USING
ELECTRONIC HEALTH DATA
FOR
COMMUNITY HEALTH

Example Cases
and Legal Analysis

November 2017

Table of Contents

Introduction

The Institute of Medicine has defined the three core functions of public health as:[1]

- Assessment, the identification of health problems;
- Policy development, the mobilization of necessary effort and resources to address health problems; and
- Assurance, making sure that vital conditions are in place and that crucial services are received.

Each of these functions requires access to high-quality data related to the nature of health problems and their potential solutions. Public health agencies obtain data from a wide variety of sources, including vital records, laboratories, inspections, public surveys, and reporting from clinicians. Yet, important gaps in the understanding of the health of populations remain. These gaps relate to the fact that many existing data sources provide data, aggregated at a high level, infrequently and with a significant delay.[2] As a result, public health agencies struggle to respond rapidly and effectively to many important health problems facing their communities.

Electronic health data refers to data generated during clinical encounters and stored electronically in electronic health records and other data systems. Because of the rapid growth in adoption of these technologies across medicine, access to electronic health data offers an opportunity for a leap forward in data access to address community health challenges. A recent survey of 45 senior public health officials found particular interest in using electronic health data "to both guide action and geographic 'hot spotting' of both communicable and chronic diseases not included in statutory reporting requirements."[3]

How specifically might a public health agency use electronic health data to move the needle on a public health challenge, and is it possible to access needed data under the law? This white paper addresses these two essential questions in the following two ways:

Use Cases. First, the paper sets out six illustrative examples of how a public health agency might use electronic health data to make progress on childhood asthma, a common and preventable chronic illness. Asthma is a disease of individuals, many

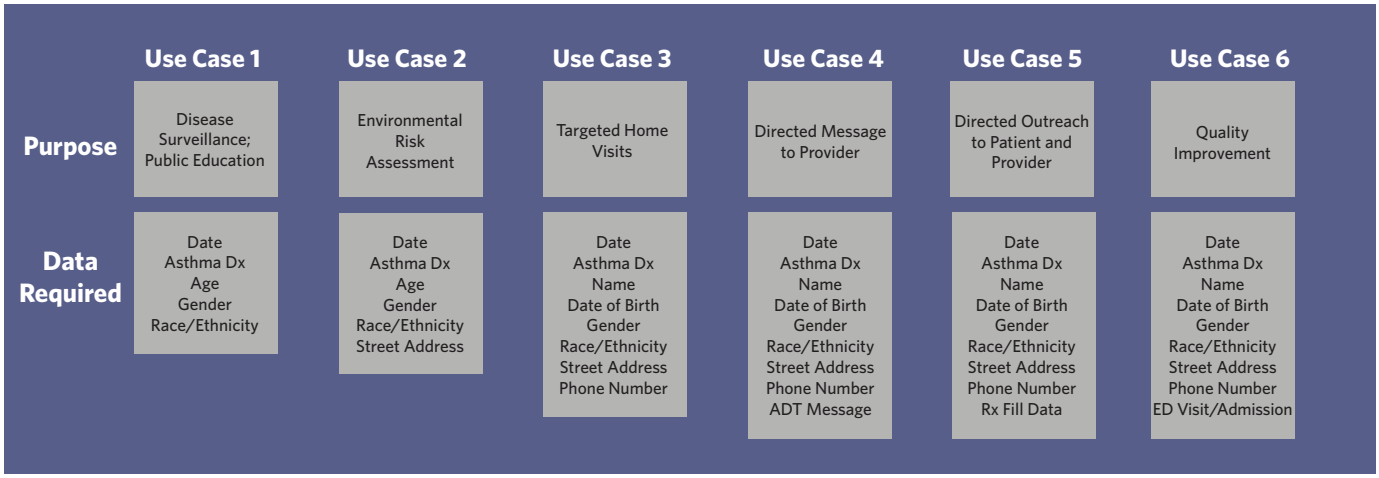

Figure 1: Data Required for Each Case

[1] Institute of Medicine. *The Future of Public Health.* 1988, available at http://www.nationalacademies.org/hmd/Reports/1988/The-Future-of-Public-Health.aspx .

[2] Sharfstein JM. Using health care data to track and improve public health. *JAMA.* 2015 May 26;313(20):2012-3.

[3] Castrucci BC, Rhoades EK, Leider JP, Hearne S. What gets measured gets done: an assessment of local data uses and needs in large urban health departments. *J Public Health Manag Pract.* 2015 Jan-Feb;21 Suppl 1:S38-48.

of whom require daily medication to prevent serious exacerbations. At the same time, asthma is a disease of the community, with poor housing conditions and air pollution leading to significant clusters of illness. These use cases cover a range of potential data applications including surveillance, geographic analysis, identification of high-risk patients, engagement with clinicians, and evaluation of interventions. Associated with each case is a brief discussion of how it might be applied to other pressing public health challenges, including the opioid epidemic.

HIPAA Analysis. Second, the paper addresses the major federal law pertaining to the use of electronic health data, the Health Insurance Portability and Accountability Act, better known as HIPAA. The authors employed standard legal research methods and consulted applicable statutes, regulations, legislative materials, secondary sources, and practice materials as necessary. HIPAA, and its implementing regulations, recognizes the legitimate need for public health agencies to gain access to private health information to carry out public health activities.[4] To do so responsibly and successfully under the law, public health agencies must be clear about their goals, specific in their requests, and take steps to assure the confidentiality of key data. In addition to an explanation of how the plan for data sharing is legal under HIPAA for each use case, the white paper includes a detailed question-and-answer summary of HIPAA's role in providing health agencies access to electronic health data.

This paper focuses on permissible voluntary disclosures under federal law—what the healthcare system can share with public health agencies under HIPAA to address major public health challenges. It is not intended to provide guidance on mandatory disclosures, and it does not address additional restrictions on data use that may be set under state law.

The paper also assumes that the data collection and use described in the following cases are conducted with a commitment to the ethical principles that animate public health, including respect for communities, social justice, and health equity. The ultimate goal of all public health activities is to protect and promote the health of communities. The activities described should be conducted with an appropriate level of attention to the privacy of the information collected and adopt the necessary protections to minimize the potential for breaches of confidentiality. Moreover, health departments should seek public input when designing interventions, provide access to care for people identified in need, and share the outcomes of key initiatives with their communities.

The paper concludes with a set of recommendations for health departments interested in gaining access to electronic health data as part of a set of activities to improve the health of their communities.

[4] U.S. Department of Health and Human Services. Disclosures for public health activities. 26 July 2013. Accessed July 10, 2017 at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-public-health-activities/index.html.

Use Case 1

Is Childhood Asthma Rising or Falling?

Purpose. The county health department is interested in reducing the burden of childhood asthma in the county. A core component of this effort is the regular assessment of the state of asthma. This is core public health surveillance—understanding the burden of disease to guide allocation of funds, inform program designs, and determine whether efforts are having the intended effect. Data reflecting time trends of asthma morbidity might allow the health department to strategically time the implementation of interventions to maximize impact. Time series data pertaining to asthmatic episodes might also be used to inform health messages to the public about environmental conditions that are likely to trigger asthma attacks.

Data Request. The health department requests a weekly data file from each area hospital with information about county residents under age 21 diagnosed with asthma during an emergency department visit or hospital admission. For each emergency department visit or hospital admission for asthma, the data file should include the following fields: date, age in years, gender, and race/ethnicity. The data file should not include name, social security number, address, or other sensitive or identifying information. The health department asks that hospitals provide this data file at least weekly with a lag of two weeks or less.

Plan for Data Use. The health department will combine and analyze the hospital data on a weekly basis for internal use. Analysis of these data will involve looking for trends by date, age, race/ethnicity, and gender. These reports will inform program development and facilitate monitoring of the burden of disease.

In addition, the health department intends to release a public report on childhood asthma every six months with key findings from surveillance. The data will be reported in aggregate, without disclosure of identifiable patient information. The health department has separately established a policy on patient privacy, based on a policy from the Centers for Medicare and Medicaid Services[5] that requires the suppression of cell sizes less than 10 in publicly released reports. This asthma report will be issued in accordance with this policy.

HIPAA Analysis. As explained below, the health department's plan to use electronic health data to assess trends in asthma is permissible under HIPAA. It would be *legal* for hospitals to share the requested data for this purpose.

In this use case, the health department has clearly articulated a need for information related to a public health activity—surveillance of pediatric asthma-related emergency department visits and hospitalizations by county residents. This clear articulation gives the health department the legal authority to request and receive protected health information from local hospitals and healthcare providers under HIPAA.

The health department has carefully described the data elements that are necessary to fulfill the public health activity. This careful inventory of data elements meets HIPAA's minimum necessary requirement (described in greater detail in this report's HIPAA section), and allows hospitals or health providers to voluntarily share the requested information with the health department.

The health department may maintain and use the health data collected from hospitals and healthcare providers for its internal surveillance program. When the health department wants to release this data to inform the public, the information must be de-identified in accordance with HIPAA. The health department has a policy, based on the Centers for Medicare and Medicaid Services' policy regarding cell size suppression, which meets HIPAA standards for de-identification. This allows the health department to comply with patient privacy requirements while also providing valuable public health information regarding asthma to the public.

[5]CMS (Medicare) Data. *CMS (Medicare) Data | CHS-NHLBI*. N.p., n.d. Web. 26 Mar. 2017. <https://chs-nhlbi.org/CHS_CMSData>.

Additional Applications. Real-time surveillance for other preventable conditions and manageable chronic illnesses using electronic health data can also facilitate health improvement. For example, health departments can monitor opioid overdoses via data on emergency department visits, complementing the reports of fatal overdoses from coroners or the Office of the Medical Examiner. Health departments can also use electronic health data to conduct surveillance on preventable causes of injury resulting from medical treatment. For example, adverse drug events are a highly cited and preventable cause of hospital admission.[6] In two different studies, investigators utilized emergency department visits to monitor adverse drug events and develop prevention strategies.[7,8]

[6]Budnitz, D.S., et al., National surveillance of emergency department visits for outpatient adverse drug events. JAMA, 2006. 296(15):1858-66.

[7]Budnitz, D.S., et al., National surveillance of emergency department visits for outpatient adverse drug events. JAMA, 2006. 296(15):1858-66.

[8]See, I., et al., Emergency department visits and hospitalizations for digoxin toxicity: United States, 2005 to 2010. Circ Heart Fail, 2014. 7(1):28-34.

Use Case 2

Where Are Housing Conditions Triggering Childhood Asthma?

Purpose. Research has shown that ambient conditions and hazards at home—including mold, cockroaches, mouse urine, and other allergens—can trigger asthma attacks.[9] Moreover, housing interventions can reduce the severity of asthma among children at risk.[10] The county health department is interested in identifying specific residential blocks in the county with high burdens of childhood asthma in order to assess environmental conditions and consider a range of potential interventions.

Data Request. The health department requests a regular data file from each area hospital with information about county residents under age 21 diagnosed with asthma during an emergency department visit or hospital admission. For each emergency department visit and hospital admission for asthma, the data file should include the following fields: specific street address, date, age in years, gender, and race/ethnicity. The data file should not include name, social security number, or other sensitive or identifying information. The health department asks that hospitals provide this data file at least weekly with a lag of two weeks or less.

Plan for Data Use. The health department will combine and analyze these data on a weekly basis to identify specific geographic areas of highest risk. Once identified, the health department will assess the external air quality in the vicinity and offer the services of environmental inspectors to assess home hazards to all in the area. The services provided will not involve releasing specific healthcare data publicly.

As the need for services is identified, the health department will coordinate with the housing authority and other agencies to arrange for the remediation of hazards. This may include community-based rodent control programs, promotion of the tobacco quitline, small home repairs, and access to legal aid for renters to obtain corrective action by landlords. The health department will not disclose any personally identifying medical information to other public sector departments involved in remediation efforts.

The health department will also use geocoded data to construct a heatmap of areas with high asthma burden in the city. This map will allow the health department to monitor whether and how areas of highest asthma burden change over time. The construction of a heatmap will also be instrumental for the health department in determining where to deploy neighborhood-based services, such as environmental monitoring. The heatmap will be maintained by the health department and will not be released in a way that permits identification of any geographic areas with fewer than 10 cases, as the health department has concluded that this would preclude identification of any individual.

HIPAA Analysis. As explained below, the health department's plan to combine and analyze patient data, including specific street addresses, on a weekly basis to identify specific geographic areas of highest risk is permissible under HIPAA. It would be *legal* for the hospitals to share the requested data for this purpose.

In this use case, the health department has clearly articulated a need for health information, including geographic data, related to a public health activity—assessment of home hazards related to asthma and the provision of remedial services to address health risks. This clear articulation gives the health department the legal authority to request and receive protected health information from local hospitals and healthcare providers under HIPAA.

The health department has carefully described the data elements that are necessary for fulfilling the public health activity. It also carefully limits the data elements to only those that are necessary to fulfill the public health activity. This careful inventory of data elements meets HIPAA's minimum necessary

[9] Matsui EC. Environmental control for asthma: recent evidence. Curr Opin Allergy Clin Immunol. 2013 Aug;13(4):417-25.

[10] Krieger J, Jacobs DE, Ashley PJ, Baeder A, Chew GL, Dearborn D, Hynes HP, Miller JD, Morley R, Rabito F, Zeldin DC. Housing interventions and control of asthma-related indoor biologic agents: a review of the evidence. J Public Health Manag Pract. 2010 Sep-Oct;16(5 Suppl):S11-20.

requirement, described in greater detail in this report's HIPAA section, and allows hospitals or health providers to voluntarily share the requested information with the health department. The health department may maintain and use the identifiable health data collected from hospitals and healthcare providers for the internal home hazard program. The health department may also release necessary information to the housing authority and other agencies to arrange for the remediation of hazards, in furtherance of the health department's public health activity. In this case, the health department is not disclosing information to other agencies about the health of an individual and therefore these disclosures do not fall under HIPAA regulation.

Additional Applications. Using electronic health data to find hot spots of illnesses can have positive benefits for health conditions beyond asthma.[11] For example, a health department can map concentrations of opioid overdoses to conduct outreach to specific parts of the city to provide naloxone and access to effective addiction treatment. In Baltimore, the health department is using electronic health data to develop maps of older adults suffering from serious falls; the goal of the city's BFRIEND initiative is to use this information to guide community-based prevention strategies.[12] Other potential examples include finding areas with high levels of uncontrolled diabetes in order to promote access to healthier food options, areas with high levels of sleep-related infant deaths to promote safe sleeping arrangements, and areas with chronic lung disease to promote smoking cessation.

[11] Comer KF, Grannis S, Dixon BE, Bodenhamer DJ, Wiehe SE. Incorporating Geospatial Capacity within Clinical Data Systems to Address Social Determinants of Health. Public Health Rep. 2011;126(Suppl 3):54–61.

[12] DASH Program.4 August 2016. Engaging Neighborhoods to Use Data for Fall Prevention. Accessed December 19, 2016 at http://dashconnect.org/2016/08/04/engaging-neighborhoods-to-use-data-for-fall-prevention/

Use Case 3

Would You Like a Home Visit?

Purpose. Health departments often run programs to improve the health of individuals with chronic or recurring conditions. In the case of asthma, health departments can send nurses and other professionals to the home to support families in reducing allergens and in properly monitoring and managing a child's asthma.[13] The health department is interested in identifying children with severe asthma who could benefit from evidence-based services at home.

Data Request. The health department requests a regular data file from each area hospital with identifying information for all individuals under age 21 admitted to the hospital with a discharge diagnosis of asthma. For each hospital admission for asthma, the data file should include the following fields: name, date, date of birth, address, phone number, gender, and race/ethnicity. The file should not include social security number or other sensitive or identifying information. The health department asks that hospitals provide this data file at least weekly with a lag of two weeks or less.

Plan for Data Use. The health department will combine these data to develop a registry of children admitted to the hospital for asthma. Those most frequently admitted will be contacted by the health department and offered home visits and care coordination. The health department will work with other city agencies to address housing conditions.

HIPAA Analysis. As explained below, the health department's plan to combine and analyze patient data, including names and specific street addresses, on a weekly basis to identify specific children for the registry of those admitted for asthma is permissible under HIPAA. It would be *legal* for the hospitals to share the requested data for this purpose.

In this use case, the health department has clearly articulated a need for health information—including identifiable demographic data, related to a public health activity—reaching out to offer important health services to children and families. This clear articulation gives the health department the legal authority to request and receive protected health information from local hospitals and healthcare providers under HIPAA. The health department has carefully described the data elements that are necessary for fulfilling the public health activity. It also carefully limits the data elements to only those that are necessary to fulfill the public health activity. This careful inventory of data elements meets HIPAA's minimum necessary requirement, described in greater detail in this report's HIPAA section, and allows hospitals or health providers to voluntarily share the requested information with the health department. The health department may use the information collected to reach out and contact the families to offer them home-based services. Then, consistent with HIPAA, the health department may use this information to support the provision of home-based services with the consent of the families.

Additional Applications. Health departments can offer different types of support to high-risk individuals with a range of medical conditions. For example, a health department can use electronic health data to identify individuals who suffer from nonfatal overdoses to offer peer support and referral to addiction treatment.[14] A health department can develop a program for high utilizers of emergency department care, or individuals suffering from preventable complications of chronic illnesses. Finding candidates for these programs through electronic health data can help ensure that limited resources are assisting those most in need.

---

[13] Le Cann P, Paulus H, Glorennec P, Le Bot B, Frain S, Gangneux JP. Home Environmental Interventions for the Prevention or Control of Allergic and Respiratory Diseases: What Really Works. J Allergy Clin Immunol Pract. 2016 Sep 21. pii: S2213-2198(16)30313-0.

[14] Pollini RA, McCall L, Mehta SH, Vlahov D, Strathdee SA. Non-fatal overdose and subsequent drug treatment among injection drug users. Drug Alcohol Depend. 2006 Jun 28;83(2):104–10.

Use Case 4

Don't Forget to Check the Asthma Care Plan

Purpose. Many children with asthma return time and again to the emergency department because they lack a consistent source of primary care.[15] It is difficult for families to follow asthma care plans when each visit brings about a new set of instructions. To address this problem, a health department might be interested in developing a tool to flag patients at highest risk and alert clinicians at the moment of care about the existence of care plans and the need for greater coordination.

The health department is interested in alerting emergency departments when children with severe asthma are present, so that clinicians can check the asthma care plan and understand specific patient needs.

Data Request. The health department requests that the hospital permit the local health information exchange to match, in real time, the Admission, Discharge and Transfer (ADT) message created at the start of every emergency department visit with a list of children with asthma care plans, and then alert both the hospital and the health department when a child with a care plan is seen in the hospital. The ADT message includes patient name, date of birth, and address, as well as chief complaint and insurance information.

Plan for Data Use. The health department will maintain a registry of children with severe asthma (following Use Case 3), which will be linked to an application containing a care management plan for each child. The Health Information Exchange will cross-check the ADT against the registry through an automated electronic process to identify a positive match. When there is a match, the Health Information Exchange will send the emergency department an alert that will make the child's asthma care plan accessible to the clinician and the health department an alert to update the care plan. The health department will only receive the alert from the Health Information Exchange for children in the registry.

HIPAA Analysis. As explained below, the health department's request is permissible under HIPAA. It would be *legal* for the hospitals to share the requested data for this purpose.

In this use case, the health department has clearly articulated a need for hospitals to permit the health information exchange, which has access to ADT feeds for clinical care, to make a match.[16] The match both provides clinicians with access to a patient's asthma care plan to ensure proper treatment and coordination of care and allows the health department to track the needs of high-risk children This clear articulation gives the health department the legal authority to request and receive protected health information from local hospitals and health care providers under HIPAA.

In this case, the health department does not obtain information for patients not matched by the health information exchange.

The health department has carefully described the data elements that are necessary for fulfilling the public health activity. This meets HIPAA's minimum necessary requirement and allows hospitals or health providers to voluntarily share the requested information with the health department.

In this case, the health department is only sharing information back to a hospital for treatment purposes, which is a permitted disclosure under HIPAA. The health department is making no further disclosures that might implicate restrictions under HIPAA.[17]

Additional Applications. Health departments can use electronic health data to enhance coordinated care for patients with a variety of conditions. In Louisiana, clinicians receive alerts when patients with HIV infection in need of treatment seek episodic care.[18] Other potential examples include efforts to assist high-risk patients with sickle cell disease, high-risk pregnancy,[19] and risk of serious falls.

---

[15] Behr JG, Diaz R, Akpinar-Elci M. Health Service Utilization and Poor Health Reporting in Asthma Patients. Int J Environ Res Public Health. 2016 Jun 30;13(7). pii: E645.

[16] This exchange would need to be covered by a data sharing or other relevant agreement.

[17] There are other mechanisms for this match to take place besides through a Health Information Exchange. These include: match by the hospital itself, or match by the health department. If the latter, the hospital could establish a business associate agreement with the hospital for this purpose.

[18] Herwehe, J et al., Implementation of an innovative, integrated electronic medical record (EMR) and public health information exchange for HIV/AIDS. J Am Med Inform Assoc, 2012. 19(3):448-52.

[19] Ahmed L, Jensen D, Klotzbach L, et al. Technology-enabled transitions of care in a collaborative effort between clinical medicine and public health: A population health case report. 31 March 2016. National Academy of Medicine. Accessed July 10, 2017 at https://nam.edu/wp-content/uploads/2016/03/Technology-Enabled-Transitions-of-Care-in-a-Collaborative-Effort-between-Clinical-Medicine-and-Public-Health.pdf.

Use Case 5

Are Children Filling Their Prescriptions for Needed Asthma Medications?

Purpose. Children with moderate to severe asthma use "controller" medications, such as inhaled corticosteroids. However, studies have shown that doctors may underuse these medications, leaving children dependent on "rescue" medications.[20] A particular concern is that overuse of rescue medications by some children may increase the risk of death.[21] The health department is interested in helping promote medication adherence by working with physicians of asthma patients.

Data Request. The health department requests that hospitals add source of payment to the regular data file submitted by hospitals in Use Case 3 (i.e. name, address, date of visit). For children with multiple emergency department visits and hospitalizations for asthma, the health department will request prescription fill data from a pharmacy data service (which is also covered by HIPAA).

Plan for Data Use. For identified children who are not receiving a regular prescription for a controller medication, the health department will provide outreach to the families of patients and their primary care doctors to support improved access to therapy.

HIPAA analysis. As explained below, the health department's data requests to hospitals for source of payment and prescription fill data are permissible under HIPAA. It would be *legal* for the hospitals and pharmacy data services to share the requested data for this purpose.

In this use case, the health department has clearly articulated a need for health information related to a public health activity—promoting medication adherence by working with the physicians of patients with asthma to prescribe asthma "controller" medications. This clear articulation gives the health department the legal authority to request and receive protected health information from local hospitals, healthcare providers, and pharmacy data services under HIPAA.

The health department has carefully described the data elements that are necessary for fulfilling the public health activity. In this case, the data requested is limited to identifying information described in Case 3 as well as source of payment data and prescription fill data for children with multiple emergency department visits. This meets HIPAA's minimum necessary requirement and allows hospitals, health providers, or pharmacy data services to voluntarily share the requested information with the health department.

In this case, the health department is only sharing information back to clinicians and/or patients for treatment purposes, which is a permitted disclosure under HIPAA. The health department is making no further disclosures that might implicate restrictions under HIPAA.

Additional Applications. In addition to asthma, use of electronic health data can facilitate public health oversight of other clinical conditions. In one study, researchers analyzed electronic health data from family medicine practices to identify and follow up with patients with diabetes not receiving treatment according to guidelines.[22]

---

[20] Hasegawa K, Ahn J, Brown MA, Press VG, Gabriel S, Herrera V, Bittner JC, Camargo CA Jr; MARC-37 Investigators. Underuse of guideline-recommended long-term asthma management in children hospitalized to the intensive care unit: a multicenter observational study. Ann Allergy Asthma Immunol. 2015 Jul;115(1):10-6.e1.

[21] Spitzer WO, Suissa S, Ernst P, Horwitz RI, Habbick B, Cockcroft D, Boivin JF, McNutt M, Buist AS, Rebuck AS. The use of beta-agonists and the risk of death and near death from asthma. N Engl J Med. 1992 Feb 20;326(8):501-6.

[22] Crosson JC, Ohman-Strickland PA, Hahn KA, DiCicco-Bloom B, Shaw E, Orzano AJ, et al. Electronic Medical Records and Diabetes Quality of Care: Results From a Sample of Family Medicine Practices. Ann Fam Med. 2007 May;5(3):209-15.

Use Case 6

Is This Program Reducing Illness from Asthma?

Purpose. The health department would like to initiate a quality improvement project to assess the impact of specific interventions.

Data Request. The health department requests from area hospitals a single data file that includes children in the county who have been seen in the emergency department or hospitalized for asthma in the previous six months. The data requested includes name, date of birth, street address, date of visit, gender, race/ethnicity, and emergency department visit or hospitalization.

Plan for Data Use. The health department will combine the data files from the hospitals to assess trends in hospital care for asthma for different groups of patients, including:

- Those that live in geographic areas that received specialized interventions, compared to those who do not;
- Those who were offered case management services, compared to those who were not; and
- Those who have an updated asthma care plan, compared to those who do not.

The health department intends to employ these data to determine whether to continue or change specific intervention efforts.

HIPAA Analysis. As explained below, the health department's request to hospitals for data to use for program assessment is permissible under HIPAA. It would be *legal* for the hospitals to share the requested data for this purpose.

In this use case, the health department has clearly articulated a need for health information to assess a public health activity for the purpose of quality assurance and improvement. In this regard, hospital data enables the health department to determine whether to continue or change specific public health intervention efforts to improve the health of the community that it serves. This clear articulation gives the health department the legal authority to request and receive protected health information from local hospitals and healthcare providers under HIPAA.

The health department has carefully described the data elements that are necessary for fulfilling the public health activity. In this case, the data requested is limited only to the information necessary to complete the quality improvement project. This meets HIPAA's minimum necessary requirement and allows hospitals and health providers to voluntarily share the requested information with the health department.

In this case, the health department is only using the data for internal quality improvement activities and the health department is not sharing this information outside the agency. In this case, it is clear that the health department is not conducting research, which might implicate other restrictions under HIPAA.

Additional Applications. Many programs that seek to improve health outcomes are not regularly evaluated for effectiveness but should be. For example, a health department that refers to addiction treatment might be able to compare the rates of overdose by type of therapy or treatment provider. Similarly, community-based tobacco cessation programs, diabetes nutrition programs, and falls prevention efforts can be assessed using electronic health data.[23]

[23] Wilson, Sandra R., et al. A controlled trial of an environmental tobacco smoke reduction intervention in low-income children with asthma. *CHEST Journal* 120.5 (2001): 1709-1722.

HIPAA Analysis and Related Questions

The FAQs below address the HIPAA Privacy Rule as it relates to the sharing of healthcare data with public health agencies and to the data's use by public health agencies.

This information is intended to provide general guidance to assist public health agencies and others to assess HIPAA's applicability to a variety of situations that involve data sharing for public health purposes. This information is not intended to provide legal advice; readers should consult their attorney regarding legal compliance for specific data sharing proposals.

Beyond HIPAA, a public health agency should identify any other state or federal laws that apply to its collection, sharing, and protection of specific data and ensure that data sharing is consistent with all laws.

SECTION 1: ABOUT HIPAA

Q: What is HIPAA?

A: The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[24] is a federal law that establishes national standards for electronic healthcare transactions. HIPAA governs most clinical health data, including all electronic health records data, and sets minimum standards that "covered entities" must meet to ensure an appropriate level of privacy and security for patient data.

Q: What is the HIPAA Privacy Rule?

A: The Privacy Rule requires covered entities to apply appropriate safeguards to protect the privacy of personal health information (known as "protected health information") and sets limits and conditions on potential uses and disclosures of patient information without authorization.[25]

Q: What is "Protected Health Information" (PHI) under the HIPAA Privacy Rule?

A: PHI is information, including demographic information:[26]

- In any form: written, electronic, or oral
- Relating to past, present, or future
  - Physical or mental health status or condition
  - Provision of healthcare
  - Payment for provision of healthcare
- That identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual
- Information is no longer PHI 50 years after individual's death

Generally, HIPAA is concerned with record-level data. However, while aggregate data may not directly identify an individual—due to a combination of data elements, small cell size, or other data reasonably available—the risk that individuals might be identified must also be considered with regard to aggregate data.

SECTION 2: SHARING OF DATA FROM HEALTHCARE ORGANIZATIONS TO PUBLIC HEALTH AGENCIES UNDER HIPAA

Virtually all healthcare organizations, including clinics and hospitals, are considered "covered entities" subject to the HIPAA Privacy Rule.[27]

Q: As "covered entities," can healthcare organizations disclose PHI to public health agencies under the HIPAA Privacy Rule?

A: Yes. The Privacy Rule includes a provision that recognizes the legitimate need for public health agencies to have access to

[24] Pub. L. 104-191, 42 U.S.C. §300gg et seq.

[25] 45 CFR Parts 160 and 164, which can be accessed through the electronic Code of Federal Regulations at https://www.ecfr.gov. HHS' Office for Civil Rights, which enforces HIPAA, provides numerous resources and guidance documents on its website at https://www.hhs.gov/hipaa/index.html.

[26] 45 CFR 160.103, 164.502.

[27] Healthcare organizations that do not transmit electronic information for the purpose of payment are not covered. 45 CFR 160.103, 164.104.

PHI to carry out public health activities. This provision allows covered entities to disclose PHI to "public health authorities" and their authorized agents, without a patient's prior authorization.[28] A public health authority is a public health or other agency that is legally authorized to receive the information for the public health purposes of preventing or controlling disease, injury, or disability, including, but not limited to, public health surveillance, investigation, and intervention.[29]

Q: When does HIPAA permit healthcare organizations to share data with public health agencies?

A: The public health provision applies to both uses and disclosures that are *required by law* and uses and disclosures that are *authorized by law*. In this regard:

- A covered entity may use or disclose PHI to a public health agency to the extent that such use or disclosure is *required by law* and the use or disclosure complies with and is limited to the relevant requirements of such law.[30] Thus, the Privacy Rule allows healthcare providers to comply with mandatory reporting law requirements.
- A covered entity may use or disclose PHI to a public health agency that is *authorized by law* to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions.[31] If a public health agency has the legal authority to collect and use information for public health purposes, this provision allows a covered healthcare provider to voluntarily provide PHI without the patient's prior authorization.[32] Often in a voluntary reporting arrangement, an agreement stating the data elements and the uses of the data will be signed between the parties either in the form of a data sharing agreement or a memorandum of understanding.

Q: How much data is a healthcare organization authorized under HIPAA to share with a public health department?

A: The HIPAA Privacy Rule has a "minimum necessary standard" that requires covered entities to reasonably limit lawful disclosures of PHI to public health agencies to the minimum amount necessary to accomplish the intended purpose or carry out a function.[33]

Q: Who has the burden of deciding what level of detail meets the minimum necessary standard for public health disclosures?

A: Covered entities are not required to make a minimum necessary determination for public health disclosures that are made with an individual's authorization or for disclosures that are required by law.[34] Disclosures to a public health authority that are authorized by law, including voluntary disclosures, allow a covered entity to reasonably rely on the judgment of the public health agency as to the minimum amount of information that is needed to accomplish the public health purpose.[35] Under these circumstances, the minimum necessary standard shifts the burden of disclosure from providers to public health agencies, especially in the case of voluntary disclosures for public health purposes. This means that public health agencies should carefully evaluate what information is being requested from providers and how that information fulfills the stated public health purpose. Public health agencies might alleviate a healthcare provider's concerns, if any, about HIPAA compliance 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 reasonably rely on such a written statement, or if a written statement would be impracticable, an oral statement of such legal authority.[36]

Q: What should covered entities do to comply with the minimum necessary standard?

A: For routine or recurring public health disclosures, such as regular, real-time reporting of asthma-related health data

---

[28] 45 CFR 164.512(b).

[29] 45 CFR 164.501, 164.512(b).

[30] 45 CFR 164.512(a).

[31] 45 CFR 164.512(b).

[32] 64 Fed Reg 59929 (November 3, 1999). The U.S. Department of Health and Human Services interpreted "authorized by law" to mean that "a legal basis exists for the activity . . . [and] include[s] both actions that are permitted and actions that are required by law."

[33] 45 CFR 164.502(b), 164.514(d).

[34] 45 CFR 164.502(b).

[35] 45 CFR 164.514(d)(3)(iii)(A).

[36] 45 CFR 164.514(h)(2)(iii). An example of such a statement, issued by the Wisconsin Department Health and Family Services regarding reporting of animal bites, which is not mandatory, is posted at http://www.co.washington.wi.us/uploads/docs/CHN_Bite_Reporting_HIPAA.pdf. Accessed July 31, 2017.

by area healthcare providers, covered entities may establish standard protocols. These protocols should detail minimum necessary policies and procedures as well as address the types and amount of PHI that may be disclosed for the intended purpose.[37]

Q: May a covered entity share de-identified information that does not include PHI with a public health agency?

A: Yes. HIPAA does not apply to "de-identified" information. If information satisfies HIPAA's de-identification standards,[38] healthcare organizations may share it with public health agencies, other organizations, and even the public.

Q: When is information de-identified?

A: For HIPAA, information is de-identified if it meets either the "safe harbor standard" or the "expert determination standard" described below. While the risk of re-identification does not have to be "zero" (i.e., most likely impossible), these standards are to ensure that the risk that information will identify an individual is sufficiently small.

Safe harbor. The safe harbor de-identification method requires the removal of 18 specified identifiers of the individual or of relatives, employers, or household members of the individual. These identifiers include personal information, such as name, address, and social security number. They also include 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). Once these identifiers are removed, data are deemed de-identified 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.[39]

Expert determination. This method requires a formal determination and documentation by a qualified statistician using accepted analytic techniques to conclude that the risk of re-identification is substantially limited.[40]

The safe harbor method is often favored for de-identification because it does not require access to a qualified statistical expert. However, removing all 18 identifiers often diminishes the usefulness of the data, making the expert determination process the only way to obtain the detail needed for a defined purpose.

Q: Are there options for disclosure to public health agencies that fall between full individual level data and fully de-identified data?

A: Yes. The HIPAA Privacy Rule allows covered entities to disclose a "limited data set" for public health purposes pursuant to a limited use agreement.[41] A limited data set is still PHI. However, it is more useful than de-identified data 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). When it is sufficient for the intended public health purpose, a limited dataset has some advantages for healthcare organizations over fully identifiable data. For example, a covered entity is not required to provide an accounting for a disclosure where information disclosed is part of a limited data set.[42]

Q: Does disclosure by a covered entity under HIPAA to a public health agency depend on whether the public health agency itself is covered under HIPAA?

A: No, disclosure does not depend on the HIPAA status of the public health agency. However, the HIPAA status of the public health agency does pertain to the disclosure of data, as noted below in Section 4.

---

[37] 45 CFR 164.514(d)(3)(i).

[38] 45 CFR 164.514(a); See, OCR Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule, November 26, 2012. Accessed July 31, 2017 athttp://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

[39] 45 CFR 164.514(b).

[40] *Id.*

[41] 45 CFR 164.514(e).

[42] 45 CFR 164.528.

SECTION 3: PUBLIC HEALTH USE OF DATA FROM HEALTHCARE ORGANIZATIONS

Q: How might a public health agency use PHI that it obtains from a healthcare organization that is a covered entity under HIPAA?

A: Public health agencies, which obtain PHI from covered entities, may use this information for the full range of public health activities that include, but are not limited to:

- Identify, measure, and monitor health problems and trends
- Choose, prioritize, and target interventions to address health problems
- Mobilize necessary effort and resources to implement strategies
- Make sure that responses are implemented, vital conditions are in place, and crucial services are received to address health problems
- Determine outcomes and assess effectiveness
- Assess and improve strategies to address health problems and quality of services
- Assure and improve their own operations to provide for the public's health

SECTION 4: DISCLOSURE BY PUBLIC HEALTH AGENCIES

Under HIPAA, a public health agency can fall into one of three categories:

(1) a covered entity, subject to the HIPAA Privacy Rule; *or*

(2) a noncovered entity, not subject to the rule; *or*

(3) a hybrid entity, with at least a portion of the agency not subject to the rule.

Many public health departments are structured as hybrid entities. To be a hybrid, a public health agency identifies the portions of its agency that function as a healthcare provider, a health plan, or a healthcare clearinghouse. These portions are considered covered by HIPAA, while other portions (such as public health activities not involving patient care) are not covered. HIPAA sets out a process that a public health agency must follow to become a hybrid.[43]

Q: If a public health agency is a noncovered entity under HIPAA, or the public health function is considered noncovered as part of a hybrid agency, then how may public health agencies share PHI that has been provided by healthcare organizations?

A: In this case, HIPAA does not apply to the disclosure of PHI. A public health agency would still need to meet its legal and ethical responsibilities for its entire agency as a steward of personal health information, and any use agreements under which the data was obtained.

Q: Alternatively, If the public health agency is covered by HIPAA, what restrictions for sharing of PHI provided by healthcare organizations apply?

A: In this case, the entire agency would be subject to the HIPAA Privacy Rule, including its operational requirements, restrictions on data use and disclosure, and penalties for noncompliance. A full discussion of these requirements is beyond the scope of this document. Some of these requirements include:

- The agency is prohibited from using or disclosing PHI unless required or allowed by the HIPAA Privacy Rule.[44]
- Under the public health provision, a covered public health agency may use and disclose PHI to other public health agencies and to its and their authorized agents for public health purposes.[45]
- The minimum necessary standard applies to disclosures of data.[46]
- When disclosing PHI to its own agents, a public health agency might need to treat these agents as its business associates, and follow HIPAA's business associate requirements, including the requirement that a covered entity enter into a business associate agreement with its business associates.[47]
- As a covered entity, the public health agency would need

[43] 45 CFR 164.103, 164.105.

[44] 45 CFR 164.502.

[45] 45 CFR 164.512(b).

[46] 45 CFR 164.502, 164.514.

[47] 45 CFR 164.502, 164.504.

to be able to provide an accounting of its disclosures of PHI concerning an individual upon his or her request.[48]

Q: Where public health agencies are able to share health information, what are some best practices related to privacy?

A: Public health agencies may join with other organizations to form initiatives or coalitions to achieve a public health objective, for example, by targeting interventions and resources to specific populations or geographic areas. In fact, standards for national voluntary accreditation of state, local, tribal, and territorial health departments envision health departments that lead collaborative efforts to assess and address public health issues facing the community.[49] These may include cross-sectoral environmental, policy, and systems-level efforts that directly affect the social determinants of health and advance health equity.[50]

Best practices include:

- Identifiable data shared should be the minimum necessary for the intended purpose. If de-identified data can be used to meet the intended purpose, it should be used. All organizations that share PHI to achieve a public health objective should sign a data sharing agreement that governs the disclosures, uses, and protection of data.
- In general, unless there is a specific emergency, it is not ethical to release individually identifiable health information publicly without consent.
- It is considered appropriate to release data in aggregate in a manner that prevents re-identification.
- There should be a clear articulation of the legal basis for data sharing. For example, if data sharing relies on the public health provision in HIPAA, a written document should clearly identify the public health goal, identify the types of data to be analyzed in support of the goal, and the role of the collaborating organization(s) in achieving the goal. To use the public health provision, the terms should be clear that public health is leading the project and the other organizations are participating agents that are supporting public health to achieve its objectives. The legal basis should also reference other applicable federal, state, and local law.
- Public health agencies should have sufficient security, policies, training, and other practices that allow the agency to comply with relevant regulations, ethical standards, and agreements.

SECTION 5: GEOCODING

Q: What is geocoding?

A: Geocoding is the use of personal identifiers to link data to a specific location by translating an address into a set of XY coordinates that can be used to plot a location on a map.[51] For geospatial information, personal identifiers include a person's street address and ZIP code. GIS coordinates are considered an "equivalent geocode," meaning that they are as good as a street address. This can be especially useful for surveillance and tracking based on environmental factors.

Q: How does HIPAA treat geocoded health information?

A: Pinpointing a location on a map (particularly useful in mapping cases to identify clusters) could enable the determination of an individual's identity. This means public health agencies should consider health data with a geocode to be PHI, subject to the standards discussed above.

Q: What is best practice for releasing data that includes geocodes?

A: Geographic masking is a scientific method that may be used to preserve the privacy of PHI. The specific geographic masking method to be used would be based on the purpose for geocoding and the tolerable risk for re-identification.[52] Utilizing an expert in geographic masking would be necessary,

[48] 45 CFR 164.528.

[49] Public Health Accreditation Board (PHAB), Standards & Measures for Domain 1: Conduct and Disseminate Assessments Focused on Population Health Status and Public Health Issues Facing the Community, and Domain 4: Engage with the community to identify and address health problems. Accessed July 31, 2017 at http://www.phaboard.org/wp-content/uploads/SM-Version-1.5-Board-adopted-FINAL-01-24-2014.docx.pdf.

[50] HHS, Office of the Assistant Secretary for Health, *Public Health 3.0: A Call to Action to Create a 21st Century Public Health Infrastructure.* Accessed July 31, 2017 at https://www.healthypeople.gov/sites/default/files/Public-Health-3.0-White-Paper.pdf

[51] Zand M. Geospatial data and HIPAA. Bigdatamedsci.com 18 February 2014. Accessed July 31, 2017 at http://bigdatamedsci.com/2014/02/18/geospatial-data-and-hipaa/.

[52] Armstrong MP, Rushton G, and Zimmerman DL. Geographically masking health data to preserve confidentiality. *Statistics in Medicine* 1999;18: 497-525.

but it would likely allow for the release of more robust geocoded data outside of the public health agency.

SECTION 6: PUBLIC RECORDS LAWS AND PROTECTED HEALTH INFORMATION

Q: What are public records laws?

A: Federal and state public records laws set requirements for the disclosure of public records by public bodies. This can include all federal or state agencies, county and other local governments, school boards, other boards, departments, commissions, councils, and public colleges and universities. Public records laws are aimed at disclosing information regarding the affairs of government and the official acts of those who represent them as public officials and public employees, so residents may be informed and can fully participate in the democratic process.

Q: What is covered by a public records law?

A: In general, public records laws apply to all governmental records absent a specific exemption. These laws usually contain exemptions for personal medical information or records that would constitute a clearly unwarranted invasion of an individual's privacy, but this may vary by jurisdiction.

Q: Why should public health agencies be concerned with public records laws?

A: Before collecting PHI, a public health agency should be familiar with its ability to protect confidential data from disclosure through a public records request. In most cases, the ability to protect such data is found in a provision of the public records law itself. If the public health agency is not covered by HIPAA, then HIPAA would provide no protection of data from disclosure.

If a public health agency is a covered entity, HIPAA permits disclosure of PHI when "required by law." If a public records law only permits, but does not mandate, the disclosure of PHI, or exempts PHI from the law's disclosure requirement, such disclosures are not "required by law." In these cases, a covered entity only would be able to make the disclosure if permitted by another provision of the Privacy Rule.[53]

SECTION 7: PUBLIC HEALTH PRACTICE VS. RESEARCH

Q: What is considered research under HIPAA?

A: The definition of research in the HIPAA Privacy Rule is the "systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[54] Research is designed to generate generalizable knowledge that benefits those beyond the study participants who bear the risks of participation.[55] Public health practice is not research.

Q: How do you distinguish between public health practice and research?

A: The key difference is that public health activities are not meant to contribute to generalizable knowledge, but rather, they are aimed at protecting the health of the population. The primary intent of an activity is the most important factor in distinguishing between public health practice and research. The intent of public health practice is "to identify and control a health problem or improve a public health program or service."[56] This means that internal quality improvement, program evaluation and assessment are part of public health practice. There are other specific characteristics that can help distinguish public health practice from research. These include:

(1) Legal authorization for the activity at the federal, state, or local level;

(2) A governmental duty to perform the activity;

(3) Performance or oversight of the activity by a governmental public health authority with public accountability;

(4) Legitimate authority for non-voluntary participation in the activity; and

(5) Activity is supported by principles of public health ethics that focus on populations while respecting the dignity and rights of individuals.[57]

[53] 45 CFR 164.512(a).

[54] 45 CFR 164.501.

[55] MacQueen KM. Public health research … or is it practice? 23 September 2005. Accessed July 31, 2017 at https://www.niehs.nih.gov/research/resources/assets/docs/public_health_research_or_is_it_practice_508.pdf.

[56] Centers for Disease Control and Prevention. Distinguishing public health research and public health nonresearch. Policy No. CDC-SA-2010-02. 29 July 2010: 2. Accessed July 31, 2017 at https://www.cdc.gov/od/science/integrity/docs/cdc-policy-distinguishing-public-health-research-nonresearch.pdf.

[57] Hodge JG, Gostin LO. Public health practice vs. research: A report for public health practitioners including cases and guidance for making distinctions. 24 May 2004. Accessed July 31, 2017 at http://www.cste2.org/webpdfs/cstephres-rpthodgefinal.5.24.04.pdf.

Q: When is a public health activity also considered research?

A: If the secondary aim of a public health activity is to produce and disseminate generalizable knowledge then that activity would be deemed public health research. Any research involving human subjects must comply with human subjects' protections and other research related laws, including HIPAA.[58]

Q: Is interest in publishing the results of an activity enough to turn a project into research under HIPAA?

A: No, interest in publication alone is not dispositive in distinguishing public health practice from research. The primary purpose of the activity determines whether the activity is public health practice or research, as described above.

[58] 45 CFR 164.512(i).

Recommendations for Interested Public Health Agencies

The use cases and HIPAA analysis above demonstrate the broad potential for public health agencies to address important challenges through access to electronic healthcare data. Public health agencies interested in exploring opportunities to move forward might consider taking several steps.

(1) Define key public health issues and goals with broad community support.

Public health agencies can start by defining critical issues and building consensus around the need to address them. A discussion on data sharing can then be set in the context of public interest in addressing childhood asthma, the opioid epidemic, or other important challenges. (It is rarely persuasive to ask anyone to share data for the sake of sharing data.)

(2) Develop a data request with a clear explanation, plan for privacy protection, and plan for data use.

As the use cases demonstrate, the specificity of a request makes it possible for others to consider the value and cost of participation. It may be helpful to engage with key sources of data as the request is developed to be sure that what is requested is feasible.

(3) Obtain legal review to assure key participants of compliance with HIPAA and other applicable state and local laws.

A legal review can provide assurance that plans are compatible with key standards in HIPAA and other applicable state laws. It is hoped that this paper can serve as a starting point for this review.

(4) Provide for public engagement on the purposes, use, and protection of data.

Public engagement provides an important measure of transparency about plans for data sharing and public health action. Public health agencies can create and implement an engagement strategy that strengthens support for actions to improve health outcomes.

Authors

Joshua M. Sharfstein, M.D., is associate dean for Public Health Practice and Training at the Johns Hopkins Bloomberg School of Public Health. Dr. Sharfstein is the former health commissioner of Baltimore, Principal Deputy Commissioner of the U.S. Food and Drug Administration, and Secretary of Maryland's Department of Health and Mental Hygiene. He is an elected member of the National Academy of Medicine and the National Academy of Public Administration. Dr. Sharfstein also serves as an adviser for Audacious Inquiry, a Maryland-based health information technology company.

Denise Chrysler, J.D., serves as director for the Mid-States Region of the Network for Public Health Law at the University of Michigan School of Public Health. Previously, she served as the public health legal director for the Michigan Department of Community Health (MDCH). In this position, she coordinated the legal needs of the Public Health Administration and provided legal expertise and assistance regarding public health powers, programs, and services. She also served as the Michigan Department of Community Health's chief privacy officer, its Freedom of Information Act coordinator, and on its Institutional Review Board.

Jennifer Bernstein, J.D., M.P.H., serves as deputy director for the Mid-States Region of the Network for Public Health Law at the University of Michigan School of Public Health. She works extensively on health information and data sharing issues, serving as a partner representative of the Joint Public Health Informatics Taskforce and as a Learning Health Community Governance committee member. Previously, she was a Hogg Foundation Mental Health Policy Fellow at the University of Texas at Austin, advocating for the expansion of trauma informed care for foster children throughout the state of Texas.

Luciana Armijos is a recent M.P.H. graduate of the Johns Hopkins Bloomberg School of Public Health.

Laura Tolosa-Leiva is a student in the MSPH program in Health Policy and Management at the Johns Hopkins Bloomberg School of Public Health.

Holly Taylor, PhD, M.P.H., is an associate professor of Health Policy and Management at the Johns Hopkins Bloomberg School of Public Health and is core faculty of the Johns Hopkins Berman Institute of Bioethics.

Lainie Rutkow, J.D., Ph.D., M.P.H., is an associate professor of Health Policy and Management at the Johns Hopkins Bloomberg School of Public Health. She is the assistant director of the Johns Hopkins Center for Law and the Public's Health, and is core faculty of the Johns Hopkins Center for Mental Health and Addiction Policy Research, the Johns Hopkins Center for Injury Research and Policy, and the

Suggested citation: Sharfstein, J.M., Chrysler, D., Bernstein, J., Armijos, L., Tolosa-Leiva, L., Taylor, H., and Rutkow, L. (2017, December). *Using Electronic Health Data for Community Health: Example Cases and Legal Analysis*. Retrieved from http://www.debeaumont.org/EHDforCommunityHealth