Public Health Collection, Use, Sharing, and Protection of Information

Issue Brief

Introduction

Public health agencies need to collect, use, and share information to prevent disease and injury and protect the public against health threats. Information is essential to every aspect of emergency preparedness and response, including for example:

- Information about community needs and resources for planning, response, and recovery
- Surveillance and reporting data for early detection of a disease outbreak or other threat
- Medical information, biospecimens, environmental samples, and other information acquired through investigation to determine the source and nature of the threat
- Test results and expert analyses to determine and take appropriate action and monitor results
- Information sharing among public health agencies, with law enforcement, healthcare providers and other stakeholders for prevention, investigation, and response
- Contact identification and follow-up to contain the spread of disease and ensure treatment
- Informational alerts and advisories to coordinate response and communicate with the public
- Post-incident data to measure, evaluate, and improve preparedness

Often, public health agencies need to collect, use, and share personal and health information that identify individuals. To prevent and manage a public health emergency, agencies must understand federal and state laws that apply to this information. When responding to a public health threat, public health officials must understand both their authority and their responsibilities. An important responsibility of public health officials is to protect the privacy of individuals. This responsibility must be balanced against the responsibility to protect the public and inform it of public health threats within the community. Agencies must also understand laws that define the public's right to information held by government and exemptions that might apply to protect sensitive or private information from public disclosure.

This issue brief covers legal authorities to collect and use identifiable information through surveillance, inspections and investigations, to share information for emergency preparedness and response, and to withhold information to protect individual privacy or the national security.

I. Legal Authority to Collect, Use, and Share Information to Protect the Public

States may exercise police powers to protect the public's health and safety. Police powers include basic communicable disease control activities to protect the public against natural, accidental, or intentional threats. Historically, the U.S. Supreme Court has held that states may enact laws that restrict individual liberties when necessary to protect the community. In *Jacobson v. Massachusetts*,[1] the Supreme Court upheld a mandatory vaccination law to protect the community against smallpox. It follows that states may enact laws to require reporting of private health data, search medical and hospital records to locate information about the source and spread of communicable disease, collect and test specimens, and disclose information to the extent necessary to protect the public from communicable diseases and other public health threats.

II. Legal Authority for Public Health Surveillance

Public health surveillance is the ongoing systematic collection, analysis, and interpretation of outcome-specific data for use in the planning, implementation, and evaluation of public health practice. The value of public health surveillance is closely linked to the timely dissemination of data and information about health events to those responsible for prevention and control.[2] Data for public health surveillance are provided from many and diverse sources and may or may not be identifiable to an individual.

Case Reports

Case reports are critical to detection and control of epidemics, food borne illness, chemical exposures, environmental contamination, and other public health threats. All states have enacted laws to mandate reporting of specific diseases or clusters of diseases to state or local health departments. Mandatory reporting typically applies to healthcare providers and laboratories. Other entities may also have reporting obligations, such as schools, day care centers, or camps. Since diseases that are considered notifiable are determined by state law, they vary from state to state.[3]

Case reports allow state and local public health authorities to identify and investigate cases, monitor the spread of disease, and implement control strategies as indicated. Control strategies include monitoring, contact tracing, treatment, quarantine, isolation, and use of pharmaceutical countermeasures when available.[4] Because of these uses, case reports include identifiable information.

States have also enacted reporting requirements beyond specific diseases that indicate a public health threat. These laws vary in coverage and detail. For example, reporting may be required for "outbreaks and single cases of diseases of public health importance" (Maryland);[5] "any outbreak or suspected outbreak, including, but not limited to, foodborne, waterborne, or nosocomial disease or a suspected act of bioterrorism" (New Jersey);[6] "unusual occurrence of a disease, infection or condition" (Pennsylvania);[7] and "all cases of known or suspected contagious or infectious diseases . . . all cases of persons who harbor any illness or health condition that may be caused by chemical terrorism, radiological terrorism, epidemic or pandemic disease, or novel and highly fatal infectious agents and might pose a substantial risk of a significant number of human fatalities or incidents of permanent or long-term disability" (South Carolina).[8]

Syndromic Surveillance

In addition to case reports, a few states mandate reporting to electronic syndromic surveillance systems. Syndromic surveillance systems detect clinical case features that are discernible before confirmed diagnoses are made.[9] Data provided may be de-identified or identifiable. Syndromic surveillance systems focus on routinely gathered information that indicate an emerging disease or other public health threat, such as fever, rash, gastrointestinal illness, and respiratory conditions.[10] These systems provide health data in real time to facilitate immediate analysis and feedback to those charged with investigation and follow-up of potential outbreaks.[11] Data may include patient's chief complaints in emergency departments, clinical impressions on ambulance log sheets, laboratory test orders, prescriptions filled, and over-the-counter prescription sales and products (e.g. thermometers). Public health agencies may monitor additional data sources not specific to disease syndromes, such as school or work absenteeism.[12] Health agency staff, assisted by automated data acquisition and generation of statistical alerts, are able to make inquiries or investigate the public health significance of any anomalies.

Nebraska[13] and North Carolina[14] have passed laws requiring that their state health department establish a syndromic surveillance system and specify by rule data elements that hospital emergency departments must report to the system. North Carolina's law expressly prohibits collection of personal identifiers. Both states' laws make syndromic surveillance confidential, although de-identified data may be provided to the CDC.

States without express mandates regarding syndromic surveillance may request data pursuant to general public health powers or public health surveillance authority. Data may be submitted without personal identifiers, although indirect identifiers may be necessary to re-identify individuals for investigation should an outbreak be indicated. Without personal identifiers, syndromic surveillance data should not threaten individual privacy. However, data may include proprietary information that business data sources may want protected from disclosure to their competitors or the general public. Absent clear statutory protection, public health agencies may want to execute datasharing agreements with data sources that include confidentiality provisions to the extent allowed by law.

Electronic Health Information

Information technology has increased the ease and utility of obtaining and disseminating information.[15] Public health surveillance is expected to improve due to increased use of electronic health records (EHR) and electronic exchange of health information. The Health Information Technology for Economic and Clinical Health Act (HITECH),[16] part of the American Recovery and Reinvestment Act of 2009,[17] provides financial incentives to eligible healthcare providers that implement and meaningfully use certified EHR technology. To demonstrate meaningful use, eligible providers select among a menu set of objectives and measures, which must include at least one public health objective. The three public health objectives in the Stage 1 menu set are submission of electronic data to public health in the context of 1) immunizations, 2) reportable laboratory results (eligible hospitals only), and 3) syndromic surveillance.[18]

Data Collection and Right to Privacy

The U.S. Supreme Court has upheld public health surveillance and reporting requirements against challenges based on individual privacy. Although privacy is not explicitly covered, the U.S. Constitution provides a limited right to privacy, including "informational privacy."[19] However, public health reporting requirements and access to health information are permissible when they are reasonably directed to the preservation of health and properly respect a patient's confidentiality and privacy.[20] For this reason, in *Planned Parenthood of Central Missouri v Danforth*,[21] the Supreme Court upheld recordkeeping and reporting requirements and public health authority to review required records related to abortion.

In *Whalen v Roe,*[22] the Supreme Court upheld a state law that required physicians who prescribed Schedule II controlled substances to provide a copy of those prescriptions to the New York State Department of Health. The law was intended to prevent the diversion of drugs into "unlawful channels" by preventing individuals from obtaining controlled substances from more than one physician or using stolen or altered prescriptions, preventing pharmacists from refilling dangerous prescriptions, and preventing physicians from over-prescribing. The Court rejected privacy challenges to the law's requirement that patients' names and addresses be collected and retained by the state, finding the requirement a reasonable exercise of the state's broad police powers. Requiring such disclosures to representatives of the state having responsibility for the health of the community, does not automatically amount to an impermissible invasion of privacy. The Court held that the reporting requirement was not "meaningfully distinguishable from a host of other unpleasant invasions of privacy that are associated with many facets of healthcare" comparing it to "reporting requirements relating to venereal disease, child abuse, injuries caused by deadly weapons, and certifications of fetal death."[23]

While the Court upheld the reporting requirement at issue in *Whalen v Roe*, it recognized that the government's right to accumulate great quantities of information – much of which is personal in character and potentially embarrassing or harmful if disclosed – has bounds. "The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures." The New York statutory scheme, and its implementing procedures, showed a proper concern with, and protection of, an individual's interest in privacy. Thus, the Court need not, and did not, "decide any question which might be presented by the unwarranted disclosure of accumulated private data – whether intentional or unintentional – or by a system that did not contain comparable security provisions."[24]

III. Legal Authority for Public Health Investigations

When surveillance systems, whether formal or informal or at the state, local or federal level, do detect cases or clusters of usual disease or other potential health threats, a public health investigation may be triggered. A public health investigation involves confirming the occurrence of an outbreak through active data and information gathering, identifying and characterizing cases of disease, developing and testing hypotheses explaining the cases, and, finally, implementing control measures to inhibit the further spread of the disease or condition as needed.[25]

Investigations are usually conducted by state and/or local public health agencies, which provide front-line detection and response to public health threats. The CDC may provide consultation or assistance at the request of the state public health agency or become involved with large scale threats, especially if they involve more than one state. Other federal agencies may be involved with investigating and responding to threats, such as the Food and Drug Administration (FDA) or the United States Department of Agriculture (USDA) when the threats involve foods or other products under their jurisdiction.[26]

State laws provide general legal authority to public health agencies to investigate the causes of disease, illness, disability, or other conditions. State laws may also include more specific investigative provisions. For example, under Michigan's Public Health Code, state and local health departments "may inspect, investigate, or authorize an inspection or investigation to be made of any matter, thing, premises, place, person, record, vehicle, incident, or event."[27]

During an investigation, public health investigators may need to enter and search the premises of an individual or business, copy records, take biological specimens or environmental samples for testing, and remove evidence that might be relevant to the public health concern. Usually, individuals, families, and businesses cooperate with public health investigations by providing access to premises, records, samples and specimens. However, absent consent, public health officials may need to obtain an administrative warrant to search premises and obtain evidence. A knowing and voluntary consent by an individual with actual or apparent authority over the premises to be searched or items to be seized is an exception to the warrant requirement established by the United States Constitution.[28]

The Fourth Amendment of the U.S. Constitution protects against unreasonable searches and seizures and requires a warrant:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

A search occurs when government action infringes upon an expectation of privacy that society recognizes as reasonable, for example, an individual's expectation of privacy in their home, business, vehicle, and person.[29]

Searches also include the collection and subsequent analysis of biological samples.[30] A seizure occurs when government action meaningfully interferes with an individual's possessory interest in property, for example, seizure of items that belong to the individual. The basic purpose of this Amendment is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials. Absent an exception, the Fourth Amendment applies to health and safety inspections and to public health investigations, requiring an administrative warrant. However, the standard for an administrative warrant is not as high as it is for criminal investigations. In administrative searches, probable cause is supported not by the traditional definition of likelihood to believe that evidence of a crime will be found in the area to be searched, but rather probable cause is satisfied by reasonable legislative or administrative standards for conducting an area search with respect to a particular dwelling.[31]

Generally, the Fourth Amendment warrant requirement does not apply to information provided by third parties. Mandatory reporting schemes for information obtained by medical personnel during the ordinary course of treatment do not violate the Fourth Amendment, even if that information is ultimately provided to law enforcement.[32] Even so, Fourth Amendment protection may apply if medical providers or public health investigators are too closely involved with law enforcement activities or their immediate objective is to generate evidence for law enforcement purposes. For example, the U.S. Supreme Court held that public hospital employees violated pregnant women's Fourth Amendment rights by testing their blood for cocaine. While the testing program might result in drug abuse treatment for some women – thereby benefitting the patient, their unborn child, and public health – the program was designed to collect evidence that would be turned over to the police for potential criminal prosecution.[33]

If an official fears that evidence may be destroyed or moved, he or she may wish to obtain an administrative warrant, rather than simply asking the owner or third party for permission to search. With a warrant, investigators may be accompanied by law enforcement for assistance, if necessary, to execute the warrant and seize evidence within the warrant's purview. State law should be reviewed to determine the requirements and process for obtaining and executing an administrative warrant.

Although not constrained by the Fourth Amendment, at times, individuals or organizations may request "legal process" before turning over property or information they hold about others to protect themselves against claims of wrongdoing. For example, in 2004, state health departments in Iowa and Michigan requested that Northwest Airlines provide contact information for passengers and crew aboard flights that landed in their respective states after it was determined that a passenger with measles was aboard those flights. The state health departments requested this information to contact individuals to inform them of exposure and provide information on reducing the possibility of illness. In response to the airline's concerns about privacy interests, each state used legal process under their respective state's law to compel disclosure of contact information: Iowa's health department obtained a court subpoena whereas Michigan's health department issued an imminent danger order.[34]

Fourth Amendment constitutional law is complicated and a court's determination may be difficult to predict for a specific case. Whether public health action is a "search" (i.e. infringes upon an expectation of privacy that society recognizes as reasonable), satisfies warrant requirements, or meets an exception depend on facts and context and balancing various interests. Additionally, while a public health search may be allowed by the Fourth amendment, state requirements may exceed federal constitutional requirements. Public health agencies should work closely with legal counsel to ensure that their investigations comport with the Fourth Amendment, especially when criminal activities are implicated. For additional information about public health investigations and the Fourth Amendment, see *Authorities and Limitations in Sharing Information Between Public Health Agencies and Law Enforcement Issue Brief*.

IV. Legal Authority for Public Health Sharing of Information

Public health agencies must often decide what information, if any, to share outside the public health agency. They may face competing interests when trying to protect individual privacy, protect the public, and inform the public.

Few states have laws that comprehensively address both public health privacy and disclosure.[35] According to one study, after personally identifiable health information is reported to or collected by a state health department, half of the states have no statutory provision or clearly applicable case law that imparts a continuing expectation or presumption of privacy or confidentiality of that information. Such information may be used and disclosed by state health officials in ways that, although it may be bounded by ethical expectations or practices, is subject to few legal restrictions. Some of these states do have limited protections, but they only apply to specific diseases or conditions, such as HIV, STDs, or tuberculosis.[36]

Privacy protections are important to ensure the public's trust and protect individuals from embarrassment, discrimination, and stigma. At the same time, exceptions are necessary to address rare but compelling situations where necessary to protect the public's health. Twenty-three of the twenty-five states with privacy protections allow health departments to disclose identifiable information, without consent, when necessary to protect the public. Three states (Maryland, Nebraska, and New Hampshire) have no statutory exception for disclosure to protect the public health. Similarly, most of these states lack law regarding the sharing of information about potential disease outbreaks and other public health events among public health agencies, between law enforcement and public health within each state, and between each state and the federal government. The law in Oregon is an example that appears to cover all needed exceptions to privacy. The Oregon Revised Statutes provide that "information obtained by the Oregon Health Authority or a local public health administrator in the course of an investigation of a reportable disease or disease outbreak is confidential" although several enumerated exceptions allow release of the minimum amount of information necessary to state and federal agencies, healthcare workers, persons with communicable diseases, and to certain others if there is "clear and convincing evidence that the release is necessary to avoid an immediate danger to other individuals or to the public."[37]

There may be rare, but compelling circumstances, where disclosure may be necessary, even though state law provides no applicable exception to privacy protections. If time permits, public health officials might seek a court order authorizing disclosure without consent. At some point, ethical considerations may dictate disclosure to warn third parties or the community of an imminent threat. In the mental health field, legal and ethical principles have developed regarding a duty to warn third parties of potential danger based on information learned in providing treatment. This "duty to warn" evolved from the California Supreme Court's decision in *Tarasoff v Regents of the University of California*,[38] which held that a mental health professional has a "duty to protect victims" who are being threatened with bodily harm by their patient. A health officer facing a decision about revealing confidential information to protect a third party or the general community should consult with his or her attorney to identify relevant legal responsibilities and evaluate competing moral claims. The situation and bases for action should be documented in case subsequent events lead to second guessing.

Public health agencies must often decide whether to share identifiable information with other entities in the public and private sector that have a role in protecting or providing for the public's health, safety, and welfare. Potential partners for sharing information are numerous including, for example, other public health

agencies, governmental agencies that protect and regulate food sources, animal health, and the environment, social services agencies, emergency management and homeland security departments, law enforcement, and the healthcare sector. Some states have statutory language recognizing the need to share information to investigate and respond to a threat; other states may rely on their general authority to support such sharing. When identifiable information is not necessary, public health agencies might be able to avoid legal questions by simply providing de-identified information.

Most, if not all, state public health agencies support national public health surveillance by voluntarily sharing a portion of their data with the Centers for Disease Prevention and Health Promotion (CDC). The data from states are used by CDC to evaluate disease trends, publish aggregate data, assess the effectiveness of prevention and control measures, identify populations or geographic areas at high risk, formulate prevention strategies, develop public health policies, and work with the international community to identify and contain global outbreaks.[39] For national reporting, personally identifiable information is generally unnecessary and CDC does not request it for this purpose.

Public health agencies must also decide what information to share with the public and the media and the timing of such disclosures, especially when information is preliminary or incomplete. Communication with the public is crucial, especially in times of crisis. Requests for information are frequently directed to public health agencies, which must comply with Freedom of Information laws. Under such laws, requested information must be provided unless an exception applies. Public health agencies must review requested information to determine the risk that public disclosure might jeopardize an investigation or response, expose private or sensitive information, or threaten security. If the public health agency has concerns about disclosure, it will need to determine what information that it might withhold under applicable law and clearly articulate the basis for denying the request for information.

Health officials face many questions and challenges when deciding how much information they can or should disclose to inform the public while still protecting individual privacy. Even without personal identifiers, the more information the health agency discloses, the greater the risk to personal privacy. For example, even though an individual's name is withheld, a health official must consider whether information (e.g. county of residence, age, or surrounding circumstances) might allow an individual to be identified. For instance, information disclosed by public health staff might be used by the press as leads or combined with other information to identify an individual.

The health official may be asked questions about a specific individual. Does the health official violate privacy by publicly talking about an individual who has already been publicly identified, for example, by the media, family, or individual? Andrew Speaker's name was published throughout the media as the individual who caused an international scare when he flew with multi-drug resistant tuberculosis from Atlanta, Georgia to Europe for his wedding and honeymoon. Nonetheless, consistent with its policy, the CDC did not identify Mr. Speaker in its communications even after his name had been published.[40] When identifying information is public or a case is likely to generate a lot of media interest, consent from the individual or family to reveal identifying information is the safest course to prevent the appearance or a claim of breach of privacy. If a health official reveals identifying information based on the family's consent, it is important that the public is informed that permission was given to maintain its trust.

To address competing interests, the challenge of informing the public while protecting privacy, and the wide variation in information released by public health agencies, the Association of Health Care Journalists, Association of State and Territorial Health Officials, and National Association of County and City Health Officials have developed guidance for health officials and journalists related to the release of information concerning deaths, epidemics or emerging diseases.[41]

V. Legal Authority for Public Health Protection of Information

All 50 states, the District of Columbia, and some territories have some form of freedom of information (FOI) law that governs documents at the state and local (cities, counties, school districts) level. The federal government also has a FOI law that applies to documents held by the CDC and other federal agencies. These laws may be called "Freedom of Information," "Public Records," "Open Records," or "Sunshine" laws. FOI laws ensure an open government. They are based on the premise that democratic governments must remain accountable to their citizens through the disclosure of information. By requiring governmental agencies to provide access to requested documents, FOI provides a vehicle for citizens and organizations to gain access to government-held documentation. For most states, these laws are statutory. In a few states – including California and North Dakota – the state's constitution also covers the public's right to information. [42]

The provisions of state FOI laws vary significantly with respect to issues such as the time period within which an agency must provide the requested documents, how much an agency is allowed to charge for providing documents, whether the state government provides an ombudsman, whether the document requester must give a reason for wanting the documents, and so on. Generally, the reason for requesting a document is irrelevant and some FOI laws prohibit government from requiring the requester to state the purpose of the request.[43] On the other hand, the purpose of a request may be relevant in some instances where, for example, certain categories of records may be released for limited purposes only, such as administrative, statistical, or qualified research purposes. Additionally, the purpose may be relevant to exemptions that include a balancing test, such as exemptions that require an individual's privacy interest to be balanced against the public's interest in disclosure.[44]

Generally, records obtainable under FOI laws include all "agency records" – such as print documents, photographs, videos, maps, e-mail and electronic records – that are under an agency's possession and control. The person making the request must describe the records with reasonable or sufficient particularity so that the agency can locate the documents being requested. Once the request has been received by the agency, the agency must respond to the request within the period dictated by statute. Under some laws, failure to respond within a mandated time is considered a denial. The agency, upon receipt of request, may either release documents in full, release documents in part, withhold documents in full or not find any responsive documents. Generally, FOI laws are to be construed in favor of disclosure and exemptions are to be narrowly construed. If the requester disagrees with an agency's decision, he or she may appeal as provided by statute.

Applicability of FOI Laws to Public Health Emergency Preparedness and Response

This general policy of public disclosure may prove problematic in the event of a public health emergency, such as an infectious disease outbreak. Disclosing the identity of infected individuals covered by isolation and quarantine orders may subject them to discrimination or retaliatory activities, while disclosing the scope of government containment efforts may intensify public panic. Additionally, some information may need to be withheld to protect national security, such as diagrams of utilities or communications systems and other essential components of a community's infrastructure that may be targets for terrorists. In these situations, the government may seek to maintain the confidentiality of certain public records to protect individuals and the public at large. Even so, the government's ability to restrict access to public records is extremely limited and depends on the applicability of an exemption to disclosure. If an exemption applies, then the agency must identify the exemption in its denial.

Exemptions to the General Rule of Access to Public Records

The exemptions to disclosure vary among the states. Public health agencies should review their FOI law to determine specific exemptions that might apply in their state. Public health agencies must also consider court opinions that interpret the scope and applicability of these exemptions to various factual scenarios. The following are categories of exemptions that might apply to sensitive information held by a public health agency. While these categories are common to most states, all categories may not be covered by all states and the terms of applicability may vary.

Information Not Subject to Disclosure Under Another Law

FOI laws recognize the array of federal and state laws that require agencies to keep certain information confidential. Thus, FOI laws exempt from disclosure "information not subject to disclosure under another law." This means the public is prohibited access to either public records or identifiable information in public records declared confidential by state statute such as communicable disease reports, HIV patient data, patient medical records, immunization data, cancer registries, or vital records. Access is also prohibited when federal privacy laws prohibit disclosure, such as educational records protected by the Family Educational Rights and Privacy Act (FERPA),[45] substance abuse diagnosis and treatment records covered by federal regulations,[46] or identifiable information about veterans or their families covered by the VA Claims Confidentiality Statute.[47]

The federal Privacy Rule,[48] adopted by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA),[49] establishes minimum national standards to protect individually identifiable health information. Generally, however, information covered by the Privacy Rule does not qualify for exemption as "information not subject to disclosure under another law." In other words, when a FOI law requires disclosure, it trumps HIPAA. This is because the Privacy Rule does not supersede state disclosure requirements. HIPAA defers to state law by permitting disclosures that are required by state law if the disclosure meets the requirements of the law.[50] Thus, the Supreme Court of Ohio ordered a city health department to release lead citations and lead-risk-assessment reports to a newspaper under Ohio's FOI law, even though the reports identified addresses of children with blood tests showing elevated lead levels.[51] While the Privacy Rule may not protect individually identifiable health information from disclosure, depending on a state's law, other FOI exemptions that cover personal privacy, health information, or medical records may apply.

At times, federal agencies may provide sensitive information to state or local public health agencies, requesting that the information be kept confidential. Public health agencies should review their laws to ensure that they are able to protect this information from disclosure should it be covered by a FOI request. When state law is uncertain, the public health agency may want to seek the federal agency's advice on federal laws that might apply.

Personal Privacy

In many states, information of a personal nature may be exempted from disclosure. The legal source for this exemption varies among states and may be based on federal[52] or state constitution,[53] FOI or other statutes, or caselaw.[54] Some states have laws that grant rights to individuals regarding information that the government collects and maintains about them. For example, Minnesota's Data Practices Act requires state government to give individuals notice of the legal basis for collecting their information, whether providing

the information is mandatory, and with whom the law requires their information be shared. State government is prohibited from disclosing an individual's private information unless allowed by law.[55]

Many states have statutory exemptions under their FOI law covering "information of a personal nature if public disclosure of the information would constitute a clearly unwarranted invasion of an individual's privacy" (Michigan),[56] "personnel, medical or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy" (California),[57] or "personal documents" relating to an individual, including any information relating to "personal finances, medical or psychological facts." (Vermont).[58] Whether disclosure of information would constitute an unwarranted invasion of an individual's privacy is a factual question that requires weighing the public's interest in disclosure and the individual's interest in personal privacy.[59]

Illinois' FOI law includes exemptions for both "private information" and for "personal information contained within public records, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information." These terms are defined by its FOI law. "Private information" refers to unique identifiers, including a person's social security number, driver's license number, employee identification number, biometric identifiers, personal financial information, passwords or other access codes, medical records, home or personal telephone numbers, personal email addresses, and home addresses if attributable to a person. "Unwarranted invasion of personal privacy" means "the disclosure of information that is highly personal or objectionable to a reasonable person and in which the subject's right to privacy outweighs any legitimate public interest in obtaining the information." However, disclosure of information that bears on the public duties of public employees and officials shall not be considered an invasion of personal privacy.[60]

Generally, a "personal privacy" exemption does not apply to corporations. For example, the U.S. Supreme Court ruled that corporate information does fall within the federal FOIA exemption for personal privacy.[61] The Court established that the term "personal" is often used to only refer to the individual and never used to refer to a corporation and is in fact more often used to refer to strictly non-business information.

Whether the personal privacy exemption applies to deceased individuals varies by state and may depend on judicial interpretation of a personal right to privacy. For example, with regard to an autopsy report, the Michigan Supreme Court ruled that the personal privacy exemption does not apply to individuals who are decreased[62] whereas an Illinois court ruled that autopsy reports are covered by this exemption.[63]

Information that is de-identified does not usually raise privacy concerns. That said, in this era of electronic databases and linkage capabilities, it may be difficult to determine whether information that has been stripped of personal identifiers is "identifiable." In *Southern Illinoisan v Dept of Public Health*,[64] the Illinois Supreme Court ordered the state health department to provide a newspaper with cancer registry data it had requested under Illinois' FOI law, even though the state's expert witness could re-identify individuals from the supposedly de-identified information. The expert, based on her extensive education, knowledge, and experience, could determine identity using her six-step process. Regardless, the Court ruled, this does not necessarily mean, without more, that a threat exists that other individuals will be able to do so as well.

Health information or Medical Records

All or most states protect identifiable health information or medical records. This information may be protected from disclosure by a stand-alone law that covers medical records (Arizona),[65] by a specific exemption to a state's FOI law (Michigan),[66] or by more general exemptions regarding information of a personal nature that relates to a particular individual (Massachusetts).[67] Not all states provide absolute

protection. For example, West Virginia's FOI law protects "[i]formation of a personal nature such as that kept in a personal, medical, or similar file, if the public disclosure thereof would constitute an unreasonable invasion of privacy, unless the public interest in by clear and convincing evidence requires disclosure in the particular instance."[68] 911 logs, recordings or transcripts may be subject to disclosure (Oklahoma),[69] exempt from disclosure (Wyoming),[70] or considered on a case-by-case basis after determining whether the "public interest in disclosure outweighs interest in nondisclosure" (South Dakota).[71] Likewise, protection or disclosure of identifiable information in public ambulance reports or search and rescue operations vary among the states.[72]

Business Information

Documents and information maintained by the private sector are not public records, and thus, not subject to FOI requests. However, when information and documents are submitted by private entities and individuals to government agencies, they are public to the extent they form part of the records of that agency. Businesses may be reluctant to reveal information about their sales, services, distribution routes, inventories, or infrastructure if such information may be disclosed to competitors or the general public. This type of information may be important to surveillance, preparedness planning, and emergency response.

Most states protect business information from disclosure to some extent, but the degree of and criteria for exemption from FOI laws vary. For example, in Idaho, Rhode Island, and South Dakota, FOI laws provide exemptions for most business documents with commercial information, financial data, and trade secrets.[73] In contrast, in Illinois, disclosure must be likely to harm the competitive position of the business that submitted the information.[74] Utah and Wyoming require, in addition, that the government show that the disclosure would hinder its ability to collect such information in the future.[75] Massachusetts and Michigan both protect trade secrets or commercial or financial information, but only if the information is voluntarily provided to an agency for use in developing governmental policy and upon a promise of confidentiality.[76]

Investigatory Records

During the course of an investigation, health agencies might want to withhold information or preliminary findings until an investigation is complete. State laws vary on their protection of investigatory records – some apply only to criminal investigations, while others include civil and administrative investigations. If an investigation is pending, investigatory records may be withheld if disclosure would interfere with the investigation. A balancing test may be required comparing the public's interest in nondisclosure and the public's interest in access. Once an investigation is completed, the public interest in disclosure is likely to prevail. Laws vary on whether autopsy reports are confidential, some states make such reports that result from investigations by medical examiners confidential, while other states require disclosure, and for others disclosure may depend on whether the autopsy is performed as part of a criminal investigation or whether the investigation is complete.[77]

National and/or State Security

States have enacted an array of laws to protect information that might jeopardize public safety or state or national security if publicly disclosed. These laws may protect emergency response plans, evacuation plans, security plans and procedures, vulnerability assessments intended to prevent or mitigate a terrorist attack, emergency health procedures in case of a terrorist attack, and architectural drawings of government buildings and infrastructure such as utility plants, bridges and water supply, sewage disposal, transportation

and communications systems.[78] Some states – such as New Jersey, North Carolina, and Ohio – have defined "public records" subject to the state FOI law to exclude certain security-related information.[79] FOI laws in other states contain exemptions from disclosure, which vary in coverage and criteria for withholding information from the public. Some states require that interests in disclosure and nondisclosure be balanced. In Michigan and Missouri, for example, security information is not exempt from disclosure if "the public interest in disclosure outweighs the public interest in nondisclosure in the particular instance."[80]

When claiming an exemption, public health agencies should be prepared to explain how disclosure of requested information could jeopardize security or public safety. The Connecticut Supreme Court ruled that a town must release electronic maps (Geographic Information System data) to an open records requester despite the town's claim that the information could compromise public safety. The court held "[g]eneralized claims of a possible safety risk" are not enough to satisfy the government's burden of proof on an exemption claim.[81] In Texas, per the Attorney General's Informal Ruling, as with any exception to disclosure, a security-related claim must be accompanied by an adequate explanation of how the responsive records fall within the scope of the claimed exemption.[82]

Some states have enacted special procedures that must be followed if denying a request for government records for security reasons. Indiana law requires that the agency consult with the counterterrorism and security council prior to denying a request. If the request is denied, either the agency or the council must provide a general description of the record being withheld and of how disclosure of the record would have a reasonable likelihood of threatening the public safety.[83] In Georgia, in the event of a court challenge to official nondisclosure of security-related records, the court may review the documents in question in private and condition any disclosure upon such measures as the court finds necessary to protect against the endangerment of life, safety, or public property.[84]

VII. Federal Laws Governing Information Collection, Use, and Protection

For the most part, state law governs state and local public health agencies' collection, use, sharing, and protection of personal and health information to prevent and respond to a public health emergency. Some federal laws that impact state and local public health agencies are discussed below; however, this is not intended to be an exhaustive list of all federal laws that might apply.

Several laws authorize the federal government to establish surveillance systems and collect surveillance data provided by state and local health departments. For example, the Public Health Security and Bioterrorism Preparedness and Response Act of 2002[85] authorized funding to improve public health surveillance and reporting at the state and local level and to integrate federal, state, and local systems.[86]

While the federal government has established systems to collect and integrate information, generally, state and local reporting is voluntary and information is provided consistent with a particular state's law. Of course, the federal government, exercising its spending power, may provide funding to state and local governments to improve public health surveillance or engage in other activities to protect the public, conditioning funding on data sharing. Conversely, the federal government may condition funding on a state's ability to protect information. In this regard, the CDC requires states that receive funding to establish and maintain cancer registries to agree to protect the privacy of the participants and the information collected.[87]

Federal laws may require that federal, state, and local agencies keep information confidential.[88] For example, certain information regarding vaccine tracking and distribution provided by HHS to state and local governments is confidential.[89] The federal government is authorized to allow state and local health officials to access this information to provide for the needs of its populations during an influenza pandemic or time of

vaccine shortage or supply disruption. In turn, state and local governments are to protect the confidentiality of this information. Additionally, information concerning critical infrastructure that is voluntarily provided to the federal government by the private sector is privileged and confidential. [90] The law was passed by Congress to encourage private industries to share infrastructure security information with the government by promising confidentiality of those records. While the federal government may share this information with state and local government and agencies, those agencies must protect its confidentiality.[91]

Federal regulations adopted under HIPAA and the Family Educational Rights Privacy Act (FERPA) also impact public health agencies' collection, use, sharing, and protection of personal and health information.

HIPAA Privacy Rule

Healthcare providers – including physicians, hospitals, laboratories, and health plans – are major data sources for disease prevention and control. Most of these providers are covered entities that are subject to privacy standards established by the federal Privacy Rule[92] adopted by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA).[93] The Privacy Rule established national minimum standards to protect the privacy of individually identifiable health information (referred to as "protected health information" or "PHI") and gives patients an array of rights with respect to that information. A covered entity is prohibited from using or disclosing PHI without the written authorization of the patient unless required or permitted by the Privacy Rule. A covered entity that violates the Privacy Rule is subject to civil or criminal penalties.

The Privacy Rule need not impede the collection, use, and disclosure of PHI by public health agencies to prevent or protect the public from disease or other threats. The Privacy Rule does not apply to "de-identified information," e.g. aggregate statistical data or data stripped of individual identifiers. Information may be de-identified by removing 18 identifiers specified in the Rule, provided that the covered entity does not have actual knowledge that the remaining information can be used alone or in combination with other reasonably available information to identify a subject (safe harbor de-identification).[94] These identifiers include personal identifiers (such as name, address, telephone number, birth date, social security number) and non-personal identifiers (such as geographic information smaller than a state and dates directly associated with an individual). Alternatively, a covered entity may rely on a determination by a properly qualified statistician using accepted analytic techniques who concludes the risk of re-identification is substantially limited (statistical de-identification). Since an expert must determine that information is statistically de-identified, most covered entities opt for the safe harbor by removing the specified identifiers.

The Privacy Rule also allows covered entities to disclose a "limited data set" for public health purposes pursuant to a limited use agreement.[95] A limited data set is more useful for public health purposes because it includes dates (such as admission, discharge, service, date of birth or death), geography (city, county, five digit zip code); and ages (in years, months or days). Disclosure of limited data sets to public health agencies may be sufficient for some public health purposes, such as syndromic surveillance.

More importantly, the Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information to carry out their public health activities.[96] The Privacy Rule was not intended to interfere with the implementation of state law such as mandatory reporting of diseases, immunizations, or information for vital records. A covered entity is allowed to disclose PHI as required by such laws.[97]

Moreover, the Privacy Rule was not intended to interfere with public health's mission. In order to balance personal privacy with public health, the Privacy Rule permits covered entities to disclose PHI without authorization to public health authorities and their authorized agents for public health purposes, including

but not limited to public health surveillance, investigations, and interventions.[98] Accordingly, physicians, laboratories, and other healthcare providers may provide fully identified health information to public health agencies without violating HIPAA. This exception requires that a legal basis exists for the activity and includes both actions that are permitted and actions that are required by law. This means that state or local laws need not specify each and every case in which use of PHI may be necessary to protect the public. To the extent that a public health agency is a covered entity, it may use, as well as disclose, PHI for public health purposes.[99]

Disclosures of PHI to public health agencies may be supported by several additional exceptions to HIPAA's authorization requirement. These exceptions may also allow covered entities to provide necessary information to organizations and individuals that are neither public health agencies nor their agents without the patient's authorization. These include: (1) for treatment of the individual or payment for care,[100] (2) to family and friends involved in a patient's care if the patient is unable to indicate his or her oral consent,[101] (3) to avert a serious threat to health or safety of a person or the public,[102] (4) to protect national security,[103] (5) to law enforcement under certain conditions,[104] and (6) for administrative or judicial proceedings.[105] Of course, the HIPAA Privacy Rule does not apply to disclosures made by entities that are not covered by HIPAA. This means that the HIPAA Privacy Rule should not restrict communications by organizations providing shelter, food, or other assistance that is not healthcare.

For a more detailed discussion of HIPAA's provisions as applied to use and disclosure of identifiable health information for public health purposes, see materials contained in the *Public Health and Schools Toolkit*.

Although the Privacy Rule need not interfere with public health surveillance and investigation, some healthcare providers might hesitate or refuse to provide needed information based on their misunderstanding of the Privacy Rule or fear of violating its standards. Public Health agencies can alleviate some qualms by giving the healthcare provider a written statement explaining the legal basis under which the information is requested. In this regard, the Privacy Rule states that a covered entity may rely, if such reliance is reasonable under the circumstances, on such a written statement, or, if a written statement would be impracticable, an oral statement of such legal authority.[106]

Family Educational Rights and Privacy Act

State laws may require that schools report communicable disease cases, immunizations, or other matters of public health importance. However, schools that receive funds for a program administered by the U.S. Department of Education may be limited by the Family Educational Rights and Privacy Act (FERPA) [107] and federal regulations adopted thereunder.[108] FERPA is a federal law that protects the privacy of student education records while allowing students and parents greater access to these records. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. Any state law that conflicts with FERPA and its regulations is pre-empted by the federal law, and the federal requirements take precedence over the state requirements.

Schools may disclose students' records, without consent, if allowed by exceptions set out in FERPA or its regulations. These exceptions include directory information (such as name and contact information), information necessary to protect the health or safety of the student or other individuals, information necessary to comply with a judicial order or lawfully issued subpoena, and disclosures to organizations conducting certain studies for or on behalf of the school.[109]

For a more detailed discussion of FERPA's provisions as applied to disclosure of student records for public health purposes, see materials contained in the *Public Health and Schools Toolkit*.

VIII. Data Protection and Data Security Laws

This Issue Brief has focused on "data privacy" including appropriate collection, use and disclosure of personal or sensitive information. "Data security" is equally important and essential to ensure privacy. Such security includes practices to ensure that stored data is safe from unauthorized access and is transferred in a secure manner. Although beyond the scope of this Issue Brief, public health agencies must identify and ensure compliance with federal and state laws that apply to the security of data they maintain. These include laws that cover electronic health information, such as the HIPAA security rule,[110] and databases that contain sensitive personal information such as state identity theft protection laws. In addition to setting security standards, these laws may require notification of individuals whose information is compromised and establish sanctions for security breaches.

Conclusion

State law mostly governs collection, use, and sharing of information by public health agencies to prevent disease and injury and protect the public against health threats. These laws vary state-by-state. Public health agencies need to understand their legal authority to collect and use identifiable information. They also need to understand their responsibilities, including their responsibility and legal authority to protect sensitive or private information from public disclosure.

Sources:

[1] *Jacobson v. Com. of Massachusetts*, 197 U.S. 11 (1905). Available at http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=197&invol=11. Accessed Nov. 15, 2012.
[2] Stoto M. "Public Health Surveillance in the Twenty-First Century: Achieving Population Health Goals While Protecting Individuals' Privacy and Confidentiality." *The Georgetown Law Journal.* 96:703-719. Available at http://georgetown.lawreviewnetwork.com/files/pdf/96-2/Stoto.PDF. Accessed Nov. 15, 2012. *See also O'Connor*, J. "Informational Privacy Protections: Do State Laws Offer Public Health Leaders the Flexibility They Need?" 2009. Available at http://www.sph.unc.edu/images/stories/academic_programs/hpaa/documents/oconnor.pdf. Accessed Nov. 15, 2012. *See also* American Health Information Management Association (AHIMA). "Homeland Security Act, Patriot Act, Freedom of Information Act, and HIM (Updated)." November 2010. Available at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048641.hcsp?dDocName=bok1_048641. Accessed Nov. 15, 2012.
[3] Mariner W. "Mission Creep: Public Health Surveillance and Medical Privacy." *Boston University Law Review.* 87:347-395. Available at http://www.bu.edu/law/central/jd/organizations/journals/bulr/volume87n2/documents/MARINERv.2.pdf. Accessed Nov. 15, 2012.
[4] Stoto M. "Public Health Surveillance in the Twenty-First Century: Achieving Population Health Goals While Protecting Individuals' Privacy and Confidentiality." *The Georgetown Law Journal.* 96:703-719. Available at http://georgetown.lawreviewnetwork.com/files/pdf/96-2/Stoto.PDF. Accessed Nov. 15, 2012.
[5] Md. Regs. Code title 10 § 06.01.03 (2002).
[6] N.J. Admin. Code title 8, § 57-1.3 (2002).
[7] 28 Pa. Code § 27.3 (2002).
[8] S.C. Code Ann. § 44-29-10 (2002).
[9] Mariner W. "Mission Creep: Public Health Surveillance and Medical Privacy." *Boston University Law Review.* 87:347-395. Available at http://www.bu.edu/law/central/jd/organizations/journals/bulr/volume87n2/documents/MARINERv.2.pdf. Accessed Nov. 15, 2012.

[10] Association of State and Territorial Health Officers (ASTHO). "Information Management for State Health Officials The Impact of the HIPAA Privacy Rule on Syndromic Surveillance." 2004. Available at http://astho.org/Programs/e-Health/Privacy/Materials/The-Impact-of-the-HIPAA-Privacy-Rule-on-Syndromic-Surveillance-(2004). Accessed Dec. 31, 2012.
[11] CDC. "What is Syndromic surveillance?" *MMWR.* 2004. 53:5-11. Available at http://www.cdc.gov/mmwr/preview/mmwrhtml/su5301a3.htm. Accessed Nov. 15, 2012.
[12] *Ibid.*
[13] 173 Neb. Admin. Code Ch.1 § 003(2002).

[14] N.C. Admin. Code title 15A, r. 19A.0102 (2002) and N.C. Admin. Code title 15A, r. 19A.0103 (2002).
[15] Mariner W. "Mission Creep: Public Health Surveillance and Medical Privacy." *Boston University Law Review.* 87:347-395. Available at http://www.bu.edu/law/central/jd/organizations/journals/bulr/volume87n2/documents/MARINERv.2.pdf. Accessed Nov. 15, 2012.

[16] Health Information Technology for Economic and Clinical Health Act, also known as the HITECH Act, Pub. L. 111-5, 42 U.S.C. 300jj et seq.; 17901 et seq.
[17] American Recovery and Reinvestment Tax Act of 2009, Pub. L. 111-5, 123 Stat. 306.
[18]CDC. "Meaningful Use." Available at http://www.cdc.gov/ehrmeaningfuluse/. Accessed Nov. 15, 2012.*See also* The Office of National Coordinator for Health Information Technology. "Meaningful Use." Available at http://www.healthit.gov/policy-researchers-implementers/meaningful-use. Accessed Dec. 31, 2012.
[19]*Whalen v. Roe*, 429 U.S. 589 (1977). *See also* Gorkin R. "The Constitutional Right to Information Privacy: NASA v. Nelson." 2012. Available at http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1063&context=djclpp_sidebar. Accessed Nov. 15, 2012.
[20] *Planned Parenthood of Missouri v. Danforth,* 428 U.S. 52 (1976). Available at http://www.law.cornell.edu/supct/html/historics/USSC_CR_0428_0052_ZS.html. Accessed Nov. 15, 2012.
[21] *Ibid*.
[22] *Whalen v. Roe,* 429 U.S. 589 (1977). Available at http://www.law.cornell.edu/supct/html/historics/USSC_CR_0429_0589_ZO.html. Accessed Nov. 15, 2012.
[23] *Ibid*.
[24] *Ibid*.
[25] O'Connor J. "Informational Privacy Protections: Do State Laws Offer Public Health Leaders the Flexibility They Need?" 2009. Available at http://www.sph.unc.edu/images/stories/academic_programs/hpaa/documents/oconnor.pdf. Accessed Nov. 15, 2012.
[26] The Food Safety Research Consortium. "The Essential Role of State and Local Agencies in Food Safety and Food Safety Reform." Available at http://www.thefsrc.org/State_Local/StateLocal_June17_background.pdf. Accessed Nov. 15, 2012.
[27] M.C.L. § 333.2241; M.C.L. § 333.2446.
[28] *Florida v. Jimeno*, 500 U.S. 248 (1991). Available at http://www.law.cornell.edu/supct/html/90-622.ZS.html. Accessed Nov. 15, 2012.
[29] Michigan Department of Attorney General and Michigan Department of Community Health. "Public Health Law Bench Book for Michigan Courts." October 2007, p 18. Available at http://www.michigan.gov/documents/ag/Michigan_Public_Health_Bench_Book_221936_7.pdf. Accessed Nov. 15, 2012.
[30] *Ibid.* p 19.
[31] G Goodman R, Hoffman R, Lopez W, et al (eds). *Law in Public Health Practice*, 2d Ed. New York: Oxford University Press, 2006, p 154. *See also* chapter endnote 54; *Camara v. Municipal Court*, 387 U.S. 523 (1967). Available at http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=387&invol=523. *See also See v. City of Seattle*, 387 U.S. 541 (1967). Available at http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=387&invol=541. Accessed Nov. 15, 2012.
[32] *Ferguson v. City of Charleston,* 532 U.S. 67, 121 S. Ct. 1281, 149 L. Ed. 2d.205 (2001). Available at http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=000&invol=99-936. Accessed Nov. 15, 2012.
[33] *Ibid*.
[34] Interview of Denise Chrysler, J.D., who served as director of the Michigan Department of Community Health Office of Legal Affairs during this measles incident.
[35] O'Connor J. "Informational Privacy Protections: Do State Laws Offer Public Health Leaders the Flexibility They Need?" 2009. Available at http://www.sph.unc.edu/images/stories/academic_programs/hpaa/documents/oconnor.pdf. Accessed Nov. 15, 2012.
[36] *Ibid*.
[37] Oregon Statutes, ORS § 433.008. Available at http://www.oregonlaws.org/ors/433.008. Accessed Nov. 15, 2012.
[38] *Tarasoff v. Regents of University of California*, 17 Cal 3d 425, 131 Cal. Rptr. 14, 551 P.2d 334 (1976). Available at http://www.stanford.edu/group/psylawseminar/Tarsoff%20I.htm. Accessed Nov. 15, 2012. For discussion of data disclosure and ethics, see Fairchild A, et al.. "Public Goods, Private Data: HIV and the History, Ethics, and Uses of Identifiable Public Health Information." Available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1804110. Accessed Dec. 31, 2012.
[39]CDC. "National Notifiable Diseases Surveillance System (NNDSS)." Available at http://wwwn.cdc.gov/nndss/. Accessed Nov. 15, 2012.
[40] *Speaker v. Centers for Disease Control and Prevention,* 623 F.3d 1371, 1386 (11th Cir. 2010), Ct Apls No 12-11967 09-14-2012. Available at http://law.justia.com/cases/federal/appellate-courts/ca11/12-11967/12-11967-2012-09-14.html and http://www.networkforphl.org/_asset/xdm731/TB-Control---Speaker-District-Ct--Decision.pdf. Accessed Nov. 15, 2012.
[41] Guidance on the release of information concerning deaths, epidemics or emerging diseases. Available at http://healthjournalism.org/secondarypage-details.php?id=965. Accessed Nov. 30, 2012.
[42] California Constitution, Article 1, §3(b): North Dakota Constitution, Article XI, Section 6.
[43] 5 I.L.C.S. § 140.3(c); (Illinois - a public body may not require the requester to specify the purpose for a request, except to determine whether the records are requested for a commercial purpose or whether to grant a request for a fee waiver). Idaho Code § 9-338(4); (the statute prohibits public agencies from inquiring as to why a person wants a public record). G.S. § 132-6(b); (North Carolina - the requester's purpose is irrelevant, and public officials are prohibited from inquiring about it).
[44] *Hempel v. City of Baraboo*, 284 Wis. 2d 162, 599 N.W.2d 551, 568 (2005); *Gray v. Salem-Keizer School District*, 139 Or. App. 556, 912 P.2d 938 (1996).
[45] Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g.

[46] 42 C.F.R. Part 2.
[47] 38 U.S.C. § 5701, implemented by 38 C.F.R. §§ 1.500-1.527.
[48] 45 C.F.R. Parts 160 and 164.
[49] Pub. L. 104-191, 42 U.S.C. § 300gg *et seq*.
[50] 45 CFR 164.512(a)
[51] *Cincinnati Enquirer v. Daniels*, 108 Ohio St.3d 518; 844 N.E.2d 1181 (Ohio 2006). Available at http://www.sconet.state.oh.us/rod/docs/pdf/0/2006/2006-ohio-1215.pdf. Accessed Nov. 30, 2012.
[52] *Fadio v. Coon,* 633 F.2d 1172, 1175 n.3 (5th Cir. 1981). (Legislature cannot authorize by state an unconstitutional invasion of privacy). *See also* Reporters Committee for Freedom of the Press. Available at http://www.rcfp.org/open-government-guide. Accessed Nov. 15, 2012.
[53] Cal. Const. Art 1, § 3(b)(3).
[54] *Lamy v. N.H. Public Utilities Commission*, 152 N.H. 106 (2005) (court uses a three-step analysis to determine whether disclosure of public record constitutes an invasion of privacy). Available at http://caselaw.findlaw.com/nh-supreme-court/1073489.html. Accessed Nov. 15, 2012.
[55] Minnesota Statutes § 13.05 (2012). Available at https://www.revisor.mn.gov/statutes/?id=13.05. Accessed Nov. 15, 2012.
[56] M.C.L. § 15.243(1)(a). Available at http://www.legislature.mi.gov/(S(k54g34i2kgkkyxr1ia5vreet))/mileg.aspx?page=getObject&objectname=mcl-15-243. Accessed Nov. 15, 2012.
[57] Cal. Gov't. Code § 6254(c).
[58] 1 V.S.A. § 317(b).
[59] Hempel v. City of Baraboo, 284 Wis. 2d 162, 599 N.W.2d 551, 568 (2005); Gray v. Salem-Keizer School District, 139 Or. App. 556, 912 P.2d 938 (1996); Baker, P.C. v. City of Westland, 245 Mich. App. 90 (2001).
[60] 5 I.L.C.S. § 140/7, 5 I.L.C.S. § 140/2.
[61] *FCC v. AT&T*, 562 U.S. ___ (2011), Mar1, 2011. Available at http://www.supremecourt.gov/opinions/10pdf/09-1279.pdf. Accessed Nov. 15, 2012.
[62] *Swickard v. Wayne Medical Examiner*, 438 Mich. 536; 475 N.W.2d 304 (1991). But see, *Baker, P.C. v. City of Westland*, 245 Mich. App. 90 (2001), wherein the court held that the FOIA's privacy exemption may be applied to deceased private citizens and their families where there is no public interest in disclosure.
[63] *Trent v. Coroner of Peoria County*, 349 Ill App 3d 276, 812 NE2d 21 (2004).
[64] *Southern Illinoisan v. Dept. Pub. Health*, 319 Ill. App.3d 979 (2001). Available at http://www.state.il.us/court/Opinions/AppellateCourt/2004/5thDistrict/June/Html/5020836.htm. Accessed Nov. 15, 2012.
[65] Ariz. Rev. Stat. § 12-2294 (Medical Records).
[66] M.C.L. § 15.243(1)(l).
[67] M.G.L. § c.4 s. 7 cl. 26.
[68] W. Va. Code § 29B-1-4(2). *Hechler v. Casey*, 175 W. Va. 434, 333 S.E.2d 799 (1985). See also *Robinson v. Merritt*, 180 W. Va. 26, 375 S.E.2d 204 (1988).
[69] 51 O.S. §§ 24A.8.A.4.
[70] Wyo. Stat. § 16-4-203(d)(x).
[71] S.D.C.L. § 1-27-1.5(5).
[72] A.R.S. § 36-2220(A); (With some exceptions, information, records, and data related to the administration or evaluation of the Arizona emergency medical services system or trauma system are open to the public). OIP Op. Ltr. N. 9-33 (Dec. 31, 1991); (Hawaii - An ambulance report about a deceased individual must be made available for public inspection). 1 M.R.S.A. § 402(3)(H); (Maine - Medical records and reports of municipal ambulance, rescue, and other emergency units are not available). Wis. Stat. § 256.15(12)(b); (Public ambulance transport records are public, including the name of the person transported, date of call, dispatch times and destination, but no information disclosed "may contain details of the medical history, condition or emergency treatment of any patient").
[73] Idaho Code §§ 9-340D(1)-(3), (5), (6), (8): R.I. Gen. Laws § 38-2-2(4)(i)(B): S.D.C.L. §§ 1-27-1.5(3): and 1-27-1.6.
[74] 5 I.L.C.S. 140/7(1)(g).
[75] Utah Code Ann. § 63G-2-305(2). Wyo. Stat § 16-4-203(d)(v) *and see Sublette County Rural Health Care District v. Miley*, 942 P.2d 1101 (Wyo. 1997).
[76] M.G.L. c. 4, § 7,cl. 26(g). M.C.L.A. § 15.243(1)(f).
[77] Op. Att'y. Gen. Ala. No. 2007-015, 2006 Ala. AG (Dec. 4, 2006); (Alabama - records of the county coroner's autopsies are public records subject to disclosure under the Public Records Law, unless there is a pending criminal investigation). AS 40.25; (Alaska - the medical examiner's investigative report is privileged and confidential, and not subject to disclosure). C.R.S. 24-72-204(3)(a)(I); (Colorado - Coroners' autopsy reports are specifically excluded from the general medical records exemption). Conn. Gen. Stat. §19a-411; (Supreme Court held that autopsy reports are exempt from disclosure).
[78] Ala. Code § 36-12-40 (Supp. 2005). S.G. § 10-618(j)(2), (Maryland). For additional examples, see Reporters Committee for Freedom of the Press. "Guide Compare Tool; Comparing: E. Homeland Security Measures,". Available at http://www.rcfp.org/open-government-guide (Select all states and topic "Homeland Security"). Accessed November 15, 2012. See also, Homefront Confidential. "Prepared by How the War on Terrorism Affects Access to Information and the Public's Right to Know." September 2005. p 73. Available at http://www.rcfp.org/sites/default/files/homefront-confidential.pdf. Accessed Nov. 15, 2012.

RCW 42.56.420(1) (Washington). *See also Northwest Gas Ass'n v. Washington Utilities and Transp. Comm.*, 141 Wn. App. 98, 168 P.3d 443 (2007). RCW 42.56.420(2)-(5).
[79] N.J.S.A.§ 47:1A (New Jersey). G.S. 132-1 (North Carolina). Ohio Rev. Code § 149.433(B).
[80] M.C.L. § 15.243(1)(y). Mo.Rev.Stat. § 610.021(18) (Provision to sunset 12/31/12).
[81] Reporters Committee for Freedom of the Press. "Guide Compare Tool; Comparing: E. Homeland Security Measures." Available at http://www.rcfp.org/open-government-guide (Select all states and topic "Homeland Security"). Accessed Nov. 15, 2012.
[82] *Ibid*.
[83] *Ibid*.
[84] *Ibid*.
[85] Pub. L. 107-188, 42 U.S.C. 300hh *et seq*.
[86] Mariner W. "Mission Creep: Public Health Surveillance and Medical Privacy." *Boston University Law Review.* 87:347-395. Available at http://www.bu.edu/law/central/jd/organizations/journals/bulr/volume87n2/documents/MARINERv.2.pdf. Accessed Nov. 15, 2012.
[87] CDC. "National Program of Cancer Registries Cancer Surveillance System Rationale and Approach." P 13. Available at http://www.cdc.gov/cancer/npcr/pdf/npcr_css.pdf. Accessed Nov. 15, 2012.
[88] Homefront Confidential. "Prepared by How the War on Terrorism Affects Access to Information and the Public's Right to Know." September 2005. p 73. Available at http://www.rcfp.org/sites/default/files/homefront-confidential.pdf. Accessed Nov. 15, 2012.
[89] Public Health Service Act, 42 U.S.C. § 247d-1.
[90] Critical Infrastructure Information Act of 2002, Pub. L. 107-296, 6 U.S.C. 131 *et seq*., which is part of the Homeland Security Act of 2002.
[91] *Ibid*.
[92] 45 C.F.R. Parts 160 and 164.
[93] Pub. L. 104-191, 42 U.S.C. § 300gg et seq.
[94] 45 C.F.R. § 164.514(b).
[95] 45 C.F.R. § 164.514(e)(1).
[96] CDC and HHS have provided significant guidance on the impact of the HIPAA Privacy Rule on public health practice. See "HIPAA Privacy Rules and Public Health: Guidance from CDC and the U.S. Department of Health and Human Services." *MMWR*. 2003. 52:1-12. Available at http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm. Accessed Nov. 30, 2012.
[97] 45 C.F.R. § 164.512(a).
[98] 45 C.F.R. § 164.512(b)(1)(i).
[99] 45 C.F.R. § 164.512(2)(b).
[100] 45 C.F.R. § 164.501, 45 C.F.R. § 164.502, 45 C.F.R. § 164.506.
[101] 45 C.F.R. § 164.510(a)(3).
[102] 45 C.F.R. § 164.512(j).
[103] 45 C.F.R. § 164.512(k)(2).
[104] 45 C.F.R. § 164.521(f); 45 C.F.R. § 164.512(k)(5).
[105] 45 C.F.R. § 164.512(e).
[106] 45 CFR 164.514(h)(2)(iii). An example of such a memo, issued by the Michigan Department of Community Health, is posted on CDC's website at http://www.cdc.gov/phlp/docs/Dir_Memo_HIPAA&communicabledis_072004_1.pdf. Accessed Nov. 30, 2012.
[107] Family Educational Rights and Privacy Act (FERPA), Pub. L. 93-380, 20 U.S.C. § 1232g.
[108] 34 C.F.R. Part 99.
[109] 34 C.F.R. § 99.31.
[110] 45 CFR Part 160 and Subparts A and C of Part 164.

This document was compiled from April–November 2012 and reflects the laws and programs current then. It reflects only portions of the laws relevant to public health emergencies and is not intended to be exhaustive of all relevant legal authority. This resource is for informational purposes only and is not intended as a substitute for professional legal or other advice. The document was funded by CDC Award No. 1U38HM000454 to the Association of State and Territorial Health Officials; Subcontractor Subcontractor University of Michigan School of Public Health, Network for Public Health Law – Mid-States Region.