PARTNERSHIP *for*
PUBLIC HEALTH LAW
Advancing Public Health Through Law
A Collaboration of APHA, ASTHO, NACCHO, and NALBOH

Legal Issues Related to Sharing of Clinical Health Data with Public Health Agencies

April 2016

I. Introduction

This[1] memorandum discusses legal issues related to the sharing of clinical health data by primary care providers (PCPs) with public health agencies for public health purposes.[1] To allow for the efficient and useful transfer of clinical health data, public health agencies need to have the legal authority to collect and use the data, the capacity to identify and comply with any data collection or use restrictions, and the ability to maintain community trust by complying with federal and state data privacy and security laws. Both federal and state laws apply to the sharing of clinical health data with public health agencies and state laws vary greatly.

This memorandum discusses the importance and benefits of sharing clinical data with public health agencies, enabling public health agencies to provide essential services that promote and protect the public's health. It describes the major types of clinical health data that PCPs might provide to public health agencies and the information systems that transfer and manage this data. This memorandum covers laws that govern PCPs in providing data to public health agencies and provides assistance for identifying and analyzing relevant laws in a particular state. These include laws that facilitate and laws that might be a barrier to the flow of data from PCPs to public health agencies. Finally, after considering the legal landscape, this memorandum provides recommendations to encourage PCPs in providing data to public health agencies.

This memorandum focuses on data provided by PCPs to state and local health departments. PCPs might also provide data to federal agencies that protect and promote the public's health, which implicate additional data laws that apply to federal agencies such as the

[1] This memorandum was prepared by the Network for Public Health Law for the Partnership for Public Health Law, a collaboration of the American Public Health Association, the Association of State and Territorial Health Officials, the National Association of County and City Health Officials, and the National Association of Local Boards of Health.

federal Privacy Act. Discussion of laws that apply to federal agencies, though important, is beyond the scope of this memorandum.

II. Definition of clinical data

Primary care includes health promotion, disease prevention, health maintenance, counseling, patient education, diagnosis and treatment of acute and chronic illnesses in a variety of health care settings. The clinical data collected during patient encounters with PCPs are an important source of information for improving population health. These data can provide insight on a variety of metrics such as pandemic disease, chronic disease management, injuries and patient utilization patterns. They can be especially useful for public health agencies. For example, access to health status data may allow for better case management for clients and access to demographic and socioeconomic data may allow public health agencies to better combat health disparities.[2]

Recognizing the importance of improved data collection, the Affordable Care Act (ACA) has data collection standards for race, ethnicity, sex, primary language and disability status. The Department of Health and Human Services' (HHS) regulations promulgate a set of minimum uniform data collection standards for inclusion in population health surveys aimed at identifying racial and ethnic health disparities.[3] Some HHS surveys directly target patients or PCPs, such as the Medical Expenditure Panel Survey and the National Immunization Survey.[4] The major types of clinical health data are highlighted below in Table 1.[5]

Table 1. Major types of clinical health data[6]

Type of Data	Description of Data
Demographic and Socioeconomic	Personally identifiable information such as age, sex, race, ethnicity, education and related demographic and socioeconomic variables.
Health Status	An individual's health status, including morbidity, disability, diagnoses, problems, complaints, and signs and symptoms as well as behavioral and health risk factor data.
Health Resources	The capacity and characteristics of the provider, plan or health system.
Healthcare Utilization	The nature and characteristics of an individual's medical care visits, encounter, discharge, stay or other use of healthcare services. It also includes information on time, date, duration, tests, procedures, treatment, prescriptions and other elements of the health care encounter.

Healthcare Financing and Expenditure	An individual's healthcare costs, prices, charges, payments, insurance status and sources of payment.
Healthcare Outcomes	The outcomes of an individual's prior or current prevention, treatment, counseling or other interventions on future health status over time in a cyclical, longitudinal process.
Clinical Trial	Data collected during a prospective, biomedical or behavioral research study of human subjects that is designed to answer specific questions about biomedical or behavioral interventions.

Clinical data come in a variety of formats such as raw data collected in report forms during trials, coded data stored in computerized databases and summary data made available through journals and registries. As discussed in Section V, laws may treat subsets of clinical data differently, depending on the data provider or the type of data.

Clinical data may be stored in either paper records or electronic health records (EHRs). EHRs are real-time records that contain information about a patient's medical history, diagnoses, medications, immunizations, radiological images, laboratory reports and other test results.[7] The Meaningful Use program sets specific objectives that eligible health care providers must achieve to qualify for Centers for Medicare & Medicaid Services monetary incentives.[8] Some of these objectives relate specifically to data sharing with public health agencies, including cancer registries, syndromic surveillance and other specialized registries. This program has accelerated the adoption of EHRs. Potential benefits to utilizing an EHR system as a tool for sharing clinical data with public health agencies include:

- Automatic functions through EHRs can increase reporting and data sharing with public health agencies, as well as save money
- EHRs can be created, managed and consulted by several organizations, including public health agencies
- EHRs can provide retrospective information about an individual across time, care providers and geographic jurisdictions[9]
- Improved data quality and efficiency in disease reporting

III. Importance and benefits of sharing clinical data with public health agencies

Clinical data and information are necessary for the operation of public health agencies and the protection and improvement of population health. Though PCPs and public health

agencies have complementary functions and a common goal of ensuring a healthy population, they operate largely independently and most functions, like data sharing, are not well integrated.[10] Clinical data enable public health agencies to perform essential services to accomplish their three core functions:

1. Assessment – Collecting, investigating and analyzing information about health problems;
2. Policy development - Weighing available information, deciding which interventions are most appropriate, and ensuring that the public interest is served by measures that are adopted; and
3. Assurance - Promoting and protecting public interests through programs, events, campaigns, regulations and other strategies, and making sure that necessary services are provided to reach agreed upon goals.

Improved technological capabilities and an increased ease of routine data analysis have increased public health interest in the use of clinical health data for public health purposes. Greater access to clinical data will allow for timely, relevant, and high-quality decision making by public health agencies that lead to better population health outcomes. Below are some potential benefits to increased clinical data sharing with public health agencies.

a. Improved Public and Population Health Outcomes

By efficiently leveraging clinical data for quality improvement and prevention activities, sharing clinical data can improve public and population health outcomes. For example, collecting standardized, systematic data in electronic health records could improve public health reporting and surveillance. Through syndromic surveillance data submission, immunization information systems (registries), and electronic laboratory reporting, providers can transmit population health data to public health agencies. Also, with a greater quantity and quality of data available, public health organizations can better monitor, prevent, and manage disease. Studies have demonstrated that data transmission from physician-owned practices in primary care settings can be used by public health agencies on a large scale to track the delivery of recommended preventive and health-promoting services and improve health outcomes for patients.[11]

b. Expanded communication between PCPs and public health agencies

More pathways for sharing clinical care data with public health agencies will allow for improved communication and greater collaboration that could lead to better integration

between the two health sectors. For example, immunization reporting systems, as well as Michigan's reporting of height and weight, provide benefits beyond surveillance. They return valuable clinical decision support to practitioners. Immunization registries can provide consolidated immunization histories at the point of care for use by a vaccination provider in determining appropriate patient vaccinations. Michigan's BMI reporting system generates clinical support tools to guide the clinician through appropriate assessment and counseling for children identified as overweight or obese.[12] Public health agencies can utilize clinical information to remind providers when individual patients need immunizations, to track vaccine uptake, or to give providers access to clinical protocols as well as assess which practices provide the best evidence for health intervention strategies.

c. Greater Resources for fulfilling public health services

The core mission of public health is defined by the Essential Public Health Services, detailed in Appendix A. Carrying out these functions require a large amount of information regarding the community and the health of populations. Greater access to clinical health data can augment existing public health data to provide superior resources for program development, implementation and evaluation. Evidence of the response to H1N1 and Ebola illustrate how access to this type of data is important for public health agencies playing a critical role in achieving both national and global health security to the emerging threats caused by the globalization of diseases, travel, food and medicines.

IV. Laws that govern PCPs sharing clinical data with public health agencies

Law both facilitates and impedes public health's collection, use, disclosure, and protection of electronic health data. Law facilitates the flow of data from PCPs by mandating or authorizing their disclosure to public health agencies and protecting PCPs from liability for data disclosure. Law might be a barrier to the flow of data from PCPs to public health agencies, for example, by prohibiting data sharing outright, requiring specific authority to collect data, limiting sharing of certain data elements, or establishing onerous conditions for data sharing. At the same time, safeguards to protect privacy and security might encourage data sharing by PCPs and promote the public's trust.

Since state law defines public health authority to obtain clinical data, conditions vary state to state. The resulting patchwork of laws can create challenges for data sharing across jurisdictional borders. Additionally, within a state, law might establish varying standards

depending on the type, source, or intended use of data. Multiple standards can impede data sharing for public health purposes. To ensure full legal compliance, applicable laws must be identified. The following describes common types of laws that might apply. This list is not exhaustive for all states and any court or attorney general opinions interpreting law must also be considered.

A. Legal authority enabling PCPs to share clinical data with public health agencies

Patient privacy and confidentiality are a bedrock of health care. To ensure quality diagnosis and treatment, patients must trust that their communications with their health care providers will be kept private. Law and professional ethics prohibit disclosure of health information without a patient's consent. Generally, licensing laws require health care professionals and health care facilities to maintain patient confidences. However, law also establishes exceptions when the privacy interests of individuals must give way to larger societal concerns. Public health agencies are often exempted from patient consent and authorization requirements for data used in the course of fulfilling public health functions. These laws may also provide specific protection from liability by granting health care providers immunity for disclosures made to public health agencies.

Under the U.S. Constitution, states may exercise police powers to protect the public's health, safety, and welfare. 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.[13]

States have enacted statutes and adopted regulations mandating PCPs to provide clinical data for a wide range of public health activities. During an emergency, governors or health officials might issue declarations or orders that mandate reporting of health information needed to respond to a public health threat. Much of this data is personal in character and potentially embarrassing or harmful if disclosed. The move from paper to electronic reporting has benefitted public health tremendously. At the same time, accumulation of electronic information adds security risks. Thus, the right to collect and use such data is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.[14]

In addition to mandatory reporting, laws may specifically authorize, but not require, health care providers to submit information regarding their patients. For example, while 49 states operate immunization information systems, few states mandate that all health care providers report immunizations administered.[15] Instead, most states promote and support voluntary reporting by a variety of providers. Michigan administrative rules provide another

example, by allowing – but not requiring – physicians to report children's height and weight to the Michigan Care Improvement Registry, absent objection of the parent. [16] The registry calculates BMI real-time on screen to assist providers in assessing and treating their patients.

Health care providers may submit clinical information to public health agencies that collect data for public health activities under their general powers. Immunization Information Systems (IIS) and syndromic surveillance are two common examples.

Over the last decade, laws that specifically authorize immunization information systems have increased substantially. That said, nine states continue to operate their IIS based upon general public health authority.[17] Of these, providers in Georgia, Pennsylvania, and Wisconsin may voluntarily submit immunization information for children and adults unless the parent or individual has opted out of reporting.[18]

Emergency departments in many states provide health data in real time to public health syndromic surveillance systems. These systems gather information – such as fever, rash, gastrointestinal illness, and respiratory conditions – that can indicate an emerging disease or other public health threat, before a confirmed diagnosis is made. Health agency staff, assisted by automated data acquisition and generation of statistical alerts, are able to then make inquiries or investigate the public health significance of any anomalies. For example, when emergency department data triggered a statistical alert, the Texas Department of States Services was able to quickly identify a viral gastroenteritis outbreak in a nursing home. Viral gastroenteritis is not a notifiable condition in Texas. Thus, the outbreak would likely have been undetected by traditional surveillance techniques.[19]

Nebraska and North Carolina laws specifically require hospital emergency departments to report syndromic surveillance information. [20, 21] States without express mandates have adopted regulations or initiated syndromic surveillance under general public health powers or public health surveillance authority.[22] For example, the Oregon Health Authority conducts syndromic surveillance pursuant to its general duty to assess the public health status and needs of the state through statewide data collection and its responsibility to conduct epidemiological investigations of public health importance.[23] The Health Authority executes data use agreements with emergency departments that submit specified data elements to the state's syndromic surveillance system, ESSENCE. [24, 25] During the 2009 H1N1 pandemic, syndromic data were used for monitoring virus activity, measuring the impact on the health care system and informing the opening of influenza assessment centers in several jurisdictions, and supporting communications and messaging.[26]

Finally, laws in Iowa, Massachusetts, Michigan, and New York allow health care providers to voluntarily submit clinical information to public health agencies for studies that address a wide range of public health concerns, as identified by the state public health agency. Under the Michigan Public Health Code, these projects may include epidemiologic surveys, health services research, evaluation of public health programs, demonstration projects, and health statistical activities. [27] Using this authority, Michigan's public health agency established a population-based lupus registry to receive clinical data for public health purposes.[28] In Iowa, Massachusetts, and New York, health care providers may submit information to the public health agency for studies for the purpose of reducing morbidity or mortality. [29, 30, 31] Each of these laws encourage reporting by providing immunity from liability to data providers and protecting data that are submitted from use in legal proceedings.

B. Legal authority that prohibits or limits PCPs in sharing clinical data with public health agencies

Both federal and state laws impact clinical data that PCPs might provide to public health agencies. Such laws may restrict government authority to collect data, establish privacy rights in data, and create prerequisites, limitations, and conditions for sharing data.

a. State government data practice laws

Some states have enacted data practice laws that control how government data is collected, created, maintained, used and disseminated. Much like the federal Privacy Act of 1974, these laws govern any data containing personal identifiers, including health related identifiers, which is under the custody or control of a state agency.[32] The Minnesota Government Data Practices Act (MGDPA), for example, creates legal obligations and requirements on government entities regarding government data. The MGDPA regulates what data can be collected, who may see or have the data, procedures for access to the data and classification of specific types of government data.[33]

b. State public health data reporting laws

Laws that require or authorize PCPs to submit clinical data to public health agencies frequently include conditions and limitations. For example, Minnesota's immunization data statute limits data elements that the state public health agency and providers may exchange, without consent, to ten elements specified in the statute.[34]

Laws may require an individual's or parent's specific consent, obtained by a PCP or

through other means, to include health information in a registry. For example, Texas law requires the written or electronic consent of the individual or the individual's legally authorized representative before any information relating to the individual is included in its immunization registry.[35]

Other laws may allow immunization reporting unless an individual has "opted out."[36] As discussed above, Michigan's law allows health care providers to report children's height and weight, but not if the parent has opted out. Each law that authorizes PCPs to provide clinical information to public health agencies must be carefully reviewed to determine any restrictions or prerequisites.

c. Privacy laws

Clinical health data are often comprised of individual patient's identifiable health information, which are protected under various federal or state laws. Laws may apply to health information in general, a certain kind of health information, or health information from certain sources or provided for certain purposes. Many of these laws have provisions that allow PCPs to provide clinical information to public health agencies for public health purposes, without patient consent.

Most health care providers are covered entities that are subject to privacy standards established by the federal Privacy Rule adopted by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA). [37, 38] The Privacy Rule establishes national standards for maintaining the privacy and security of identifiable health information, known as protected health information (PHI). PHI is any information held by a covered entity that concerns health status, provision of health care, or payment for health care that can be linked to an individual.[39]

The Privacy Rule prohibits disclosure of an individual's PHI unless the individual authorizes the disclosure or an exception applies. The Privacy Rule recognizes the legitimate need for public health agencies to have access to PHI to carry out their public health mission. It allows health care providers to disclose PHI, without the patient's authorization, to the extent that such disclosure is required by law.[40] Thus, the Privacy Rule allows PCPs to comply with mandatory reporting laws. Additionally, the Privacy Rule allows PCPs to disclose PHI to public health agencies for the purpose of preventing or controlling disease, injury, or disability including but not limited to public health surveillance, investigation, and intervention.[41] The Privacy Rule includes additional exceptions that would allow PCPs to disclose PHI to public health agencies, such as for treatment of the individual, to avert a serious threat to health or

safety of a person or the public, to protect national security, for law enforcement under certain circumstances, and for administrative or judicial purposes. [42, 43]

Many states have privacy and confidentiality laws that apply to clinical data. These state laws would thus supplement HIPAA and may require a greater amount of protection for health information. In the case where a more stringent provision of State law is contrary to HIPAA, HIPAA provides an exception to preemption for the more stringent provision of State law, and the State law prevails. For example, the Texas Medical Records Privacy Act requires covered entities to provide patients with electronic copies of their EHR within 15 days of the patient's written request for the records. This provision reduces the timeframe a covered entity has to produce EHR records following a patient's request from 30 days under HIPAA, making it more stringent.[44]

The Family Education Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records.[45] It applies to schools that receive funds under any program administered by the U.S. Department of Education. FERPA prohibits schools from disclosing personally identifiable information from students' education records without the consent of a parent or eligible student (students who have reached 18 or attend a post-secondary institution). FERPA provides some exceptions, allowing a school to share certain information without parental consent. Unfortunately, unlike the HIPAA privacy regulations, FERPA does not allow schools to broadly share identifiable student information with public health agencies for public health purposes. Instead, FERPA allows such sharing only in connection with a health or safety emergency or to evaluate or improve educational programs.

In addition to privacy laws that apply to health information in general, federal and state laws may identify types of health information that are particularly sensitive, and provide more stringent standards for disclosure to public health agencies. Federal regulations, as well as state laws, provide stringent standards for disclosure of alcohol and drug abuse patient records.[46] Depending on the state, types of health information that are provided with heightened legal protections might also include mental health, developmental disabilities, HIV/AIDS and other sexually transmitted disease status, and genetic and counseling information.[47] In addition to health privacy laws, health care providers may be limited in sharing certain data with public health agencies by consumer protection laws. For example, many states have laws that restrict collection and disclosure of social security numbers.[48]

Privacy laws generally restrict disclosure of identifiable information, but may permit PCPs to provide de-identified information. Public health agencies should assess whether identifiable information is necessary for the proposed use. When laws allow – but do not require – disclosure of identifiable information, many health care providers decline to share

patient clinical data.[49] This makes other types of data, such as de-identified data and limited data sets, important for carrying out public health activities.

De-identified data is aggregate statistical data or data stripped of individual identifiers. Each applicable law may establish standards for de-identification, which can vary. Some laws may include specific requirements for de-identification. Under the HIPAA Privacy Rule, 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). [50] 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).

While de-identified clinical data may be sufficient for some public health activities, such data may have limited value because certain data elements, such as dates and demographic data, may be removed. The HIPAA Privacy Rule allows covered entities to disclose a "limited data set" for public health purposes pursuant to a limited use agreement.[51] 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).

d. Laws regarding transport of data

Technological advances for transfer of clinical data from PCPs to public health agencies may implicate additional laws, such as laws specific to Health Information Exchanges. Some states have enacted laws requiring patient consent to include or transmit their health information through health information exchange. For example, Nevada's law states that a patient may not be compelled to participate in an HIE. Opt-in and opt-out consent models apply, depending on the type of information transmitted.[52] Similarly, Massachusetts requires that providers that connect to the statewide HIE establish a mechanism to allow patients to opt-in to the health information exchange and to opt-out at any time.[53]

State and federal law also govern security requirements for the transport and storage of health information maintained by public health agencies. Though security and breach mitigation laws are beyond the scope of this memorandum, it is important for health

departments to consider the risk in collecting more information than is needed to carry out public health functions, especially when the information is individually identifiable or sensitive. Understanding any limitations on the secondary uses of data is also important when sharing or receiving data to or from third parties, such as PCPs.

V. Assessing laws that impact PCPs' sharing of clinical data with public health agencies

Since laws vary between states, each jurisdiction will need to identify and assess laws that apply to PCPs and public health agencies in its jurisdiction. The following areas of inquiry may assist states in assessing both state and federal laws.

a. Identify public health authority to collect information

When addressing any proposed collection, use or sharing of data, it is important to first determine where the authority for such a collection, use or sharing of the information is derived. This authority may come from a number of sources, including general authority derived from state police powers, specific authority granted under a statute or authority derived from the consent of an individual to share their PHI. To improve PCPs' compliance with mandatory reporting requirements to public health agencies or other access to data that is required by law, it is helpful to cite to the agency's authority and be able to explain to PCPs the legal basis for the data sharing.

b. Conduct an extensive survey of state and federal data sharing laws

It is imperative to conduct an extensive survey of all state and federal laws that apply to your jurisdiction. Since laws vary across jurisdictions, it is also crucial to conduct a survey of the laws of any other jurisdiction from which you are collecting, sharing or using health information. Many types of state and federal laws will govern how information can be transferred, shared and stored, including data practices laws, health information privacy laws (both general and specific laws applicable to certain kinds of conditions, providers or purposes), health information security laws, right to privacy statutory or common laws and emergency management laws.

c. *Identify any prerequisites, conditions, or limitations on data sharing*

Even when data sharing is mandated or permissible by law, there will be prerequisites, conditions or limitations placed on the sharing of data between PCPs and public health

agencies. These prerequisites, conditions and limitations will govern things such as the acceptable uses and linkages of information, how information can be transferred, shared or stored, and what privacy and security measures apply to the transfer, use, storage and disposal of the information. It is important to create a comprehensive catalog of legal data sharing requirements, as well as any reporting requirements or deadlines.

d. Determine if a Data Use Agreement is necessary or desired

A data use agreement (DUA) is a legally binding agreement among entities when sharing personally identifiable data that is covered by a legal authority, such as an authorizing statute. The agreement delineates the confidentiality requirements of the relevant legal authority, security safeguards, and each entity's data use policies and procedures. The DUA serves as both a means of informing data users of these requirements and a means of obtaining their agreement to abide by these requirements. Additionally, the DUA serves as a control mechanism for tracking an entity's data and the reason for the release of the data.[54]

Though the law may set out many of the terms necessary for the sharing of health information, DUAs serve to further outline the terms and conditions of the transfer. DUAs may be a required precondition to sharing of the certain information, such as limited data sets, or it may be a tool for to help minimize risk and maximize cooperation between parties. Specifically, DUAs can address important issues that are not covered by law or may need more detailed terms or clarification than provided by law such as limitations on data use, specifying explicit security measures or liability for harm.

VI. Recommendations to promote data sharing

Greater sharing of clinical health data can have great benefits and can enhance many public health functions beyond traditional reporting and surveillance. Even when the law allows for the sharing of data from PCPs to public health agencies, it is important for the public to be comfortable with what data is being shared and how. To ensure public trust, the benefits to sharing the data must outweigh the risks. Data sharing should maintain the underlying goals of protecting individual privacy, reducing the risk of data misuse and enhancing public trust in sharing clinical health data by demonstrating its personal and community benefit. Below are several recommendations towards developing a robust data sharing program between PCPs and public health.

A. Expand voluntary sharing of data

To increase the voluntary sharing of clinical health data that is not mandated by law, it is important for public health agencies to build relationships with PCPs that are founded on trust. A crucial step towards building trust is to be transparent about the purpose for requesting clinical health data, the potential uses of the data and the legal authority under which the data is being requested. Though providing such information may not be legally required, it may increase voluntary participation in a data sharing transaction.

The opportunities for voluntary collaboration between PCPs and public health agencies to share data are expansive. For example, the ACA requires nonprofit hospital organizations to conduct community health needs assessments (CHNA) and, in the process, consult with community members, including those with expertise in public health. Public health agencies are also responsible for the creation of Community Health Assessment (CHA) and Community Health Improvement Plans (CHIP). In some states, this is a mandatory requirement that predated the ACA. Additionally, a CHA and CHIP are required parts of the new Public Health Accreditation process. These present opportunities for collaboration between hospital systems and public health agencies.[55] Though the CHNA process is mandatory, collaboration with any specific outside entities is not required in each jurisdiction. Yet the role of clinical data in the development of both CHNAs and CHAs is crucial to understanding the health needs of the population and developing a strategy to address those needs. A voluntary collaboration through a joint CHNA/CHA development effort may be a good place to develop a new or expand upon an existing clinical data sharing program, since nonprofit hospitals are required by law to conduct CHNAs every three years. For example, in New York, local health departments (LHDs) are being asked to work with local hospitals as well as other area partners to complete a Community Health Assessment that includes a Community Health Improvement Plan. This collaboration with local health departments enable local hospitals to complete a Community Service Plan that mirrors the Community Health Needs Assessment and Improvement Strategy required for nonprofit hospitals per the Affordable Care Act.

B. Assess the need for data

When public health agencies collect and store data, they assume the legal responsibility that the data is appropriately protected, used, and disclosed. It is important to assess the need for the collection or storage of any type of data to minimize risk. When data security is compromised, state and federal breach notification laws may require that public health agencies notify individuals whose information is compromised, the press, and enforcement authorities. Violations of privacy and security laws may result in financial penalties.

C. Establish data use agreements

When data sharing is not mandated by law, it is useful to have a formal agreement that sets out the rights and responsibilities of the parties engaged in voluntary data sharing transactions.

The development and adoption of DUAs between PCPs and public health agencies could greatly increase the sharing of clinical health data. DUAs act as a rulebook for the sharing of data between organizations. They can be extremely detailed and apply to specific types of data, control secondary uses of clinical health data and enumerate limitations, restrictions and permissions on the data. DUAs can help build trust and establish rules between organizations by clearly defining expectations for the data sharing relationship.

D. Increase incentives to share data

In cases where required data sharing is not in place, voluntary sharing of clinical health data could be improved through increasing the value proposition for PCPs to share such data. This incentive model could be used both as an enticement, by providing a benefit, or as an inducement, by conditioning a necessary service on the sharing of data. Incentives for the sharing of clinical health data will increase PCPs' likeliness to engage in a data sharing program. For example, a public health agency that maintains an immunization information system could induce greater participation in the system by providing an integrated vaccine ordering capability to PCPs that report adult vaccination into the system.

Reciprocity can also be used as an incentive to increase participation in a data sharing program. By creating a bi-directional data sharing program, PCPs may voluntarily provide data to public health agencies. For example, if an immunization information system provides PCPs value by providing not just data, but actionable information through a clinical decision support system, they may more readily participate.

E. Revise federal laws to align authority to obtain data

It is important to better align the authority of public health agencies to obtain data under HIPAA and FERPA in matters regarding confidential medical records from PCP's through on-campus services or any other health information collected by an educational institution. This would promote clarify and authorize school based PCP's to securely exchange student health information with public health authorities, as defined in public health law for each state, for the purposes of ensuring coordinated healthcare services.

F. Revise state laws to expand authority to obtain data

Though public health agencies have authority to obtain many types of clinical health data for public health purposes, specific enabling legislation can increase the collection of clinical health data. Mandatory reporting requirements are an effective means to obtain specific categories or types of clinical health data. Expanding current legislation to include additional categories of mandatorily reported data or granting specific authority to request and collection certain types of data will increase sharing of clinical health data with public health agencies. Public health agencies should also maximize the use of their existing authority, such as employing laws that allow for voluntary data sharing or exercising rulemaking authority to expand existing data sharing programs.

G. Harmonize state data sharing laws

Many PCPs, such as large health care organizations, operate in several states. State data sharing laws vary greatly across jurisdictions and are often in conflict with one another. Having to manage data sharing requirements across multiple jurisdictions likely discourages large organizations from engaging in voluntary data sharing with public health agencies. Harmonizing state data sharing laws among jurisdictions might decrease the burden on multi-jurisdictional organizations and could encourage voluntary participation in data sharing programs.

H. Fill the gaps in data management

Robust data management systems provide permission controls, audit trails and documentation. They allow data to be combined more easily across time, locations and sources. By implementing a comprehensive data management system, public health agencies will be better able to account for all collections, uses and disclosures of data as well as ensure implementation of proper privacy and security measures. Providing such assurances will engender greater trust, encouraging PCPs to voluntarily share clinical health data.

I. Streamline patient consent laws and systems

Data sharing is permissible with the authorization of individual patients. Many patients, when provided with the opportunity to contribute data for the public good, will authorize such sharing. Simplifying patient consent laws to make them more comprehensible will help individuals better understand the potential uses of their data and therefore make better informed decisions about how they wish to have their data shared by PCPs and used by public

health agencies. The development of centralized repositories that maintain patient consents for the uses of their clinical health data will allow patients greater control over their own health data while also allowing for the increased sharing of clinical health data of individuals providing authorization for such sharing.

J. Use statistical de-identification or limited data sets

De-identification will always result in some loss of information, and hence a reduction in data utility, but by using a statistical de-identification method, there is greater control over the balance between privacy (i.e., a very small risk of data re-identification) and data utility (i.e., a minimal loss to the data). In cases were re-identification is of greater concern because case numbers are low or a condition is rare, data suppression might be considered. Generally, the process of statistical de-identification involves applying one or more of three different techniques:

a. Generalization. A process to reduce the precision of a data field. For example, a date can be generalized to a month and year or to a five-year interval. This process maintains the truthfulness of the data.

b. Suppression. A process for replacing a value in a data set with a missing or NULL value. For example, a 55-year-old mother in a birth registry would be an outlier and easily identifiable, so her age value would be suppressed.

c. Subsampling. A process for releasing only a simple random sample of the data set rather than the whole data set. For example, a 50% sample of the data may be released instead of all of the records.

If statistical de-identification cannot be accomplished, then a limited data set could be an alternative. A limited data set is protected health information from which certain specified direct identifiers have been removed. A limited data set may be used and disclosed for public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.

VII. Conclusion

The potential benefits to increased data sharing between PCPs and public health agencies are extensive. Though law is often seen as a barrier to increased data sharing efforts, a fine tuned strategic plan to increase data sharing can be developed that works within and

around any legal confines to maximize data sharing efforts. As discussed above, promoting the sharing of data by PCPs with public health agencies requires a clear understanding of a public health agencies' legal authority to collect and use data, the capacity to catalog all laws governing the sharing and use of data, identifying and complying with any limitations or restrictions, and the ability to maintain community trust by complying with federal and state data privacy and security laws. Additional strategies can be applied from the recommendations provided in the memorandum to encourage PCPs in providing data to public health agencies.

---

[1] For the purposes of this memorandum, public health agencies will mean an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate.

[2] Coletta, Michael. "Public Health Case Management." EPublic Health Blog. September 25, 2012. Accessed July 7, 2015. https://ephinformatics.wordpress.com/category/public-health-case-management/.

[3] "Implementation Guidance on Data Collection Standards for Race, Ethnicity, Sex, Primary Language and Disability Status." U.S. Department of Health and Human Services. Accessed July 9, 2015. http://aspe.hhs.gov/datacncl/standards/aca/4302/index.pdf.

[4] For a comprehensive list of HHS population health surveys, see "Guide to HHS Surveys and Data Resources." U.S. Department of Health and Human Services. Accessed July 9, 2015. http://aspe.hhs.gov/sp/surveys/index.cfm.

[5] Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good: Workshop Summary. Institute of Medicine (US) Roundtable on Value & Science-Driven Health Care. Washington (DC): National Academies Press (US); 2010.

[6] Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good: Workshop Summary. Institute of Medicine (US) Roundtable on Value & Science-Driven Health Care. Washington (DC): National Academies Press (US); 2010.

[7] "Learn EHR Basics." HealthIT.gov. May 21, 2014. Accessed February 10, 2015.

[8] "Meaningful Use Definition and Meaningful Use Objectives of EHRs." HealthIT.gov. February 6, 2015. Accessed June 20, 2015. http://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives.

[9] "Meaningful Use Definition and Meaningful Use Objectives of EHRs." HealthIT.gov. February 6, 2015. Accessed June 20, 2015. http://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives.

[10] Primary Care and Public Health Exploring Integration to Improve Population Health. Washington, D.C.: National Academies Press, 2012.

[11] De Leon, Samantha, and Sarah Shih. "Tracking the Delivery of Prevention-oriented Care among Primary Care Providers Who Have Adopted Electronic Health Records." *Journal of the American Medical Informatics Association* 18, no. Supplement 1 (2011): 91-95.

[12] "BMI." Michigan Care Improvement Registry. Accessed July 2, 2015. http://www.mcir.org/BMI.html.

[13] *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.

[14] Citation needed

[15] Martin DW, Lowery NE, Brand B, Gold R, Horlick G., Immunization Information Systems: A Decade of Progress in Law and Policy. J Public Health Management Practice, 2013, 00(00), 1-8. Available at http://www.immregistries.org/resources/Immunization_Information_Systems___A_Decade_Laws_998321.pdf.

[16] Administrative Rule R 325.163a, Reportable information regarding height and weight.

[17] Martin DW, Lowery NE, Brand B, Gold R, Horlick G., Immunization Information Systems: A Decade of Progress in Law and Policy. J Public Health Management Practice, 2013, 00(00), 1-8. Available at http://www.immregistries.org/resources/Immunization_Information_Systems___A_Decade_Laws_998321.pdf.

[18] Survey of State Immunization Information System Legislation, CDC, National Center for Immunization and Respiratory Diseases, available at http://www2a.cdc.gov/vaccines/iis/iissurvey/Legislation-survey.asp.

[19] Norovirus Outbreak Detected by Emergency Department Syndromic Surveillance using RedBat.

Available at http://faculty.washington.edu/lober/www.isdsjournal.org/htdocs/articles/2044.pdf.
[20] 173 Neb. Admin. Code Ch.1 § 003(2002).
[21] N.C. Admin. Code title 15A, r. 19A.0102 (2002) and N.C. Admin. Code title 15A, r. 19A.0103 (2002).
[22] Expert Meeting on Privacy, Confidentiality, and Other Legal and Ethical Issues in Syndromic Surveillance.
[23] ORS 431.110, ORS 433.004.
[24] Oregon Data Use Agreement for Syndromic Surveillance. Available at http://public.health.oregon.gov/DiseasesConditions/CommunicableDisease/PreparednessSurveillanceEpidemiology/essence/Documents/essence-dua.pdf.
[25] Electronic Surveillance System for the Early Notification of Community-Based Epidemics
[26]Chu, Anna, Rachel Savage, Don Willison, Natasha S Crowcroft, Laura C Rosella, Doug Sider, Jason Garay, Ian Gemmill, Anne-Luise Winter, Richard F Davies, and Ian Johnson. "The Use of Syndromic Surveillance for Decision-making during the H1N1 Pandemic: A Qualitative Study." *BMC Public Health*, 2012, 929.
[27] Mich. Compiled Laws, §§ 333.2621 – 333.2638.
[28] Michigan Lupus Epidemiology and Surveillance Program (MILES), grant of authority available at http://www.med.umich.edu/MiLES/authority.pdf.
[29] Iowa Code, 135.40, 135.41, 135.42.
[30] Massachusetts Laws, Section 24A.
[31] New York Public Health Law § 206(1)(j).
[32] 5 U.S.C. § 552a
[33] Minn. Stat. § 13, and Minn. R. 1205
[34] Minn. Stat. § 144.3351
[35] Texas Health and Safety Code, Sec. 161.007
[36] Martin, Lowery article
[37] 45 CFR Parts 160 and 164.
[38] add cite
[39] 45 C.F.R. 160.103.
[40] 45 CFR 164.512(a).
[41] 45 CFR 164.501, 45 CFR 164.512(b)(1)(i).
[42] 45 CFR 164.506.
[43] The Privacy Rule includes twelve public interest and benefit exceptions for permitting use of disclosure of PHI without patient authorization include: 1. Required by law (45 CFR 164.512(a)); 2. Public health activities (45 CFR 164.512(b)); 3. Victims of abuse, neglect, domestic violence (45 CFR 164.512(c)); 4. Health oversight activities (45 CFR 164.512(d)); 5. Judicial and administrative proceedings (45 CFR 164.512(e)); 6. Law enforcement purposes (45 CFR 164.512(f)); 7. Decedents (45 CFR 164.512(g)); 8. Cadaveric organ, eye, or tissue donation (45 CFR 164.512(h)); 9. Research (45 CFR 164.512(i)); 10. Prevent or lessen serious threat to health or safety (45 CFR 164.512(j)); 11. Specialized government functions (45 CFR 164.512(k)); 12. Workers' compensation (45 CFR 164.512(l)).
[44] Texas Health and Safety Code, Sec. 181.001
[45] 20 U.S.C. § 1232g
[46] 42 CFR Part 2.
[47] Examples of such state laws include the following: IND. CODE. ANN. § 16-18-2-226 (mental health information); MASS. GEN. LAWS. ch. 111, § 70F; ARIZ. REV. STAT. 12-2802; 74 ILCS 110/ (mental health information); 410 ILCS 305/ (HIV/AIDS information); 410 ILCS 513/ (genetic information); 410 ILCS 50/ (medical information generally).
[48] Using Data to Improve Education: A Legal Reference Guide to Protecting Student Privacy and Data Security: State SSN Protection Laws – State-by-State Summary Table. Available at http://dataqualitycampaign.org/wp-content/uploads/2015/06/SSN-protection-laws_CHART_02-21-for-posting.pdf.
[49] K. El Emam, J. Mercer, K. Moreau, I. Grava-Gubins, D. Buckeridge, and E. Jonker. "Physician Privacy Concerns When Disclosing Patient Data for Public Health Purposes During a Pandemic Influenza Outbreak," *BMC Public Health* 11:1 (2011): 454.
[50] 45 CFR 164.514.
[51] 45 CFR 164.514.

[52] NRS 439.538; NRS 439.591.
[53] M.G.L.A. 118I § 13.
[54] "Practices Guide: Data Use Agreement." U.S. Department of Health and Human Services. Accessed July 1, 2015. http://www.hhs.gov/ocio/eplc/EPLC Archive Documents/55-Data Use Agreement (DUA)/eplc_dua_practices_guide.pdf.
[55] "Achieving the Community Health Needs Assessment Requirement for Tax - Exempt Community Hospitals in North Carolina." North Carolina Public Health. Accessed July 1, 2015. http://publichealth.nc.gov/lhd/cha/docs/CommunityNeedsAssessmentPolicyGuidance-FINAL.pdf.