access to this source of information. Again, it is expected that law enforcement in general will have less of an analytic capability compared to fusion centers as fusion centers primary function is to analyze disparate information from a variety of sources. Lastly, respondents in both samples were asked to indicate the frequency by which they conducted a variety of analytic techniques. Again, it is expected that law enforcement personnel (41.5%) conduct such analyses less often as compared to fusion centers (72.5%). However, it is worth noting that while the majority of fusion centers responded to having the capability to conduct health trend analysis, approximately one in every four of the fusion centers in the sample does not engage in this method of analysis. However, it is worth noting that 75.1% of the fusion centers indicating they did not engage in public health trend analysis also indicated they did not have access to public health information. While the data presented here is limited in detail, it does provide a glimpse of what is currently happening in the homeland security arena with respect to public health prevention and preparedness efforts. Implications of these insights will be discussed.

General observations from the data presented here indicate an existence of working relationships among public health stakeholders and law enforcement and fusion center personnel. Despite such relationships, there is a considerable gap with regard to tangible information sharing. Based on this data, it can be assumed there is significant room for improvement in these prevention and preparedness efforts.

Current Initiatives to Integrate Homeland Security and Public Health

As the data presented above illustrate, there is a lack of tangible cooperation among fusion centers, state and local law enforcement, and public health. Recognizing this gap, the Department of Homeland Security (DHS) and Centers for Disease Control and Prevention (CDC) have established initiatives in an attempt to remedy this shortcoming. There are currently four initiatives targeted towards this effort. To begin with, the concept of fusing information from multiple sources is not new to public health. In 2007 and 2008, the CDC established the Office of Critical Information Integration and Exchange (OCIIX). The mission of OCIIX is to accumulate and integrate CDC information and disseminate actionable products on emergent public health events using a meta-analytic approach to ensure all-hazards situation awareness (U.S. Government Printing Office, 2008). To this end, OCIIX was charged with establishing a new public health fusion program at the CDC, known as BioPHusion, to "incorporate information from multiple disparate data sources, facilitate the exchange of information across programs, and analyze aggregated interpreted data (information) from existing surveillance systems in order to enhance agency-wide situational awareness both domestically and globally" (Rolka, O'Conner & Walker, 2008, p.3). While BioPHusion is a robust source of information - a combination of 42 different biological related information systems - it lacks tangible information sharing components necessary to deliver its intended output. Worth noting, the model is designed to serve as a raw information collector and lacks the ability to identify intelligence requirements (e.g. desired information based on a given situation), incorporate micro-level information, establish horizontal information sharing partnerships, and employ an analytic process that yields an actionable result (Rolka, O'Conner, & Walker, 2008).

Second, the DHS created the *Health Security Intelligence Enterprise* (HSIE) to facilitate cooperation among public health and healthcare community (PH/HC) interests into the processes

of homeland security information and intelligence exchange. The establishment of an institutionalized health security information and intelligence sharing framework is designed to enhance the preparedness level of PH/HC practitioners across the country, while supporting the all-hazards approach to prevention, protection, response and recovery efforts of homeland security stakeholders (Riegle, 2009). Envisioned as a public health-specific version of the successful law enforcement *Program Manager's Information Sharing Environment* (Program Manager for the Information Sharing Environment, 2006b), it has been successful in bringing the importance of public health integration into the homeland security forefront. The HSIE is a step in the right direction and provides a formal foundation to foster collaboration among the key stakeholders, yet it lacks actionable guidelines for implementation. As a result, this initiative has yet to gain any notable traction.

Third, in March 2011 the Centers for Disease Control and Prevention (CDC) published the *Public Health Preparedness Capabilities: National Standards for State and Local Planning* – a national capabilities guide that provides actionable guidelines for public health to share information with homeland security entities. Modeled after the *Baseline Capabilities List* (U.S. Department of Justice, 2008) for law enforcement state and regional fusion centers, this document identifies 15 preparedness capabilities categorized under six domains[13] for state and local public health agencies. Each capability includes a definition of the capability and list of the associated functions, performance measures, tasks, and resource considerations for successful implementation. While the entire document is dedicated to integrating public health and national threat preparedness and prevention, each capability is predicated on the ability to share information across sectors. Specifically, this document identifies the capability of information for public health agencies as:

> "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 alerts to federal, state, local, territorial, and tribal levels of government and the private sector in preparation for, and in response to, events or incidents of public health significance" (Centers for Disease Prevention and Control, 2011e, p.55).

While each capability domain is an emphasis to communicate with all levels of law enforcement – specifically to have written directives to engage with such stakeholders – it lacks informed actionable functions for public health personnel to actually engage law enforcement in general, and fusion centers specifically. As a result, more substantive guidance is required to bridge public health and homeland security.

Lastly, the *Health Security: Public Health and Medical Integration for Fusion Centers* document published by the U.S. Department of Justice in July 2011 has established a structure by which public health information can be implemented into homeland security efforts through law enforcement state and regional fusion centers. Broadly, this initiative establishes functional guidelines by which public health and law enforcement can coordinate and conduct ongoing risk assessments, mutually access and participate in a fusion center's robust information sharing processes that allow the movement of relevant and timely information in support of threat awareness, and provide mutual access to tools and processes that allow for rapid adaptation to an evolving threat environment (U.S. Department of Justice, 2011). Perhaps the most salient aspect of this initiative is to provide a mechanism that not only incorporates disparate public health data sources, but does so in a manner that integrate this information with readily available homeland

security information in an environment where analytic techniques are commonplace. As it was noted, the BioPHusion program served as a robust source of health information, but it lacked the analytic capacity to synthesize this amount of information and communicate relevant information in a digestible and actionable format (e.g. an intelligence product).

This initiative acknowledges the critical importance that any use of health and medical data sources should be conducted in accordance with the federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. It is anticipated these initiatives are likely to enhance preparedness efforts as they are modeled in concert with existing law enforcement preparedness guidelines. Of the fusion center personnel surveyed in the data presented here, 94.9% believed the *Fusion Center Guidelines* (U.S. Department of Justice, 2003) and the *Baseline Capabilities List* (U.S. Department of Justice, 2008) were helpful in establishing operational components of their fusion centers.

Discussion and Conclusions

In sum, there remains an information sharing disconnect between public health and the entities tasked with homeland security preparedness. The data presented sheds light on the commonly held assumption that public health and homeland security are working together. While it appears willingness for such an effort exists, the data show a consistent lack of tangible information sharing among the two sectors. It is hypothesized that this disconnect can be traced back to the authority outlined in HSPD 21 in that the U.S. Department of Health and Human Services (HHS) was identified as the primary entity for creating an interoperable environment among all stakeholders. The underlying difficulty in this approach is that HHS' experience with information sharing up until this point has been one of vertical silo storage by disease category

for aggregate assessment – not the sharing of disparate sources of information across different organizations on a real-time basis. Furthermore, public health sectors have suffered from decreasing resources as well and may find it difficult to realign personnel and infrastructure to support a homeland security function. While the authority for leading the collaboration among all stakeholders legislatively remain with HHS, the initiatives currently underway have – from an operational perspective –transferred primary responsibility to the U.S. Department of Justice, U.S. Department of Homeland Security, and state and regional fusion centers who have an established culture of preparedness-based information sharing.

Perhaps the most significant barrier facing these efforts is the inability of public health information to achieve a necessary balance of specificity and sensitivity in the information that is collected. It is believed that with the integration of public health information into state and regional fusion centers it is likely to yield a collective increase in the sensitivity and specificity of identifying threats to public health and homeland security. An improvement in this effort is likely to occur as fusion centers provide a mechanism to increase both specificity and sensitivity since the amount of information available to both public health and homeland security is multiplied in combination with a homeland security infrastructure designed to share information in real-time.

Furthermore, these interoperable efforts on behalf of both public health and homeland security can be enhanced through emerging health liaison officer programs. Such programs are modeled after widely successful intelligence liaison officers and fusion center liaison officer programs currently utilized by law enforcement throughout the country. In short, a liaison officer is an individual(s) assigned to be the primary point of contact for sharing information between two organizations. In large metropolitan areas (where preparedness efforts have been

paramount), these programs are further enhanced from Urban Area Security Initiative (UASI) funding – a financial commitment[14] of resources to increase the overall level of preparedness in the United States' most populated areas. While the UASI regions tend to receive the bulk of preparedness attention, it is not only the large metropolitan areas that are having success with the liaison officer program.

A formalized example of this approach is currently being utilized by the New Hampshire Department of Health and Human Services which has created a Health Intelligence Liaison Unit designed to support information sharing among state and local government entities[15]. Aside from establishing a direct communicate link between health entities and fusion centers, health liaison officers are commonly recipients of regular information dissemination from fusion centers. The two methods of communication most commonly utilized in the liaison officer programs are e-mail and personal contact. Fusion center personnel included in the data presented in this paper indicated e-mail and personal contact were the two most commonly used mechanisms for distributing intelligence products. By establishing health officer liaison programs, public health entities can increase both the amount and quality of information they disseminate and receive. Such an effort is likely to improve a more sensitive, specific, and real-time information sharing capability among public health and law enforcement personnel – thus improving preparedness efforts.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the authorship and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research and/or authorship of this article: The study was supported by the National Institute of Justice, U.S. Department of Justice, grant number 2008-IJ-CX-0007.

Notes

1. A clarification on *information* versus *intelligence* is necessary as the two terms are commonly used interchangeably – which is incorrect. Information refers to raw pieces of information – or simply the facts. Intelligence refers to information or facts that have gone through some form of an analytic process to yield an actionable result. For purposes of information sharing within the public health sector and in many cases the state and local law enforcement sector, the sharing of *information* is paramount – not *intelligence* per se.
2. Biosphere refers to the earth's crust, waters, and atmosphere that support life and is the ecosystem comprising the entire earth and the living organisms that inhabit it.
3. Patient information refers to all information about the patient - including name, medical record number, condition, sex, age, physician name, diagnosis, medical unit, other treatment information, and simply the fact that the individual is being treated within a medical facility (The University of Chicago, 2007).
4. Law enforcement requests for patient information require law enforcement personnel to fill out patient information request forms that include fields to verify personnel and provide justification for such information. Examples of these forms can be found at: http://hipaa.bsd.uchicago.edu/Law_Enforce_CPDform.pdf and http://www.orpdmp.com/orpdmpfiles/PDF_Files/LE%20Info%20Request_v1.0.pdf
5. Codified as 28 CFR Part 23 "Criminal Intelligence Systems Operating Policies", this regulation governs inter-jurisdictional and multi-jurisdictional criminal intelligence systems that are operated by or on behalf of state and local law enforcement agencies and that are funded by or receive federal funds. Complete 28 CFR Part 23 information is available at: http://www.iir.com/28cfr/Laymensguide.pdf
6. Syndromic surveillance uses individual and population health indicators t to identify outbreaks or health events and monitor the health status of a community.
7. This research was support by funding from the National Institute of Justice, U.S. Department of Justice under grant number 2008-IJ-CX-0007 awarded in 2009. The views expressed in this paper are those of the authors and do not necessarily reflect the views of the U.S. Department of Justice or any of its agencies.
8. The National Fusion Center Conference is sponsored by the following agencies: Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice (DOJ), U.S. Department of Homeland Security, DOJ's Global Justice Information Sharing Initiative, Federal Bureau of Investigation, Office of the Director of National Intelligence, Office of the Program Manager, Information Sharing Environment, Bureau of Alcohol, Tobacco, Firearms and Explosives, Office of Community Oriented Policing Services.
9. For more information on, and a completed list of, the Federal Protective Service Homeland Security Regions visit: http://www.dhs.gov/files/reportincidents/gc_1268677752685.shtm
10. Federal Protective Service Homeland Security Region 3 includes: Delaware, Maryland, Virginia, Pennsylvania, and West Virginia.

11. Federal Protective Service Homeland Security Region 9 includes: California, Arizona, Nevada, and Hawaii.
12. Federal Protective Service Homeland Security Region 1 includes: Massachusetts, Vermont, New Hampshire, Maine, Rhode Island, and Connecticut.
13. The six domains for public health preparedness are: Biosurveillance, Community Resilience, Countermeasures and Mitigations, Incident Management, Information Management, and Surge Management.
14. The Urban Area Security Initiative from the Department of Homeland Security awarded $662,622,100 in the 2011 fiscal year to increase threat prevention efforts. For more information visit: http://www.fema.gov/government/grant/hsgp/#2
15. For more information on the New Hampshire Department of Health and Human Services, Health Liaison Officer Unit visit: http://www.dhhs.state.nh.us/dphs/liaison.htm

References

Alexander, G. C., Larkin, G. L. & Wynia, M. K. (2006). Physicians' preparedness for bioterrorism and other public health priorities. *Academic Emergency Medicine*, 13(1), 1238–1241.

Barr, C., Hoefer, D., Cherry, B., & Noyes, K. A. (2011). A process evaluation of an active surveillance system for hospitalized 2009-2010 H1N1 influenza cases. *Journal of Public Health Management* & Practice, 17(1), 4–11.

Brito, C. S., Luna, A. M., & Sandberg, E. L. (2009a). *Communication and Public Health Emergencies: A Guide for Law Enforcement*. Washington, DC: Police Executive Research Forum. Retrieved from http://www.ojp.usdoj.gov/BJA/pdf/PERF_Emer_Comm.pdf

Brito, C. S., Luna, A. M., & Sandberg, E. L. (2009b). *Benchmarks for Developing a Law Enforcement Pandemic Flu Plan.* Washington, DC: Police Executive Research Forum. Retrieved from http://www.ojp.usdoj.gov/BJA/pdf/PERF_PandemicBenchmarks.pdf

Burress, G. W., Giblin, M. J. & Schafer, J. A. (2010). Threatened globally, acting locally: Modeling law enforcement homeland security practices. *Justice Quarterly*, 27(1), 77-101.

Butler, J. C., Cohen, M. L., Friendman, C. R., Scripp, R. M., & Watz, C. G. (2002). Collaboration between public health and law enforcement: New paradigms and partnerships for bioterrorism planning and response. *Emerging Infectious Diseases*, 8(10), 1152-1156.

Carter, J. G. (2011). *Policing Innovation: Exploring the Adoption of Intelligence-Led Policing*. Dissertation. East Lansing, MI: School of Criminal Justice. Michigan State University.

Carter, D. L. & Carter, J. G. (2009a). The intelligence fusion process for state, local and tribal law enforcement. *Criminal Justice and Behavior*, 36(12), 1323-1339.

Carter, D. L. & Carter, J. G. (2009b). Intelligence-led policing: Conceptual considerations for public policy. *Criminal Justice Policy Review*, 20(3), 310-325.

Castillo-Salgado, C. (2010). Trends and directions of global public health surveillance. *Epidemiological Review*, 32(1), 93-109.

Centers for Disease Control and Prevention. (2004). *Framework for Evaluating Public Health Surveillance Systems for Early Detection of Outbreak*. Washington, DC: U.S. Department of Health and Human Services. Retrieved from: http://www.cdc.gov/Mmwr/preview/mmwrhtml/rr5305a1.htm

Centers for Disease Control and Prevention. (2011a). *BioSense Fact Sheet*. Washington, DC: U.S. Department of Health and Human Services. Retrieved from http://www.cdc.gov/biosense/files/BiosenseFactsheet.pdf

Centers for Disease Control and Prevention. (2011b). Public health then and now: Celebrating 50 years of MMWR at CD. *U.S. Morbidity and Mortality Weekly Report*, 60. Washington, DC: U.S. Department of Health and Human Services. Retrieved from http://www.cdc.gov/mmwr/pdf/other/su6004.pdf

Centers for Disease Control and Prevention. (2011c). *Summary of Notifiable Diseases: United States 2009*. Washington, DC: U.S. Department of Health and Human Services. Retrieved from http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5853a1.htm?s_cid=mm5853a1_w

Centers for Disease Control and Prevention. (2011d). *Public Health Informatics and Technology Program Office*. Washington, DC: U.S. Department of Health and Human Services. Retrieved from http://www.cdc.gov/ostlts/hop/pdfs/PHITPO_Factsheet.pdf

Centers for Disease Control and Prevention. (2011e). *Public Health Preparedness Capabilities: National Standards for State and Local Planning*. Washington, DC: U.S. Department of Health and Human Services. Retrieved from http://www.cdc.gov/phpr/capabilities/DSLR_capabilities_July.pdf

Cooney, M., Rojek, J., and Kaminski, R. J. (2011). An assessment of the utility of a state fusion center by law enforcement executives and personnel. *International Association of Law Enforcement Intelligence Analysts Journal*, 20(1), 1-18.

Danos, C. S. & Hancock, D. (2009). *Transforming Public Health Systems to Meet Today's Health Threats*. Oracle White Paper Series. Retrieved from http://www.oracle.com/us/industries/healthcare/046186.pdf

Fresenko, V. L. (2010). *Social Media Integration into State-Operated Fusion Centers and Local Law Enforcement. Potential Uses and Challenges*. Master's Thesis. Monterey, CA: Naval Post Graduate School.

Goldstein, B. D. (2010). *BioWatch and Public Health Surveillance: Evaluating Systems for the Early Detection of Biological Threats*. Institute of Medicine and National Research Council of the National Academes. Washington, DC: National Academy Press.

Graphia-Joyal, R. (2010). Are fusion centers achieving their intended purposes? Findings from a qualitative study on the internal efficacy of state fusion centers. *International Association of Law Enforcement Intelligence Analysts Journal*, 19(1): 54-76.

Harper, J. L. (2009). *Fusion Center Privacy Policies: Does One Size Fit All?*. Master's Thesis. Monterey, CA: Naval Post Graduate School.

Homeland Security Advisory Council. (2005*). Intelligence and Information Sharing Initiative: Homeland Security Intelligence an Information Fusion*. Washington, DC: U.S. Department of Homeland Security. Retrieved from http://www.dhs.gov/xlibrary/assets/HSAC_HSIntelInfoFusion_Apr05.pdf

Hsu, C. E., Chambers, W. C., Herbold, J. R., Calcote, J. C., Ryczak, R. S. & DeFraites, R. F. (2010). Towards shared situational awareness and actionable knowledge: An enhanced, human-centered paradigm for public health information system design. *Journal of Homeland Security and Emergency Management*, 7(1), 1-13.

Koh, H. K., Elqura, L. J., Judge, M. C., & Stoto, M. A. (2008). Regionalization of local public health systems in the era of preparedness. *Annual Review of Public Health*, 29, 205-218.

Macario, E., Heyden, L., Nakahara, N., & Macias-Reynolds, V. (2009). Preparing for pandemic influenza: California confronts the legal implications. *Health Promotion Practice*, 10(4), 573-578.

MacGregor, D. S. (2010). *Fusion 2.0: The Next Generation of Fusion in California: Aligning State and Regional Fusion Centers*. Master's Thesis. Monterey, CA: Naval Post Graduate School.

Masse, T., & Rollins, J. (2007). *A Summary of Fusion Centers: Core Issues and Options for Congress*. Washington, DC: Congressional Research Service. Retrieved from http://www.fas.org/sgp/crs/intel/RL34177.pdf

McHugh, M., Staiti, A. B., & Feeland, L. E. (2004). How prepared are Americans for public health emergencies? Twelve communities weigh in. *Health Affairs*, 23(3), 201-209.

Merrill, J., Caldwell, M., Rockoff, M. L., Gebbie, K., Carley, K. M., & Bakken, S. (2008). Findings from an organizational network analysis to support local public health management. *Journal of Urban Health*, 85(4), 572–584.

Morrow, C. B. & Novick, L. F. (2005). A case exercise in public health preparedness: A community outbreak of influenza-like illness. *Journal of Public Health Management & Practice*, 11(4), 306-310.

Nelson, C., Lurie, N. & Wasserman, J. (2007). Assessing public health emergency preparedness: Concepts, tools, and challenges. *Annual Review of Public Health*, 28(1), 1-18.

Nennema, M. (2008). *An Examination of State and Local Fusion Centers and Data Collection Methods*. Master's Thesis. Monterey, CA: Naval Post Graduate School.

Olson, D. (2007). *Public Health Emergency Preparedness: Disease Surveillance Skill Development Guide*. Minneapolis, MN: Center for Public Health Preparedness. University of Minnesota. Retrieved from http://www.sph.umn.edu/ce/tools/docs/phet/disease_surveillance.pdf

Program Manager for the Information Sharing Environment. (2006a). *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment*. Washington, DC: Office of the Director of National Intelligence. Retrieved from http://www.ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf

Program Manager for the Information Sharing Environment. (2006b). *Information Sharing Environment Implementation Plan*. Washington, DC: Office of the Director of National Intelligence. Retrieved from http://www.ncirc.gov/documents/public/Final_ISE_IP.pdf

Ratcliffe, J. H. & Walden, K. (2010). State police and the intelligence center: A study of intelligence flow to and from the street. *International Association of Law Enforcement Intelligence Analysts Journal*, 19(1): 1-19.

Richards, E. P., Rathbun, K. C., Brito, C. S., & Luna, A. (2006). *The Role of Law Enforcement in Public Health Emergencies: Special Considerations for an All-Hazards Approach*. Washington, DC: Bureau of Justice Assistance. U.S. Department of Justice. Police Executive Research Forum. Retrieved from https://www.ncjrs.gov/pdffiles1/bja/214333.pdf

Riegle, R. (2009). *The Future of Fusion Centers: Potential Promise and Dangers*. Testimony of Director Robert Riegle. Committee on Homeland Security. Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Washington, DC: U.S. Department of Homeland Security. Retrieved from http://www.dhs.gov/ynews/testimony/testimony_1238597287040.shtm

Rolka, H., O'Conner, J. C., & Walker, D. (2008). Public Health Information Fusion for Situation Awareness. In D. Zeng, H. Chen, & H. Rolka (Eds.), *Biosurveillance and Biosecurity*. Raleigh, NC: Springer.

Saari, S. C. (2010). *Fusion Centers: Securing America's Heartland From Threats.* Master's Thesis. Monterey, CA: Naval Post Graduate School.

Sandberg, E. L., Brito, C. S., Luna, A. M., & McFadden, S. M. (2010). *A Guide to Occupational Health and Safety for Law Enforcement Executives*. Washington, DC: Police Executive Research Forum. Retrieved from http://www.ojp.usdoj.gov/BJA/pdf/PERF_LE_OccHealth.pdf

Sarpy, S. A., Warren, C. R., Kaplan, S., Bradley, J., & Howe, R. (2005). Simulating public health response to a Severe Acute Respiratory Syndrome (SARS) event: A comprehensive and systematic approach to designing, implementing, and evaluating a tabletop exercise. *Journal of Public Health Management & Practice*, 11(6), 75-82.

Sprange, C. B., Villegas, D., Kazda, M. J., Harris, A. M., Mathew, S., & Migala, W. (2007). Assessment of physician preparedness and response capacity to bioterrorism or other public health emergency events in a major metropolitan area. *Disaster Management & Response*, 5(3), 82-86.

Sullivan, J. P. (2005). *Terrorism Early Warning and Co-production of Counterterrorism Intelligence*. Paper presented at the Canadian Association of Security and Intelligence Studies, Montreal. Quebec, Canada.

U.S. Congress. (2004). *Intelligence Reform and Terrorism Prevention Act*. Washington, DC: 108th U.S. Congress. Retrieved from http://www.nctc.gov/docs/irtpa.pdf

U.S. Congress. (2007). *Implementing Recommendations of the 9/11 Commission*. Washington, DC: 110th Congress. Retrieved from http://intelligence.senate.gov/laws/pl11053.pdf

U.S. Department of Health and Human Services. (2010). National Biosurveillance Strategy for Human Health. Washington, DC: Centers of Disease Control and Prevention. Retrieved from http://www.cdc.gov/osels/pdf/NBSHH_V2_FINAL.PDF

U.S. Department of Homeland Security. (2008). *A National Response Framework*. Washington, DC: Department of Homeland Security. Retrieved from http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf

U.S. Department of Homeland Security. (2010). *IT Program Assessment: OHA – BioWatch Gen-3*. Washington, DC: Department of Homeland Security. Retrieved from http://www.dhs.gov/xlibrary/assets/mgmt/itpa-oha-biowatchgen2010.pdf

U.S. Department of Homeland Security. (2011a). *Department of Homeland Security Strategic Sustainability Performance Plan*. Washington DC: Department of Homeland Security. Retrieved from http://www.dhs.gov/xlibrary/assets/mgmt/dhs-2011-strategic-sustainability-performance-plan.pdf

U.S. Department of Homeland Security. (2011b). *Implementing 9/11 Commission Recommendations: Progress Report 2011*. Washington DC: Department of Homeland Security. Retrieved from http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf

U.S. Department of Homeland Security. (2011c). *Office of Health Affairs*. Washington DC: Department of Homeland Security. Retrieved from http://www.dhs.gov/xabout/structure/editorial_0880.shtm

U.S. Department of Justice. (2003). *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, DC: Global Intelligence Working Group. U.S. Department of Justice. Retrieved from http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

U.S. Department of Justice. (2008). *Baseline Capabilities for State and Major Urban Area Fusion Centers*. Washington, DC: Global Intelligence Working Group. U.S. Department of Justice. Retrieved from http://www.fema.gov/pdf/government/grant/2011/fy11_hsgp_fusion.pdf

U.S. Department of Justice. (2011). *Health Security: Public Health and Medical Integration for Fusion Centers*. Washington, DC: Global Intelligence Working Group. U.S. Department of Justice. Retrieved from http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181

U.S. Government Accountability Office. (2009). *Developing a Collaboration Strategy Is Essential to Fostering Interagency Data and Resource Sharing*. Washington, DC:

Government Accountability Office. Retrieved from http://www.gao.gov/new.items/d10171.pdf

U.S. Government Accountability Office. (2011). *The Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11*. Washington, DC: Government Accountability Office. Retrieved from http://www.gao.gov/new.items/d11881.pdf

U.S. Government Printing Office. (2008). Department of Health and Human Services. Centers for Disease Control and Prevention. Statement of Organization, Functions, and Delegations of Authority. *Federal Register*, 73(96). Retrieved from http://edocket.access.gpo.gov/2008/pdf/E8-10986.pdf

U.S. House of Representatives, (2009). *Health Information Technology for Economic and Clinical Health Act or HITECH Act*. Committee on Ways and Means. Washington, DC. Retrieved from http://waysandmeans.house.gov/media/pdf/110/hit2.pdf

U.S. House of Representatives. (2011). *6 USC Chapter 1: Homeland Security Organization*. Washington, DC. Retrieved from http://uscode.house.gov/download/pls/06C1.txt

Wagner, M. M., Moore, A. W., & Aryel, R. M. (2006). *Handbook of Biosurveillance*. Maryland Heights, MO: Academic Press.

Watkins, S. M., Perrotta, D. M., Stanbury, M., Heumann, M., Anderson, H., Simms, E., and Huang, M. (2011). State-level emergency preparedness and response capabilities. *Disaster Medicine and Public Health Preparedness*, 5(1), 134-142.

The University of Chicago. (2007). *Law Enforcement Access to Patients and Patient Information*. Chicago, IL: The University of Chicago HIPAA Program Office. Retrieved from http://hipaa.bsd.uchicago.edu/law_enforce.html

The White House. (2004). *Biodefense for the 21st Century*. Washington, DC. Office of the President. The White House. Retrieved from http://www.dhs.gov/xlibrary/assets/HSPD10Biodefensefor21stCentury042804.pdf

The White House. (2007). *Homeland Security Presidential Directive 21*. Washington, DC. Office of the President. The White House. Retrieved from http://www.fas.org/irp/offdocs/nspd/hspd-21.htm

Table 1. Information Sharing Relationships by Personnel

Question	**Administrators** Fusion Center (Law Enforcement)	**Supervisors** Fusion Center (Law Enforcement)	**Investigators** Fusion Center (Law Enforcement)	**Analysts** Fusion Center (Law Enforcement)
How close is the working relationship between your organization and hospitals?				
Very Close	19.2% (25.8%)	16.7% (26.4%)	16.6% (23.6%)	0% (15.8%)
Somewhat Close	34.0% (42.7%)	61.1% (37.9%)	66.7% (41.5%)	40.0% (24.6%)
Distant	31.9% (21.8%)	22.2% (19.5%)	16.7% (21.7%)	30.0% (47.4%)
No Relationship	14.9% (9.7%)	0% (16.2%)	0% (13.2%)	30.0% (12.2%)
How close is the working relationship between your organization and public health agencies?				
Very Close	47.9% (26.4%)	27.7% (19.5%)	16.6% (23.6%)	10.0% (22.8%)
Somewhat Close	25.0% (44.7%)	55.6% (46.0%)	66.7% (37.3%)	50.0% (15.8%)
Distant	16.7% (22.3%)	16.7% (21.9%)	16.7% (28.2%)	30.0% (54.4%)
No Relationship	10.4% (6.6%)	0% (12.6%)	0% (10.9%)	10.0% (7.0%)
How satisfied are you in the relationship you have with public health officials in your state?				
Very Satisfied	21.3% (17.1%)	10.5% (5.6%)	0% (6.8%)	0% (6.0%)
Satisfied	46.8% (60.5%)	73.7% (58.4%)	85.7% (48.3%)	40.0% (41.8%)
Not Satisfied	29.8% (11.6%)	10.5% (23.6%)	14.3% (24.6%)	50.0% (13.4%)
No Relationship	2.1% (10.8%)	5.3% (12.2%)	0% (20.3%)	10.0% (38.8%)

Table 2. Information Sharing Actions

Question	State, Local, Tribal Law Enforcement	Fusion Center
How often do you provide actionable intelligence to hospitals?		
Very Frequently	5.3%	3.7%
Frequently	16.5%	16.5%
Infrequently	37.7%	49.4%
Very Infrequently	40.5%	30.4%
How often do you provide actionable intelligence to public health agencies?		
Very Frequently	5.3%	8.7%
Frequently	16.2%	31.3%
Infrequently	36.9%	41.3%
Very Infrequently	41.6%	18.7%
How often do you receive actionable intelligence from the state health department?		
Very Frequently	4.5%	6.4%
Frequently	15.7%	29.5%
Infrequently	37.0%	37.2%
Very Infrequently	42.8%	26.9%
Analysts have access to public health information.		
Yes	18.8%	41.7%
Do the person(s) responsible for conducting intelligence-related analysis in your agency perform public health trend analysis?		
Yes	41.5%	72.5 %