Legal Issues Concerning Identifiable Health Data Sharing Between State/ Local Public Health Authorities and Tribal Epidemiology Centers in Selected U.S. Jurisdictions

A report for the
Council of State and Territorial
Epidemiologists (CSTE)

James G. Hodge, Jr., JD, LL M
Professor, Johns Hopkins Bloomberg School of Public Health
Executive Director, Centers for Law and the Public's Health

Torrey Kaufman, JD, MPH
Georgetown and Johns Hopkins Universities
Researcher, Centers for Law and the Public's Health

Craig Jaques, BA
Research Assistant, Centers for Law and the Public's Health

Original Draft as of March 30, 2009;
Revised by CSTE (with author overview) as of November 8, 2011

Table of Contents

Acknowledgement[1]

The authors at the *Center for Law and the Public's Health: A Collaborative at Johns Hopkins and Georgetown Universities* acknowledge **Evan D. Anderson**, J.D., *Center* Senior Fellow, and **P.J. Wakefield**, *Center* Administrator, for their research, editing, formatting, and other contributions to this report.

The authors would also like to acknowledge the CSTE Tribal Epidemiology Workgroup for its contributions in reviewing and revising this document, specifically Edward Chao, Jessica Craig, John Mosley Hayes, Michael Landen, Jennifer Lemmings, Zeenat Mahal, and Annie Tran.

While the lead author (James G. Hodge, Jr.) has reviewed edits to this report made by CSTE following its original version on March 30, 2009, the authors have not conducted additional legal research to verify specific edits made by CSTE, particularly related to Tables 1 and 2.

This publication was supported by Cooperative Agreement Number 5U38HM000414-04. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of CDC.

Table of Abbreviations

Abbrev.	Term or Title
AI/AN	American Indian/Alaska Native
AIDS	Acquired immunodeficiency syndrome
CDC	Centers for Disease Control and Prevention
CSTE	Council of State and Territorial Epidemiologists
DHHS	Department of Health and Human Services
FERPA	Family Education Rights and Privacy Act
FOIA	Freedom of Information Act
HIPAA	Health Insurance Portability and Accountability Act
IHCIA	Indian Health Care Improvement Act
HIV	Human immunodeficiency virus
IHS	Indian Health Service
IRB	Institutional Review Board
MSPHPA	Model State Public Health Privacy Act
MVSRA	Model Vital Statistics and Regulations Act
OSHA	Occupational Safety and Health Administration
PHI	Protected Health Information
TEC	Tribal Epidemiology Center

I. Introduction

Identifiable health data are the lifeblood of public health surveillance and other activities. Their use is essential to effective public health activities and public health research. Public health authorities at all levels of government seek increasingly greater types and volume of personally identifiable health information, including through data exchanges between public health entities. Too often, however, acquisition and use of identifiable health information through existing public health databases are restricted or limited by privacy norms or other policies. Public health authorities might be reticent to share identifiable health data, even for legitimate public health purposes, because of concerns about individual privacy or legal interpretations of privacy laws. As a result, public health entities can lack access to health data to conduct essential services and research.

Although the veracity of this observation extends to multiple data-sharing practices, tribal public health authorities such as Tribal Epidemiology Centers (TECs) nationally have reported extensive limitations concerning data sharing with state or local public health authorities. Funded by the U.S. Indian Health Service (IHS), the nation's 12 TECs work in partnership with tribal governments or tribal government coalitions. Each TEC is designated to serve the American Indian/Alaska Native (AI/AN) population within one of the 12 IHS administrative areas, although one TEC serves two IHS areas and another TEC serves urban AI/AN populations throughout the nation. TECs rely on the sharing of existing public health data accumulated by federal, state, or local governments to conduct a variety of epidemiologic activities to improve tribal health. In March 2010, the Indian Health Care Improvement Act (IHCIA) was permanently reauthorized and required that TECs be treated as public health authorities for purposes of the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

At a meeting in Albuquerque in May 2008, the CSTE Tribal Epidemiology Subcommittee identified a series of action items and recommendations to improve public health surveillance in Indian Country. Among these recommendations is the need to better understand and encourage data sharing between TECs and state health departments. On the basis of reports from the field discussed during this meeting, TEC authorities consistently face hindrances in gaining access to state/local public health data. These barriers to data sharing predominately originate from privacy-related concerns among state/local authorities in releasing identifiable heath data to tribal entities.

In November 2008, CSTE asked the *Centers for Law and the Public's Health: A Collaborative at Johns Hopkins and Georgetown Universities* to research and assess state laws in a geographically representative sample of states with federally recognized tribes, specifically Arizona, Florida, Maine, Nevada, Oklahoma, South Dakota, and Washington, concerning the following legal question:

> ***What state-specific laws (e.g., statutes, regulations, cases) authorize or limit the sharing of identifiable public health data between state public health authorities and TECs for lawful public health activities conducted by TECs?***

This report attempts to answer this question through legal research and analysis based on a review of laws in the seven selected states. For the purposes of this report, every state and tribal government is assumed to have some general public health legal authority to acquire and use identifiable health data for public health purposes, as well as to address general threats to the public's health. This broad public health authority may allow government to respond to

public health threats, including through the sharing of identifiable data with tribal and other public health authorities.

Generally accepted legal methods of statutory and legal interpretation were used to comprehensively examine the laws of the designated seven states. The scope of laws and other legal authorities include state statutes, administrative regulations, and judicial cases. Laws identified in this report were found through legal research search engines (e.g., LexisNexis, Westlaw), publicly available websites featuring state and local legal compilations, and websites of state and local health departments and other government departments. Basic search engines (e.g., Google, Yahoo) were also used to (1) help corroborate information obtained through more specialized research search engines (e.g., LexisNexis, Westlaw) and (2) obtain the hyperlinks included in the tables.

Laws in each of the seven states were categorized on the basis of major relevant legal categories (Tables 1 and 2). These categories include state laws that

- Authorize the sharing of identifiable health data for public health surveillance, research, or other purposes;
- Specifically authorize the sharing of identifiable health data with tribal authorities;
- Limit the sharing of identifiable health data for privacy-related reasons;
- Provide exceptions to data-sharing limitations for privacy-related reasons;
- Authorize or limit the sharing of identifiable disease- or condition-specific data; and
- Are otherwise relevant to data sharing among state/local public health authorities and tribal authorities.

Although comprehensive research underlying this report is subject to limitations, the findings solely represent analyses and interpretations (and not those of legal counsel representing each jurisdiction). Input was not received from Washington state. Although a variety of electronic and other search approaches were used to identify relevant laws in each jurisdiction, some provisions might not have been found. For example, this research might not include some reported judicial cases, proposed legislation or regulations, agency opinions, compacts, or memoranda of agreement that might be relevant to addressing the specific research question. Finally, this assessment of the legal environment concerning data exchanges with TECs is based solely on the findings from the seven selected jurisdictions. The laws and statutes referenced in this report illustrate the precedence of data-sharing agreements but are not intended to provide a complete or exhaustive listing of all relevant statutes in the states. Other jurisdictions' laws may provide alternative approaches.

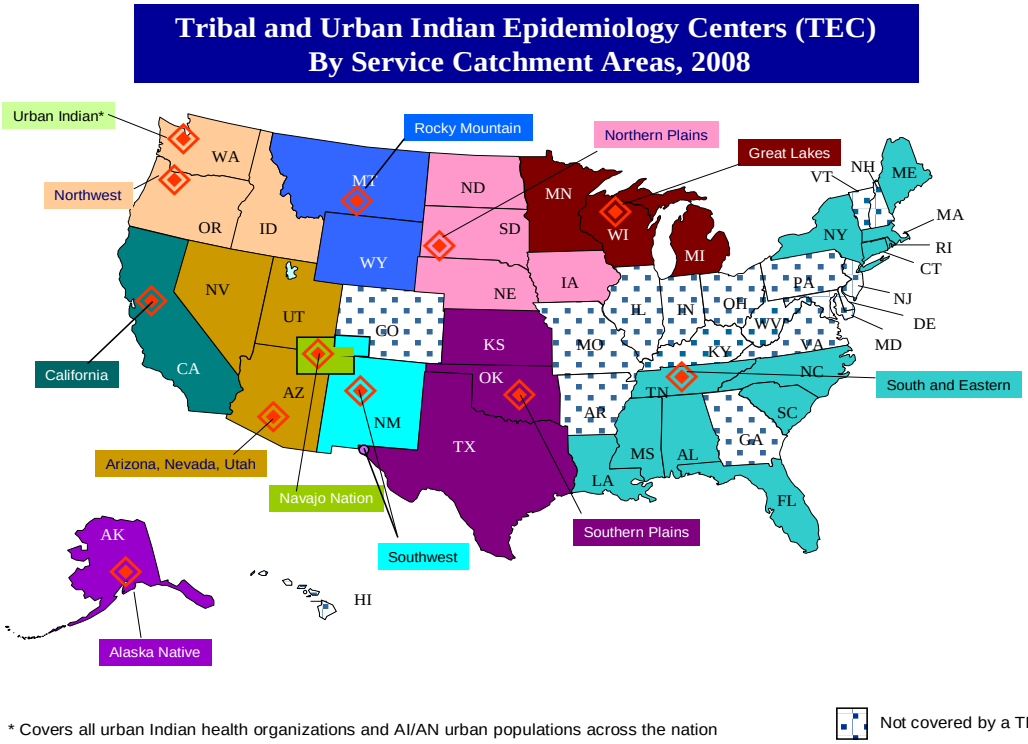
The objective throughout the report is to provide a foundation for examining potential privacy issues and solutions to further educate current and potential TECs' partners about privacy implications of state laws in selected jurisdictions, as well as to facilitate public health data sharing. **Part II** briefly explains TECs and the specific types of health data that they seek to collect and analyze for their epidemiologic activities. **Part III** discusses legal privacy norms through an overview of the differing legal concepts of privacy, confidentiality, and security. **Part IV** summarizes selected health information privacy laws and policies relevant to TECs. Various approaches taken by the selected states about their privacy laws and policies are also discussed. **Part V** provides potential legal and policy privacy issues and solutions related to future data-sharing practices between state health departments and TECs.

II. Tribal Epidemiology Centers—Brief Overview

TECs were established through the reauthorization of the IHCIA in 1996 amid growing concern about the lack of a public health surveillance system for disease control for AI/AN populations. The AI/AN populations include members from more than 582 federally recognized sovereign tribal governments in the United States. Funded through cooperative agreements with the federal IHS, TECs play a critical role in building public health capacity among AI/AN regions and communities. Working with tribal entities and urban AI/AN communities, TECs provide data dissemination services, surveillance databases, epidemiologic studies, training, responses to public health emergencies, technical assistance, and disease control and prevention services.[2] The role of TECs was strengthened in March 2010 when the IHCIA was permanently reauthorized, thus requiring TECs to be defined and treated as "public health authorities" for purposes of the HIPAA Privacy Rule. The permanent reauthorization of IHCIA directs the Secretary of the Department of Health and Human Services (DHHS) to grant each TEC access to use of the data, data sets, monitoring systems, delivery systems, and other protected health information (PHI) in the possession of the Secretary. It also requires the Director of the Centers for Disease Control and Prevention (CDC) to ensure CDC assets provide technical assistance and work closely with each TEC in strengthening AI/AN disease surveillance.

Each of the 12 TECs in the United States is designated to serve AI/AN populations within one of the 12 IHS administrative areas (Figure 1, below), with the exception that one TEC serves two IHS areas and one serves urban AI/ANs across the nation.

Figure 1. Tribal and Urban Epidemiology Centers, United States



TECs maintain a strong core of data collection, dissemination, surveillance, and epidemiologic studies. Through these efforts, each TEC is uniquely positioned to evaluate tribal and

community-specific health status, enhancing the ability of IHS to better understand and further develop the link between public health problems and behavior, socioeconomic conditions, and geography.[3] Data used by TECs are not exclusively collected through their regional work. A culmination of tribal, state, and national data sets are used to expand on the relatively small census populations encountered by TECs.[3] This combination of data allows for a comprehensive and complete picture of the status of health and behavioral characteristics of AI/AN populations.

Identifiable data that TECs request from state and municipal health departments for health status reports are largely uniform and can be broken down into five categories:

- Vital statistics,
- Notifiable condition reports,
- Hospital discharge records,
- Emergency department records, and
- Immunization and disease-specific registries.

Federal, state, and municipal health department information that TECs collect, disseminate, and study provides a unique lens to the status of AI/AN populations throughout the United States. However, improved transparency and reciprocity between tribal, state, and national data sets would allow for more comprehensive studies at each level and, ultimately, greater understanding of the population's health and improved programs to ensure these disparities are properly addressed.

III. Health Information Privacy, Confidentiality, and Security

Protecting the privacy, confidentiality, and security of identifiable health data acquired, used, or stored for public health or research activities is central to responsible data-sharing practices. Privacy concerns underlying public health data collections arise from the potential for unauthorized access, unwarranted uses or disclosures of identifiable data, and resulting discrimination against individuals or groups by government, employers, insurers, or others. Documented cases of health information privacy invasions publicized through media or other sources heighten individual fears about privacy invasions. In response, data holders might question the need to share identifiable health data for public health or other purposes. For these and other reasons, protecting data privacy and security is essential to managing modern public health data.

A. Privacy, Confidentiality, and Security

Although often used interchangeably, the terms *privacy*, *confidentiality*, and *security* have distinct legal and ethical meanings related to identifiable health information.[3] Health information *privacy* broadly refers to individuals' rights to control the acquisition, uses, or disclosures of their identifiable health data. Information privacy rights originate from ethical principles of autonomy that imply that individuals are entitled to some level of control over health data that are unique and personal to them.

Groups of individuals may also share expectations of privacy in health data related to their group characteristics but traditionally lack formal legal protections of their privacy interests.[4] For example, an American Indian population might be concerned about potential findings of a major research study suggesting they are at greater risk than the general population of developing a

specific cancer because of a genetic predisposition. Their privacy interests in these data relate to how the data are disclosed and how insurers, employers, or others may subsequently use the data to raise premiums, limit benefits, or deny opportunities. However, health information privacy laws largely do not address group privacy concerns as long as the data disclosed do not identify specific individuals.

Closely related to individual privacy interests is the concept of *confidentiality.* Confidentiality refers to the obligations of individuals or groups who receive or use information to respect the privacy interests of individuals who are the subjects of the data. In a legal sense, duties of confidentiality arise from specific relationships (e.g., doctor and patient, researcher and subject, public health practitioner and member of the public). From an ethical perspective, health information privacy rights (grounded in individual autonomy) include a corresponding duty of confidentiality to which others must adhere. These ethical norms are reflected in professional codes of ethics for doctors, nurses, and public health workers.

Security differs altogether from privacy or confidentiality. Data security refers to technologic or administrative safeguards or tools designed to protect identifiable health data from unwarranted access or disclosure. Maintaining information security has become more challenging in the modern era of digitized exchanges and large electronic databases of identifiable health records that can be hacked or infiltrated through unlawful invasions. Identifiable data have been subject to security breaches at all levels of government[5] and within private institutions. According to the Privacy Rights Clearinghouse, a nonprofit institution that compiles incidents in which personal information is lost or compromised, in 2010 alone, 604 incidents are known to have occurred in the United States in which the security of more than 12.3 million identifiable records were compromised.[6]

A number of incidents in recent years have involved compromised identifiable public health data or data held by public health authorities. For example, in May 2007, the Georgia Department of Human Resources notified parents of infants born during an 11-month period that paper records containing 140,000 parents' Social Security numbers and medical histories were improperly discarded without shredding.[7] In December 2007, a medical provider in Colorado mistakenly allowed medical records of thousands of Colorado residents (including detailed, identifiable information about emergency department visits, diagnoses, treatments, and medical histories) to be publicly accessible online for an unknown period.[8] In May 2008, a security breach at the Department of Pathology at the University of San Francisco potentially exposed information of 2,625 patients.[9] These and other published accounts, and resulting litigation nationally based on security breaches,[10] offer compelling justification to ensure data security to avoid unwarranted privacy infringements.

Although seemingly vulnerable, electronic health systems can be designed to better protect individual privacy and security than traditional paper-sharing practices through sophisticated technologic features that greatly limit access, and protect against internal and external intrusions.[11] Issues of security are paramount to protecting data privacy and confidentiality; however, legal implications related to security protections are beyond the scope of this report.

B. Identifiable versus Nonidentifiable Health Data

Not all health data are entitled to legal privacy protections. Modern health data privacy norms distinguish between individually identifiable and nonidentifiable (e.g., aggregate) data. Only identifiable health information is covered by privacy laws and policies. Identifiable health information is generally defined as any information related to past, present, or future health

conditions or status that may identify the person to whom the data relate. Identifiable health data contain specific information (e.g., names, addresses, and Social Security numbers) that directly identifies an individual or could be used to identify the individual.

Nonidentifiable health information does not (or cannot when coupled with other accessible information) identify the individuals to whom it pertains. Nonidentifiable health information includes de-identified data or data that (pursuant to the HIPAA Privacy Rule, discussed below): (1) have been stripped of unique identifiers or (2) have been certified by a qualified statistician as being incapable in their present form of identifying an individual.[12]

Data sharing involving nonidentifiable health information raises minimal, if any, privacy implications. Consequently, modern health information privacy laws do not restrict access, use, or disclosure of nonidentifiable data,[13] thus providing an incentive for data holders to de-identify health information to diminish the risk for harmful disclosures and uses of personal data.[14] However, viable uses of nonidentifiable health data can be minimal because specific information needed to track public health conditions or conduct human subjects research is removed.

C. Balancing Individual and Communal Interests

Although important, protecting individual privacy is not an absolute. Virtually all health information privacy laws are framed around the need to balance individual privacy expectations with communal needs for health data, including protecting the public's health or performing human subjects research. Balancing individual and communal interests in the acquisition, use, and disclosure of identifiable health information is a key feature of modern legal protections. Health information privacy laws generally prohibit data holders from acquiring, using, or disclosing identifiable health information unless the individual has provided informed consent or written authorization. This general prohibition is contingent on a series of exceptions that reflect the balance of individual and communal needs. Thus, health information privacy laws typically exempt from the general prohibition a range of acquisitions, uses, or disclosures that can be made without individual informed consent or authorization. As discussed below, these exceptions often include public health or human subjects research activities.

Such legal balancing can appear to be highly deferential to the needs for data of public health authorities (sometimes allowing public health authorities to exchange health data for virtually any public health purpose). However, in many instances, it can also increase the burden on public health authorities to demonstrate their need for identifiable health information for public health purposes. Data holders (such as hospitals, insurers, physicians, clinics, and even public health authorities) may be reluctant to share this information without individual authorization because the cardinal rule of privacy laws is not to share such data without authorization. Although these same laws often simultaneously allow public health authorities to receive identifiable data without individual authorization, data holders may still resist sharing data. In some cases, they deny public health authorities access to these data unless the authorities can demonstrate their legal right to acquire the data.[15] Even though these challenges may lack substantive legal support, the reality of modern privacy protections is that the balance has shifted toward protecting patients' privacy and away from promoting the public's health.

D. Distinguishing Public Health Practice and Human Subjects Research

A core premise of privacy laws is that disclosures or uses of health information for public health or research purposes should be made under clearly defined standards. This presumes that disclosures for public health practice are neatly distinguishable from disclosures for other

purposes, such as human subjects research. Yet, considerable uncertainty exists about how to distinguish research and nonresearch activities. The federal Common Rule[16] and HIPAA Privacy Rule systematically require public health authorities to distinguish human subjects research activities from clinical care and public health practice. Neither regulation, however, provides clear guidance on how to distinguish these activities. Public health activities (such as the types of surveillance, epidemiologic investigation, and program evaluation conducted by TECs) can be confused with human subjects research because both activities can involve the systematic acquisition and use of identifiable health data for health-related purposes. As a result, researchers, public health practitioners, institutional review board (IRB) members, and others may struggle to classify these activities under the applicable rules, potentially resulting in confusion, inconsistency, and breaches of confidentiality.

In 2003, CSTE assembled an expert committee to examine these issues and improve guidance on the distinctions between human subjects research and public health practice activities. The resulting document, *Public Health Practice vs. Research: A Report for Public Health Practitioners Including Case Studies and Guidance*,[17] proposed a two-stage framework for classifying these activities, as illustrated in the accompanying Checklist. Essential characteristics of public health practice (defined as the collection and analysis of identifiable health data by a public health authority for the purpose of protecting the health of a particular community, where the benefits and risks are primarily designed to accrue to the participating community) include

- Specific legal authorization for conducting the activity as public health practice at the federal, state, or local level;
- A government obligation to perform the activity to protect the public's health;
- Direct performance or oversight by a government public health authority (or its authorized partner) and accountability to the public for its performance;
- Involvement of people who did not specifically volunteer to participate (i.e., they did not provide informed consent); and
- Adherence to principles of public health ethics that focus on populations while respecting the dignity and rights of individuals.

Essential characteristics of human subjects research (defined as the collection and analysis of identifiable health data for the purpose of generating knowledge that will benefit those beyond the participating community who bear the risks of participation) include the following:

- The subjects of the research are living;
- Identifiable private health information is gathered and produced;
- Research subjects participate voluntarily or participate with the consent of a guardian, absent a waiver of informed consent; and
- The researchers adhere to principles of bioethics that focus on the interests of individuals while balancing the communal value of research.

These characteristics help distinguish public health practice from research in many cases. For example, a public health reporting requirement may be specifically authorized by tribal or state law. In such cases, corresponding data-gathering activities are classifiable as public health practice as long as their design and implementation do not cross over into research.

A second stage of the analysis provides enhanced principles of guidance to draw distinctions in more difficult cases. These principles include

- *General legal authority*. Public health authorities may conduct activities pursuant to general legal authorization (e.g., the state department of health is authorized to "control communicable and chronic diseases") that may justify classifying an activity as public health practice subject to additional analysis.
- *Specific intent.* The intent of human subjects research is to test a hypothesis and generalize findings or acquired knowledge beyond the activity's participants. Conversely, the intent underlying public health practice is to ensure the conditions in which people can be healthy through public health efforts primarily aimed at preventing known or suspected injuries and diseases, or promoting the health of a particular community.
- *Responsibility.* Responsibility for the health, safety, and welfare of human participants in research falls on a specific person, typically the principal investigator. Public health practice, however, does not always vest responsibility for participants' welfare in individuals but rather in government agencies or authorized partner entities.
- *Participant benefits.* Public health practice should contribute to improving the health of participants and populations. In contrast, research might, but does not necessarily, provide benefits to participants;
- *Experimentation.* Research can involve the application of something nonstandard or experimental to human subjects or their identifiable health data. Public health practice is dominated by the use of standard, accepted, and proven interventions to address known or suspected public health problems.
- *Subject selection.* To reduce the possibility of bias in their studies and to generalize their results, researchers may select human subjects randomly. Participants in public health practice activities are self-selected persons with, or at risk for, a specific disease or condition who can benefit from the activity.

Although no method can completely distinguish between human subjects research, public health practice, or other related activities in every case, these principles can help resolve most cases, provide consistency in decision-making on a national basis, and help apply privacy protections in public health and research settings.[18]

IV. Privacy Laws and Policies Concerning the Acquisition, Use, and Disclosure of Identifiable Health Data

Despite systematic legal reforms concerning health information privacy in the United States, no uniform approach exists to regulating privacy concerning identifiable health data.[19] Rather, through what is often described as a patchwork of existing privacy laws, the privacy of health data is legally regulated on the basis of multiple factors, including

- The type of health data that are acquired, used, or disclosed (e.g., medical information generally, disease-specific data, such as data related to cancer, genetics, human immunodeficiency virus (HIV) infection/acquired immunodeficiency syndrome (AIDS), birth defects);
- The entity acquiring, using, or disclosing the data (e.g*.,* federal, tribal, state, or local governments, private sector hospitals or clinicians, insurance companies, employers); and
- The setting in which the data are collected or used (e.g*.,* public health, research, law enforcement, national security).

Some of the major sources of federal and state privacy laws that might impact data-sharing practices of TECs are summarized below, including constitutional protections, major federal privacy laws, and state privacy laws.

A. Constitutional Health Information Privacy Protections

Constitutional principles are at the source of public health powers and privacy expectations. However, the federal Constitution neither guarantees the provision of public health services[20] nor provides strong protections of informational privacy.[21] Consequently, federal, tribal, state, and local governments are constitutionally able to regulate, protect, and promote the public's health, restricted only by minimal information privacy requirements. The U.S. Supreme Court largely defers to the government's judgment as to how best to protect private health information.[22] Other courts rely on state constitutional provisions in support of privacy rights. In general, courts regularly examine privacy issues through the administration of a flexibility test that balances the invasion of privacy against the strength of the government interest.[23] Provided government articulates a valid societal purpose and employs reasonable security measures, courts typically do not interfere with traditional government health information collections on constitutional grounds, except where government fails to assert any significant interest in acquiring identifiable data or is careless in maintaining or disclosing highly sensitive information.[24]

B. Federal Health Information Privacy Protections

For decades, federal privacy laws have been enacted or created to apply to certain types of health information collected, maintained, or funded by (or on behalf of) the federal government through specific agencies (e.g., Centers for Medicare and Medicaid Services, CDC, National Institutes of Health [NIH], IHS) for specific purposes (e.g., Medicare, public health programs, human subjects research). As described briefly below, these laws protect the privacy of individually identifiable health information in various ways.

Early federal privacy laws helped to set basic parameters for protection of all identifiable data, including health information, acquired or held by the federal government. For example, the Freedom of Information Act of 1966 (FOIA)[25] opened federal government records to public review but PHI privacy by exempting public requests for identifiable health information held by federal agencies pursuant to what is known as the FOIA (b)(6) exemption. This exemption covers information that, if released, would constitute an unwarranted invasion of personal privacy.

The federal Privacy Act of 1974[26] applies to any information collected and maintained by a federal agency in a system of records (e.g., Medicare records, health records held by the Department of Defense or Veterans Affairs) in which the information is retrieved by an individual's name, identification number, or other identifier. The Act protects individual privacy by (1) specifying situations in which information may be disclosed without the individual's consent (requiring consent in all other situations), (2) proscribing government maintenance of identifiable health information that is irrelevant or unnecessary to accomplish government purposes, (3) requiring federal agencies to publish a notice about each record system describing its purpose, and identifying disclosures outside the agency (e.g., "routine uses") that it has chosen administratively to make, (4) mandating that agencies inform requesting individuals of the statutory basis for collecting health information purposes for which it is used and consequences for not supplying the information, and (5) authorizing individuals to access their own government-held information and seek amendments to correct inaccuracies.

Modern federal privacy laws protect identifiable health information exclusively, highlighted by the HIPAA Privacy Rule. Developed by DHHS, the Privacy Rule became fully effective in April 2003 after years of legislative and regulatory efforts to create national health information privacy standards as required by Congress through HIPAA.

The Privacy Rule applies to what is known as "covered entities." Covered entities include *health plans* (e.g*.,* health insurance companies; managed-care entities; and specifically named government health programs, such as those managed by the Department of Veterans Affairs), *health-care clearinghouses* (e.g*.,* billing services, re-pricing companies, or community health information systems that process health data), and *health-care providers* (e.g*.,* doctors, hospitals, clinics) that transmit health information electronically. The Privacy Rule also applies to their "business associates" (e.g*.,* claims processors, billing managers, data analyzers, and others) of covered entities. Many others who acquire, use, disclose, or store identifiable health data, including federal, tribal, state, and local public health authorities, are beyond the scope of the Privacy Rule, provided they are not engaged in "covered functions." In other words, as long as tribal public health authorities are not engaged in activities akin to those performed by covered entities (e.g., providing health-care services), public health authorities do not comply with the Privacy Rule. Yet, as discussed below, the Privacy Rule still impacts public health authorities in many ways.

The Privacy Rule protects individually identifiable health information, (i.e., PHI), created or received in any form (e.g., electronic, paper-based) by covered entities. PHI includes identifiable health data that relate to the past, present, or future physical or mental health or condition of a person; the provision of health care to a person; or the past, present, or future payment for the provision of health care to a person.[27] As noted above, PHI does not include nonidentifiable health information or de-identified data.

Among its many requirements, the Privacy Rule specifically addresses how and under what circumstances covered entities may disclose PHI consistent with the balancing approach discussed above. In general, a covered entity may not disclose PHI without individual written authorization, subject to a series of exceptions. Included among these exceptions are disclosures without written authorization to (1) an entity for *health research purposes* (provided the entity obtains a waiver of informed consent from an IRB or privacy board in accordance with a series of considerations that are similar to the federal Common Rule considerations) and (2) *public health authorities* authorized by law to collect or receive such information for public health purposes.

Public health authorities include federal public health agencies (e.g., CDC, NIH, Food and Drug Administration, Occupational Safety and Health Administration, Environmental Protection Agency); tribal health agencies (e.g., IHS, tribal health organizations, and TECs); state public health agencies (e.g., public health departments or divisions, state cancer registries, vital statistics departments); or local public health agencies (e.g., county or city health departments, local boards of health). Subcomponents of large entities may be viewed as public health authorities even if the larger entity is only partially covered. For example, some state health departments encompass divisions that implement Medicaid services (which are clearly covered under the Privacy Rule) and public health or environmental divisions (which generally are not covered). Provided the state health department declares itself to be a "hybrid entity," the noncovered public health divisions do not have to comply with the Privacy Rule.

In addition, because public health authorities often carry out their activities with public or private partners through contracts, grants, and agreements, these partners may also be designated as public health authorities under the Privacy Rule. Thus, for example, if a local public health agency typically contracts with a private sector data handler or academic center to help acquire, use, or analyze identifiable health information, these private sector or academic entities are viewed as public health authorities just the same as the local government entity.

The Privacy Rule specifically permits covered entities to disclose PHI to public health authorities and their partners for public health purposes without individual written authorization (1) when specifically required by federal, tribal, state, or local laws (for example, laws authorizing the creation of TECs may mandate the disclosure of PHI to public health authorities for public health purposes) or (2) as generally allowed by law. Public health authorities may acquire PHI from a covered entity provided they are generally authorized by law to collect or receive information for public health purposes. Although undefined in the Privacy Rule, DHHS has broadly interpreted the scope of what is "authorized by law" as including any data collection by public health authorities for which a legal basis exists for the activity. Thus, tribal public health authorities do not have to rely on specific reporting laws to acquire and use PHI from covered entities. They can simply point to the existence of general reporting requirements as sufficient to authorize disclosures by the Privacy Rule.

Covered entities must limit the amount of data disclosed to the minimum necessary to achieve specified goals of the disclosure. However, the Privacy Rule clarifies that they can reasonably defer to public health authorities to determine the amount of information that is minimally necessary for the stated purpose.

Once PHI is disclosed to a public health authority, it may be maintained, used, and disclosed consistent with existing laws, regulations, and policies of the public health authority. Public health laws that require or authorize the disclosure of PHI for public health purposes[28] or govern the privacy and confidentiality of public health information are not affected by the Privacy Rule. Provided that state or local laws permit the sharing of such data by public health authorities across state boundaries or among agencies within the state, these disclosures may continue unabated by the Privacy Rule.[15]

Despite the legal mechanisms built into the Privacy Rule and designed to facilitate exchanges of PHI between covered entities and public health authorities, the balance between protecting privacy and promoting public health might still be compromised. Misinterpretations and misapplications of the Privacy Rule by covered entities can present barriers to public health data acquisitions. Seeking to adhere to the Rule, covered entities may mistakenly refuse to share PHI with public health authorities despite the Rule's allowance for the sharing of such information. Some covered entities use the Rule as a shield to reject requests for PHI from public health authorities, even if they have typically provided such data in the past before implementation of the Rule. Nationally, the impact of the Privacy Rule on public health and human subjects research data acquisitions has strained public health practice and research activities. Recently, a committee of the Institute of Medicine that studied these and other impacts released its report, including major recommendations for reforms of the Privacy Rule to alleviate privacy burdens.[29]

C. State Health Information Privacy Protections

Although many states have laws similar to the federal Privacy Act and FOIA, most do not have comprehensive statutes or regulations regulating the acquisition, use, and disclosure of

identifiable health data (such as the HIPAA Privacy Rule). Most state privacy laws tend to regulate specific data recipients (e.g., public health agencies, health insurers); specific medical tests, diseases, or conditions (e.g., genetic tests, HIV status, mental disorders); or particular data sources (e.g., nursing or health-care facilities, insurance companies). As discussed below, most relevant among existing state privacy laws are those that govern the acquisition, use, and disclosure of identifiable health data by state or local public health agencies, which may include the types of data collections sought by TECs.

State public health information privacy laws differ substantially in regard to the degree of privacy protections afforded.[30] Like most privacy laws, state laws balance privacy protections with the need to share identifiable health data for communal purposes. Massachusetts state law, for example, prohibits disclosure of identifiable health data without informed consent "except when necessary for disease investigations, control, treatment, and prevention purposes."[31] Montana state law authorizes named reporting of certain diseases and conditions while simultaneously respecting the confidentiality of this information through specific statutory protections. Montana law provides that with respect to investigations of epidemic and communicable diseases, health-care providers may report individual cases (including the name, address, age, sex, diagnosis, and other relevant information) to state and local health departments. Patient consent is not required. However, resulting reports and records must remain confidential. Identifiable health data may not be disclosed except in limited, enumerated circumstances (e.g*.,* to the extent necessary for the treatment, control, investigation, and prevention of conditions dangerous to the public health or to the person who is the subject of a medical record or report).

Some states' laws (1) fail to narrowly define who can have access to such data and to require persons to demonstrate why they need access, (2) lack specificity about when disclosures may be made, (3) potentially allow disclosures to persons or for purposes that are inconsistent with public health (e.g., disclosure in legal settings through court orders or subpoenas), or (4) do not address secondary disclosures of information beyond those used to justify the original collection.[30] Conversely, some states' privacy laws restrict disclosures in a way that actually limits public health authorities' ability to exchange identifiable data across jurisdictions. Several commentators have suggested that state public health information privacy laws in Arkansas, Indiana, and West Virginia, for example, do not "permit disclosure[s] to other state or local health departments for the control of communicable diseases."[32] Strict disclosure provisions can actually interfere with interstate sharing of identifiable health data for legitimate public health purposes. Under some legal interpretations, public health authorities in some states can be hampered from sharing data across jurisdictional boundaries (including between state and tribal entities) because of privacy laws that are improperly constructed so as to limit public health data exchanges.

State laws may also designate particular disease-related data as deserving additional, higher levels of privacy protections. These data might include records concerning treatment for mental health conditions; drug or substance abuse; cancer; or communicable diseases, such as tuberculosis or HIV infection. Pennsylvania protects HIV/AIDS information under its specific privacy laws. Disease-specific privacy protections may make sense when specific conditions such as HIV are viewed by individuals and society as "super-sensitive." However, model privacy proposals, such as the Model State Public Health Privacy Act (MSPHPA)[30] and the HIPAA Privacy Rule, abandon disease-specific classifications in favor of uniformly protecting all health data held within a certain setting.

Developed under the auspices of CDC in 1999, the MSPHPA provides model language for state, tribal, or local governments attempting to provide strong and consistent privacy

safeguards for public health data while preserving the ability of public health authorities to acquire, use, and disclose identifiable health data to protect communal health. The MSPHPA is based on several core privacy principles:

- Protecting health information privacy is synergistic with promoting the public's health;
- All identifiable health data acquired, used, or disclosed by public health authorities deserve equal legal protection;
- Truly nonidentifiable health information requires no legal privacy protections;
- Acquisition and use of identifiable public health data within public health agencies should be based on legitimate public health purposes; and
- Disclosures of identifiable data for non–public health purposes should be strictly limited.

Concerning the latter point, the MSPHPA permits the free exchange of identifiable data with other state, tribal, or local agencies provided the exchanges are needed to promote the public's health.[30]

In addition to MSPHPA, CDC's Model Vital Statistics and Regulations Act (MVSRA) provides model language for state governments that want to maintain a uniform system for producing vital statistic records to satisfy the legal requirements of individuals and their families and to meet public health needs at the local, tribal, state, and national levels. MVSRA provides detailed guidance to state registrars of vital statistics and state legislators who are considering revising their own state vital statistics laws and regulations. Even though the legal responsibility for the registration of vital events rests with individual states, states and CDC's National Center for Health Statistics (the federal partner) collaborate to maintain a uniform vital statistics system. Part of this cooperation includes periodic revision of MVSRA (which is currently undergoing its third revision). Under the current revision to MVSRA, language has been suggested to increase state government recognition of the public health authority of federally-recognized AI/AN governments and their health agencies, as well as the need to share data with them as a regular public health practice.

D. State Laws Concerning Data Sharing Between TECs and State or Local Public Health Agencies

Against this backdrop of national and state privacy laws and policies, we examined specific legal issues related to the ability of TECs to gain access to identifiable health information held by state/local public health agencies in seven selected states (Arizona, Florida, Maine, Nevada, Oklahoma, South Dakota, Washington). **Table 1** catalogs the findings in each jurisdiction (including hyperlinks to Web-based resources citing the laws) according to whether state laws

- *Authorize the sharing of identifiable health data for public health surveillance, research, or other purposes*. This category focuses on state laws that authorize the sharing of identifiable health data by state or local health authorities for public health surveillance, research, or other public health purposes.
- *Specifically authorize the sharing of identifiable health data with tribal authorities*. This category focuses on state laws that specifically authorize the sharing of identifiable health data by state or local health authorities with tribal authorities.

- *Limit the sharing of identifiable health data for privacy-related reasons*. This category focuses on state laws that might limit the sharing of identifiable health data by state or local health authorities because of privacy concerns.
- *Provide any exceptions to data-sharing limitations for privacy-related reasons*. This category focuses on state laws that might recognize exceptions to data-sharing limitations under privacy laws to allow tribal authorities to acquire and use the data.
- *Specifically authorize or limit the sharing of identifiable, disease- or condition-specific data*. This category focuses on state laws that specifically authorize or limit the sharing of disease- or condition-specific identifiable health data (e.g., cancer, HIV, tuberculosis) by state or local health authorities with tribal authorities.
- *Include any additional provisions relevant to data sharing among state/local public health authorities and tribal authorities*. This category lists any additional state laws not otherwise classified in the categories above that might be important to consider in assessing the research question in each jurisdiction.

Table 2, below, provides a cursory review of key legal areas addressed in each state. For the analysis below, direct references to state law are taken directly from relevant jurisdictional sections of Table 1.

Laws in five states (Arizona, Florida, Maine, South Dakota, Washington) feature some form of general legal support authorizing the sharing of identifiable health data for public health surveillance, research, or other purposes. Washington state law, for example, allows broadly for the sharing of any data, research, or findings with the general public (presumably in nonidentifiable format) and entities that have allowed the Secretary of Health to access to their data.

Beyond these general authorizations to share identifiable public health data, only four states' laws (Arizona, Maine, Oklahoma, South Dakota) authorize the sharing of such data with tribal authorities, subject to significant variations. Arizona statutory law limits disclosures from state/local public health authorities to tribal authorities to instances in which data are provided pursuant to an "enhanced surveillance advisory" during bioterrorism events. Maine explicitly mandates that all state agencies make any relevant information and data available to the Indian Tribal-State Commission. Oklahoma law mandates that when state/local public health authorities "learn of a reportable illness, health condition, unusual cluster, or suspicious event," in instances where terroristic action is suspected, they shall immediately notify tribal authorities. In the event of a catastrophic emergency, sharing of information shall be restricted to the information necessary for the treatment, control, investigation, and prevention of a catastrophic health emergency.

Identifiable data that are disease- or condition-specific (e.g., cancer, HIV/AIDS, genetic conditions) are often regulated differently among the states. Laws in five states (Arizona, Florida, Maine, Nevada, South Dakota) may allow TECs to access disease-specific data, subject to limits. South Dakota statutes similarly suggest that cancer data may be shared pursuant to confidentiality regulations (that, according to our review, have not been promulgated. Arizona law allows identifiable genetic data to be shared with authorized agents of federal, state, or county health departments. Florida allows for the sharing of tuberculosis-specific health data but only with individual informed consent or in cases of emergency.

Even though these provisions generally support data sharing among state/local public health authorities and TECs (at least for some types of data), privacy laws create barriers to data

sharing in all seven states (Arizona, Florida, Maine, Nevada, Oklahoma, South Dakota, Washington). Florida state law, for example, features several provisions that limit data sharing on privacy grounds, requiring that all health department data remain "confidential" with limited exceptions (none of which directly applies to tribal health authorities). South Dakota law states bluntly: "All information, interviews, reports, statements, memoranda, or other data procured by the department of health shall be strictly confidential." Statutory law in Nevada discusses the authority of state/local health agencies to share identifiable communicable disease information, generally limiting its disclosure to

- persons likely to have transmitted the communicable disease;
- parents of suspected case-patients;
- health-care providers;
- employers if transmission is enhanced by employment; or
- the principal director of a medical facility, school, child-care facility, or licensed prostitution house if the case-patient works there and potential exists for transmission.

Despite these general privacy limitations, most of the states studied (Arizona, Florida, Maine, Nevada, Oklahoma, South Dakota, Washington) also provide exceptions to privacy-related limitations. For example, South Dakota qualifies its blanket confidentiality protection by noting that the state department of health shall provide information "necessary for disease surveillance and control." Oklahoma provides that identifiable information shall not be disclosed by state or local health agencies but allows use of the data for statistical reporting and data analysis. Concerning communicable disease data, Nevada state law allows further disclosures (1) in some legal proceedings, (2) if an individual provides written consent, or (3) the disclosure is authorized or required by Nevada Revised Statutes 239.0115 (related to historic data collections) *or another specific statute* (emphasis added).

Additional laws in some states provide potential insight as to the allowance of data sharing between state/local and tribal health authorities. For example, Arizona's Attorney General has opined that the state health authority (and other state agencies) shall develop and implement "tribal consultations policies." Florida law supports the creation of a Health Information Systems Council to "facilitate the sharing and coordination of health-related data." Maine's Attorney General specifically recognizes the Penobscot Tribe as a "local government" for the purposes of receiving funds through the state's Disaster Relief Act. Nevada defines "municipalities" (in the context of its public health water safety laws) to include Indian tribal organizations. South Dakota law allows the state health department to contract with any public or private entity (presumably including TECs) to implement or maintain the state's health-care data system. Finally, Washington state law enables tribal authorities to be included as parties to the regional support network (pertaining specifically to mental health services).

V. Health Information Privacy Challenges Concerning Data Sharing Between State/Local Health Departments and TECs

Navigating privacy issues concerning identifiable health data within the existing patchwork of privacy laws and policies at the federal, tribal, state, and local levels is challenging. TECs across the country have experienced legal impediments to their data acquisition practices that are grounded in state public health privacy laws. Some of these legal challenges may be sustainable; others may be based on misinterpretations of existing state laws or over-extensive application of privacy protections. Although complex, many of these legal challenges might also

be resolved through affirmative policies, technical interventions, or other mechanisms. The sections below discuss several legal issues arising from TECs' request for identifiable public health data from state/local health authorities and address potential solutions grounded in balancing individual privacy and tribal communities' needs for the data.

A. Justifying Public Health Data Acquisitions

A fundamental precept of privacy laws and policies is the need to justify collections of identifiable health data. Mass acquisition of identifiable health data for no warranted purposes is a privacy violation, which state laws generally prohibit. Consequently, whenever any entity, particularly within the government, plans to acquire identifiable health information without individual informed consent, it must justify the data acquisition. TEC administrators must carefully assess the justification for their data acquisitions, identify supporting federal or tribal laws that authorize the acquisition, and communicate this information to state/local public health authorities from which data are sought. By affirmatively laying out the legal foundation for TECs to acquire identifiable health data, state/local public health authorities may be more willing to view TECs as public health partners instead of as another entity asking for confidential data to which it is not entitled.

B. Specifying Legal Authority to Acquire Data

Consistent with our initial recommendation, some TECs may consider specifying their legal authority to acquire identifiable health data at the federal or state level. Health information privacy laws (such as the HIPAA Privacy Rule) and state data sharing provisions do not necessarily require public health actors to precisely identify their legal authority to acquire identifiable health data for public health purposes. However, state/local public health authorities concerned about privacy norms might expect or demand this sort of justification before willingly sharing identifiable health data, especially because some data collected by TECs is nontraditional (in that such data might not have been routinely collected as part of other public health surveillance data). In Nevada, for example, state communicable disease data may be disclosed if authorized by "*specific statute*" (emphasis added). To the extent that TEC authorities can refer to explicit legislative (in Nevada), regulatory, or other legal sources that authorize their data collections at the federal, state, or tribal level, they may be able to successfully counter legal arguments denying access to such data.

In most of the states studied, specific legal authority may require legislative or regulatory amendments to introduce specific allowances for identifiable data sharing between state/local public health authorities and TECs. This sort of legal reform might be argued to impinge privacy norms. In reality, sharing identifiable data for public health purposes between public health authorities is routinely allowed under privacy laws. The HIPAA Privacy Rule and the MSPHPA, for example, do not limit sharing of identifiable data between public health authorities for public health purposes. State laws that contravene these principles might effectively hamper public health (to the detriment of state and tribal populations), while providing no substantial health information privacy protections (because individual privacy interests must consistently be balanced with communal public health needs for data). As long as TECs are prepared to confidentially and securely handle and store state/local public health data, state/local public health authorities should support bilateral data exchanges to promote the public's health.

C. Use of Nonidentifiable Data

As discussed above, the acquisition, use, and disclosure of nonidentifiable data do not implicate modern health information privacy laws. To the extent that TEC authorities can acquire and use nonidentifiable health data from state/local health authorities, they can avoid nearly all privacy implications. Unfortunately, in many instances, acquiring or using nonidentifiable data is not practical or possible. Issues of data accuracy and utility can minimize the value of nonidentifiable data. However, the underlying requirement of many privacy laws is clear: *use identifiable health information only to the extent necessary to accomplish the purposes of data acquisitions and no further*. If TEC authorities are able to use nonidentifiable data for their epidemiologic or other public health activities, state/local resistance to sharing based on privacy issues might be minimized (notwithstanding potential costs for state/local public health authorities to de-identify their data before their exchange).

D. Protecting Identifiable Information through Data-Protection Agreements

Existing privacy laws, such as the HIPAA Privacy Rule and multiple states' laws, authorize the use of data-protection agreements to facilitate health information exchanges among public and private actors. Multiple TECs have executed these agreements with each other and state/local public health authorities. These agreements are designed to set forth clear expectations about how to acquire, use, and disclose identifiable health data consistent with privacy laws and policies. They may be executed between parties as binding contracts or considered more informally as internal policies or memoranda of understanding. In either case, these agreements offer meaningful avenues for TECs to gain access to state/local public health data.

Although data-sharing agreements are a helpful tool to enhance data sharing, they are not always a suitable substitute for direct legal authorization and may not be relied on as surrogates for affirmative privacy protections. Execution of data-sharing agreements alone might not sustain long-term data acquisitions between the parties if privacy norms are not followed or if data needs change over time. Absent ongoing monitoring and enforcement of privacy expectations, no maintaining the privacy of identifiable health data is not ensured. Well-drafted data-protection agreements should require parties to regularly monitor their compliance, build technologic features into data systems to prevent unwarranted data exchanges, require mandatory education for persons who may access identifiable data as to their privacy requirements, and set penalties for compliance failures or identified privacy breaches.

E. Clarification of Public Health Practice and Research Uses for Identifiable Data

The right to acquire identifiable health data by public health authorities, without individual written authorization, differs according to the intended purposes and uses of the data. Identifiable data acquired by TECs or other public health authorities for public health research typically require individual authorization, subject to several exceptions. Washington state law clarifies that state agencies may share identifiable information for research without consent provided that

- An IRB has approved the information use,
- No federal laws are violated,
- A confidentiality agreement is obtained with the researcher;,
- Specific safeguards for information are established,
- Published findings do not allow individuals to be identified,
- Information is not disclosed to others, and
- All researchers participating in the project agree to the terms.

The need to distinguish public health practice and research may complicate anticipated data exchanges between TEC and state public health authorities in multiple ways. First, TEC authorities must clearly distinguish their data acquisitions for public health practice activities. Second, TEC authorities must acknowledge that their data are to be used for public health research. These data acquisitions can either require individual advance informed consent or approval through IRBs or privacy boards. Third, once data are acquired and exchanged through the system, uses must be consistent with the purpose for which the data are acquired. Failure to use the data for intended purposes may constitute a privacy violation.

Distinguishing public health practice and research activities is not always easy. The federal Office for Human Research Protections is vetting national guidance on how to distinguish research and non-research activities (including public health practice activities). Its guidance has been internally circulated among DHHS agencies but not yet publicly released for comment. Initial reviews internally within CDC and other federal agencies suggest that the Office for Human Research Protections' revised guidance may characterize increasingly more activities as research. In the interim, CSTE's approach discussed above provides a model for making these distinctions.

F. Additional State-specific Recommendations

In addition to the recommendations above, several legal strategies exist to facilitate data sharing among state/local public health authorities and TECs in the states studied. Laws in most of these jurisdictions do not seem to strongly support or reject data exchanges between TECs and state/local authorities. Facing neutrality, state/local public health authorities might resist data exchanges with TECs because they are not explicitly authorized. The general idea behind their argument is that if the law does not specifically authorize data sharing with a TEC, such sharing must be prohibited. This restrictive legal interpretation is challengeable principally because national models, such as MSPHPA, reject the notion that individual privacy protections should trump legitimate data needs of public health authorities (including TECs). In addition, pending suggested revisions to MVSRA may help increase state government recognition of the public health authority of federally-recognized AI/AN governments and their health agencies as well as the need to share data with them as a regular public health practice. Recharacterizing the legal issue is important. In many ways, the issue is not whether state laws specifically allow data exchanges with TECs but rather whether laws should support them to promote public health.

With these perspectives in mind, we list below some additional state-specific legal strategies that might facilitate future exchanges of health data between state/local public health authorities and TECs. These illustrations provide examples of potential interpretations in multiple jurisdictions (including states not studied for this report).

- *Extension of tribal recognition in Maine.* Maine explicitly mandates that all state agencies make any relevant information and data available to the Indian Tribal-State Commission. Although the limits of our research did not allow for a close look at the major objectives of the Maine Indian Tribal-State Commission, to the extent that this entity supports TECs in the state, state policy may coextensively support data exchanges between state public health authorities and TECs in Maine.

- *Genetic data in Arizona.* Disease- or condition-specific privacy laws in many states might inhibit some data exchanges for sensitive data related to cancer, HIV/AIDS, or genetics. In

Arizona, however, genetic privacy laws specifically allow for sharing of identifiable genetic data with authorized agents of federal, state, or county health departments. This list does not name tribal health departments among those authorized to receive genetic data for public health purposes. This supposed legislative oversight can be easily corrected through minimal reform. Alternatively, TECs in Arizona can claim access to such data as federally funded entities. Or they can point to Arizona's Attorney General Opinion supporting the need for the state health authority to develop and implement "tribal consultations policies" to facilitate its interaction with tribes. These policies provide sufficient, additional support for data exchanges without the need to seek legislative reforms.

- *Exceptions to privacy norms in South Dakota.* South Dakota's flat statutory requirement that all state public health data remain confidential is subject to a broad exception. Specifically, the state health department shall provide data "necessary for disease surveillance and control." This statutory clause does not specify or limit to whom the data shall be provided. Arguably, it may include TECs provided they explain the data are for "disease surveillance and control," which is easily demonstrated. Crafting a legal argument support data exchanges between state/local public health authorities and TECs in South Dakota is consistent with the legislature's minimal policy objectives of supporting effective public health surveillance and control as long as TECs can demonstrate clearly that they need data for public health surveillance purposes.

- *Council policy initiatives in Florida.* Although Florida law is unclear as to the permissibility of identifiable data exchanges between state/local public health authorities and TECs, the Florida legislature has authorized creation of a Health Information Systems Council to "facilitate the sharing and coordination of health-related data." Even though the limits of this research did not allow for exploration of the efforts of this Council, its broad mandate suggests that this entity could support tribal data needs, especially if it supports the health of Florida citizens and tribal residents alike. TEC authorities may appeal to this Council to support data exchanges at the state/local and tribal levels.

- *Tribal recognition in Washington.* Similar to Florida, Washington law does not clearly support data exchanges between TECs and state/local public health authorities. However, the Washington state legislature has firmly recognized the right of tribal authorities to participate in state public health information networks (specifically related to mental health services). This legislative recognition underlies affirmative policy of the state to support tribal initiatives and inclusion in state health outcomes. Similar legislative language reflecting this policy specifically related to TECs would be beneficial. In absence, however, general policy underlying tribal involvement may support confidential data exchanges with TECs.

VI. Conclusion

Privacy challenges are inherent in data-sharing practices between state, local, and tribal public health authorities. Law- and policy-makers at times struggle to find a common ground between individual privacy expectations and the communal health authorities' needs for identifiable health data. The public, typically supportive of the dissemination and use of their identifiable health data for public health purposes, relies on government (or other) entities acquiring their data to maintain appropriate privacy and security protections. Corresponding privacy laws can, however, stymie some data flows between state/local public health authorities and TECs despite communal objectives to use the data to protect the public's health. However, a focused,

national effort is needed to (1) fully recognize TECs' public health authority and (2) develop and implement model policy to strengthen AI/AN disease surveillance.

Although data-sharing practices remain problematic between public health authorities at all levels, the health and well-being of AI/AN communities throughout the United States are jeopardized by a failure to appropriately and responsibly share identifiable health information. Existing legal barriers that thwart these data-sharing practices should be assessed within each jurisdiction and remedied, where possible, through legal interpretations or tools discussed in this report, or approved in each jurisdiction. Risks exist for potential privacy infringements underlying public health data sharing, but the greater good is served by exchanging these data consistent with affirmative confidentiality protections adhered to by state/local public health authorities and TECs.

Table 1. Legal Issues Concerning Identifiable Data Sharing Between State/Local Public Health Authorities and Tribal Epidemiology Centers in Selected States (As of April 2011)

STATE, LEGAL ISSUE	LEGAL AUTHORITIES
Arizona: Does state law:	
Authorize the sharing of identifiable health data for public health surveillance, research, or other purposes?	**§ 36-662. Access to records** Department of Health Services officer or local health department can request records when investigating a reportable communicable disease.
Specifically authorize the sharing of identifiable health data with tribal authorities?	**§ 36-785. Information sharing during an enhanced surveillance advisory** During an event that is reasonably believed to be caused by bioterrorism, the department or local health authority must immediately notify, if appropriate, tribal health authorities with information pertaining to the enhanced surveillance advisory.
Limit the sharing of identifiable health data for privacy-related reasons?	**§ 36-665. Order for disclosure of communicable disease related information** Notwithstanding any other law, a court or administrative body shall not order the department, a county health department, or a local health department to release HIV-related information.
Provide any exceptions to data-sharing limitations for privacy-related reasons?	**§ 36-664. Confidentiality; exceptions.** Exceptions to disclosing communicable disease related information include disclosing to • A federal, state, county, or local health officer if disclosure is mandated by federal or state law. • A federal, state or local government agency authorized by law to receive the information. • A person, health care provider, or health facility to which disclosure is ordered by a court or administrative body. • Any person or entity as authorized by the patient or the patient's health care decision maker. • A person or entity as required by federal law. • A person or entity for federal or state law complying research. The disclosure may be • Specifically authorized or required by federal or state law. • Made pursuant to an authorization signed by the protected person or the protected person's health decision-maker.

	• For the purposes of research as authorized by state and federal law.
Specifically authorize or limit the sharing of disease- or condition-specific identifiable health data (e.g., cancer, HIV, tuberculosis)?	**§ 12-2802. Confidentiality of genetic testing results; disclosure** Genetic testing and information may be disclosed to • A researcher for federal and state law complying public health purposes. • A third person if approved by a human subjects review or human ethics committee concerning persons who are subject to an Arizona cancer registry. • Authorized agents of federal, state, or county health departments.
Include any additional provisions relevant to data sharing among state or local public health authorities and tribal authorities?	**Executive Order 2006-14—Consultation and Cooperation with Arizona tribes** All Executive Branch agencies shall develop and implement tribal consultation policies to guide their work and interaction with federally recognized tribes in Arizona.
Florida: Does state law:	
Authorize the sharing of identifiable health data for public health surveillance, research, or other purposes?	**§ 405.01. Release of medical information to certain study groups; exemption from liability** Any person or other organization may provide information relating to the condition and treatment of any person to research groups and government health agencies to be used in the course of any study for the purpose of reducing morbidity or mortality. **§ 119.0712. Executive branch agency–specific exemptions from inspection or copying of public records** Exemptions of confidentiality include written consent by the individual, a health emergency, a court order showing good cause, and to a health research entity, if the entity seeks the records or data pursuant to a research protocol approved by the department, maintains the records or data with approved protocols, and enters into a purchase and data-use agreement with the department. **§ 381.0022. Sharing confidential or exempt information** Unless contrary to another law, the Department of Health and the Department of Children and Family Services may share confidential information or information exempt from disclosure under chapter 119 about any individual who is or has been the subject of a program within the jurisdiction of each agency.
Specifically authorize the sharing of identifiable health data with tribal authorities?	
Limit the sharing of identifiable health data for privacy-related reasons?	**§ 405.02. Limitation on publication of released information** Research groups and government health agencies shall use or publish information only for the purpose of advancing medical research or medical education in the interest of reducing morbidity or mortality, except that a summary of such studies may be released by any such group for general publication. **§ 405.03. Confidentiality** In all events, the identity of any person whose condition or treatment has been studied shall be confidential. **§ 381.0055. Confidentiality and quality assurance activities** All information that is confidential and obtained by the Department of Health, a county health department, healthy start coalition, or certified rural health network, or a panel or committee assembled by the department, a county health department, healthy start coalition, or certified rural health network shall remain confidential. **§ 381.0273. Public records exemption for patient safety data**

	The Florida Patient Safety Records Corporation may deny a request for records or data that identify the patient if the protocol provides for intrusive follow-back contacts, has not been approved by an IRB, does not plan for the destruction of confidential records after the research is concluded, or does not have scientific merit. The agreement must prohibit the release of any information that would permit identification of any patient, limit the use of records or data in conformance with the approved research protocol, and prohibit any other use of the records or data. Copies of records or data issued pursuant to this paragraph remain the property of the corporation. **§ 119.0712. Executive branch agency–specific exemptions from inspection or copying of public records** The Department of Health may deny a request if the protocol provides for intrusive follow-back contacts, has not been approved by a n IRB, does not plan for the destruction of confidential records after the research is concluded, is administratively burdensome, or does not have scientific merit.
Provide any exceptions to data-sharing limitations for privacy-related reasons?	**§ 381.0273. Public records exemption for patient safety data** Identifiable information that is confidential and exempt from disclosure may be disclosed • With the express written consent of the patient or the patient's legally authorized representative • By court order upon a showing of good cause; or • To a health research entity if the entity seeks the records or data pursuant to a research protocol approved by the Florida Patient Safety Records Corporation, maintains the records or data with approved protocols, and enters into a purchase and data-use agreement with the corporation. Identifiable information re: patient safety may be disclosed: • With the express written consent of the person or entity reporting the patient safety data to the corporation; • By court order upon a showing of good cause; or • To a health research entity if the entity seeks the records or data pursuant to protocols approved by the corporation, maintains the records or data with approved protocols, and enters into a purchase and data-use agreement with the corporation.
Specifically authorize or limit the sharing of disease- or condition-specific identifiable health data (e.g., cancer, HIV, tuberculosis)?	**385.202 Statewide cancer registry.** • Release may be made with the written consent of all persons to whom the information applies • A contractual designee may contact individuals for the purpose of epidemiologic investigation and monitoring, if information is not further disclosed. • The Department of Health may exchange personal data with a contractual designee for the purpose of medical or scientific research, if information is not further disclosed. **§ 392.65. Confidentiality** Tuberculosis information is to be held strictly confidential except • With the consent of all persons to which the information applies; • In a medical emergency but only to the extent necessary to protect the health or life of a person or group of persons
Include any additional provisions relevant to data sharing among state or local public health authorities and tribal authorities?	**§ 381.90. Health Information Systems Council; legislative intent; creation, appointment, duties** State's interest to create a council consisting of executive-level managers for the state's health-related entities, who are appointed by the governor to facilitate the sharing and coordination of health-related data.
Maine: Does state law:	

Authorize the sharing of identifiable health data for public health surveillance, research, or other purposes?	**22 MRSA§ 42 (5)** "Department records that contain personally identifying medical information that are created or obtained in connection with the department's public health activities or programs are confidential. These records include, but are not limited to, information on genetic, communicable, occupational or environmental disease entities, and information gathered from public health nurse activities, or any program for which the department collects personally identifying medical information." Such records "may not be open to public inspection, are not public records … and may not be examined in any judicial, executive, legislative or other proceeding as to the existence or content of any individual's records obtained by the department." **22 MRSA§ 1692-B** "The Department of Health and Human Services must be given access to all confidential reports and records filed by physicians, hospitals or other private or public sector organizations, with all departments, agencies, commissions or boards of the State for the purpose of conducting investigations or evaluating the completeness or quality of data submitted to the department's disease surveillance programs. The department shall follow the data confidentiality requirements of the departments, agencies, commissions or board of the State providing this information. Upon notification by the Department of Health and Human Services, physicians or hospitals shall provide to the department any further information requested for the purpose of conducting investigations or evaluating the completeness or quality of data submitted to the department's disease surveillance programs."
Specifically authorize the sharing of identifiable health data with tribal authorities?	**§ 6212. Maine Indian Tribal-State Commission** All other agencies of the State shall cooperate with the commission and make available to it without charge information and data relevant to the responsibilities of the commission. *Data sharing agreements with Maine's tribes and the State are under way.*
Limit the sharing of identifiable health data for privacy-related reasons?	**22 MRSA § 802 (1)(B)** DHHS is charged with establishing "requirements for reporting and other surveillance methods for measuring the occurrence of communicable, occupational and environmental diseases and the potential for epidemics."
Provide any exceptions to data-sharing limitations for privacy-related reasons?	**22 MRSA § 42 (5)** "Exceptions to this subsection include release of medical and epidemiological information in such a manner that an individual cannot be identified; disclosures that are necessary to carry out the provisions of chapter 250 [Control of Notifiable Diseases and Conditions]; … and disclosures that are specifically provided for by statute or by departmental rule." "Nothing in this subsection precludes the department, during the data collection phase of an epidemiologic investigation, from refusing to allow the inspection or copying of any record or survey instrument, including any redacted record or survey instrument, containing information pertaining to an identifiable individual that has been collected in the course of that investigation. The department's refusal is not reviewable."
Specifically authorize or limit the sharing of disease- or condition-specific identifiable health data (e.g., cancer, HIV, tuberculosis)?	**10 144 255 Maine Cancer Registry Rules and Regulations** All requests for identifying information from outside of the Department of Human Services require approval by the Cancer Registry Program Subcommittee. Written assurances of confidentiality will be of primary importance in considering these requests. The department shall follow subcommittees guidelines on the release of all information.

Include any additional provisions relevant to data sharing among state or local public health authorities and tribal authorities?	**1973 Me. AG LEXIS 139** The Penobscot Tribe performs the functions of local health officer and is a "local government" for the purposes of receiving funds under the Disaster Relief Act of 1970.
Nevada: Does state law:	
Authorize the sharing of identifiable health data for public health surveillance, research, or other purposes?	
Specifically authorize the sharing of identifiable health data with tribal authorities?	
Limit the sharing of identifiable health data for privacy-related reasons?	**441A.300 Health authority: Authorization to disclose information of personal nature to certain persons.** The health authority, which is defined as the district health officer in a district, or his/her designee or, if none, the State Health Officer, or his/her designee, may disclose identifiable information to • Person likely to have transmitted the communicable disease-patient; • The parent of the suspected case-patient; • The health-care provider of a case-patient; • The employer of the case-patient if transmission is enhanced by employment; or The principal director of a medical facility, school, child care facility, or licensed prostitution house if the case-patient works there and there is the potential for transmission. Information must not be disclosed unless the health authority believes the person has been or is likely to be exposed The health authority shall disclose only for the protection of the person to whom it is disclosed.
Provide any exceptions to data-sharing limitations for privacy-related reasons?	**441A.220. Confidentiality of information; permissible disclosure.** All personal information of a communicable disease is confidential except • In a proceeding for an injunction brought pursuant to this chapter. • If the person consents in writing to the disclosure. • If the disclosure is authorized or required by NRS 239.0115 or another specific statute.
Specifically authorize or limit the sharing of disease- or condition-specific identifiable health data (e.g., cancer, HIV, tuberculosis)?	**NRS 457.240 Regulations of State Board of Health.** The State Board of Health shall by regulation 1. Prescribe the form and manner in which the information about cases of cancer must be reported; 2. Specify the malignant neoplasms which must be reported; 3. Prescribe other information to be included in each such report, for example, the patient's name and address, the pathologic findings, the stage of the disease, the environmental and occupational factors, the methods of treatment, the incidence of cancer in the patient's family, and the places where the patient has resided; and 4. Establish a protocol for obtaining access to and preserving the confidentiality of the patients' records needed for research into cancer.
Include any additional provisions	In the context of Public Health Water Safety, **445A.375. "Municipality" defined.**

relevant to data sharing among state or local public health authorities and tribal authorities?	"Municipality" means: an Indian tribe or an authorized Indian tribal organization. **2000 Nev. AG 27** Nevada Indian Commission stands alone from the Department of Education, Health and Human Services
Oklahoma: Does state law:	
Authorize the sharing of identifiable health data for public health surveillance, research, or other purposes?	
Specifically authorize the sharing of identifiable health data with tribal authorities?	**§ 6303. Reportable illnesses, health conditions, unusual clusters, or suspicious events—Duty to notify public health authorities—Sharing of information** When public health authorities (defined as the Oklahoma State Commissioner of Health or local health department that acts principally to protect or preserve the health of the public) learn of a reportable illness, health condition, unusual cluster, or suspicious event, they shall immediately notify tribal authorities if terrorism is suspected.
Limit the sharing of identifiable health data for privacy-related reasons?	**§ 6303. Reportable illnesses, health conditions, unusual clusters, or suspicious events—Duty to notify public health authorities—Sharing of information** Sharing of information shall be restricted to the information necessary for the treatment, control, investigation, and prevention of a catastrophic health emergency. **§ 1-120. Confidentiality of data—Disclosure upon court order—Immunity from liability** The forms of data shall be confidential and shall not be part of the public record.
Provide any exceptions to data-sharing limitations for privacy-related reasons?	**§ 1-120. Confidentiality of data—Disclosure upon court order—Immunity from liability** Identifying information shall not be disclosed, and shall not be used for any purpose except for the creation and maintenance of anonymous medical case histories for statistical reporting and data analysis.
Specifically authorize or limit the sharing of disease- or condition-specific identifiable health data (e.g., cancer, HIV, tuberculosis)?	
Include any additional provisions relevant to data sharing among state or local public health authorities and tribal authorities?	**§ 1-120. Confidentiality of data—Disclosure upon court order—Immunity from liability** The Division of Health Care Information shall establish a Health Care Information Advisory Committee to assist with determinations related to data collection, and information to be released and disseminated to the public.
South Dakota: Does State Law:	
Authorize the sharing of identifiable health data for public health surveillance, research, or other purposes?	**§ 34-14-1. Information obtained in medical studies confidential** All information, interviews, reports, statements, memoranda, or other data procured by the state Department of Health shall only be used for medical research.
Specifically authorize the sharing of identifiable health data with tribal authorities?	**44:20:02:08. Disclosure of reports.** The department may disclose or authorize the disclosure of confidential, pertinent, reportable disease information to

	agencies of the U.S. Public Health Service, including the Centers for Disease Control and Prevention and Indian Health Service, and other local, state, tribal, and territorial health agencies.
Limit the sharing of identifiable health data for privacy-related reasons?	**§ 34-14-1. Information obtained in medical studies confidential** All information, interviews, reports, statements, memoranda, or other data procured by the department of health shall be strictly confidential.
Provide any exceptions to data-sharing limitations for privacy-related reasons?	**§ 34-22-12 Mandatory communicable disease reports from physicians, laboratories, and institutions** The State Department of Health shall provide information necessary for disease surveillance and control.
Specifically authorize or limit the sharing of disease- or condition-specific identifiable health data (e.g., cancer, HIV, tuberculosis)?	**§ 1-43-13. Cancer data collection system—Rules for establishment, maintenance, and use** The State Department of Health shall promulgate rules on maintaining confidentiality and disseminating data.
Include any additional provisions relevant to data sharing among state or local public health authorities and tribal authorities?	**§ 1-43-20. Health care data system—Contracts for implementation or maintenance** For the health-care data system the State Department of Health may contract any public or private entity to implement and maintain part of the system.
Washington: Does State Law:	
Authorize the sharing of identifiable health data for public health surveillance, research, or other purposes?	**§ 43.70.050. Collection, use, and accessibility of health-related data** Any data, research, or findings may also be made available to the general public, including health professions, health associations, the governor, professional boards and regulatory agencies, and any person or group who has allowed the secretary of health access to data. **§ 43.70.545. Data collection and reporting rules** The department of health shall provide necessary data to local health departments for use in planning by or evaluation of any community network authorized under RCW 70.190.060
Specifically authorize the sharing of identifiable health data with tribal authorities?	
Limit the sharing of identifiable health data for privacy-related reasons?	**§ 43.70.050. Collection, use, and accessibility of health-related data** The secretary of health's access to and use of health-related data in any form where the patient or provider of health care can be identified shall not be disclosed, subject to disclosure pursuant to 42.56 RCW
Provide any exceptions to data-sharing limitations for privacy-related reasons?	**§ 70.02.050. Disclosure without patient's authorization** A health-care provider or health-care facility may disclose health-care information about a patient without the patient's authorization to the extent a recipient needs to know the information, if the disclosure is (1) for health-care education; (2) to provide planning, quality assurance, peer review, or administrative, legal, financial, actuarial services to, or other health-care operations for or on behalf of the health-care provider or health-care facility; or (3) for use in a research project that an IRB has determined worthy.
Specifically authorize or limit the	

sharing of disease- or condition-specific identifiable health data?	
Include any additional provisions relevant to data sharing among state or local public health authorities and tribal authorities?	**§ 43.70.050. Collection, use, and accessibility of health-related data** The legislature intends for the secretary of health to create an ongoing program of data collection, storage, assessability, and review, but the legislature does not intend that the department of health conduct or contract for the conduct of basic research activity. **§ 71.24.300. Regional support networks—Inclusion of tribal authorities—Roles and responsibilities** Upon the request of a tribal authority or authorities within a regional support network the joint operating agreement or the county authority shall allow for the inclusion of the tribal authority to be represented as a party to the regional support network (pertaining specifically to mental health services). **§ 70.14.150. Data-sharing agreements—Report** The Department of Social and Health Services and the health-care authority shall enter into data-sharing agreements with the appropriate agencies in the states of Oregon and Idaho to ensure the valid Washington state residence of applicants for health-care services in Washington. Such agreements shall include appropriate safeguards related to the confidentiality of the shared information.

Abbreviations: IRB, institutional review board; DHHS, US Department of Health and Human Services.

Table 2. Summary of Legal Issues Concerning Identifiable Data Sharing Between State/Local Public Health Authorities and Tribal Epidemiology Centers in Selected States (As of April 2011)

Legal Issue: Does State Law:	Arizona	Florida	Maine	Nevada	Oklahoma	South Dakota	Washington	Totals
Authorize the sharing of identifiable health data for public health surveillance, research, or other purposes?	☑	☑	☑			☑	☑	5
Specifically authorize the sharing of identifiable health data with tribal authorities?	☑		☑		☑	☑		4
Limit the sharing of identifiable health data for privacy-related reasons?	☑	☑	☑	☑	☑	☑	☑	7
Provide any exceptions to data-sharing limitations for privacy-related reasons?	☑	☑	☑	☑	☑	☑	☑	7
Specifically authorize or limit the sharing of disease- or condition-specific identifiable health data (e.g., cancer, human immunodeficiency virus infection, tuberculosis)?	☑	☑	☑	☑		☑		5
Include any additional provisions relevant to data sharing among state or local public health authorities and tribal authorities?	☑	☑	☑	☑	☑	☑	☑	7

Notes and References

[1] This Report is based, in part, on the public health information privacy scholarship and analysis of James G. Hodge, Jr., and others, including the following references: Hodge JG, Tsai JT, Anderson E. Health information privacy and the Environmental Public Health Tracking Network: Assessment of legal issues, Am Public Health Association, August 28, 2008: 1-44; Hodge JG. Health information privacy and public health. J Law Med Ethics 2004;31:4:663–71; Hodge JG, Gostin KG. Challenging themes in American health information privacy and the public's health: historical and modern assessments. J Law Med Ethics 2005;32:4:670–9; Hodge JG, Hoffman RE, Tress D, Neslund VS. Identifiable health information and the public's health: practice, research, and policy. In:.Goodman RA, Hoffman RE, Lopez W, et al. eds. Law in public health practice. 2nd ed. 2007. New York: Oxford University Press, 2007:238–61; Hodge JG, Wiley LF. An assessment of legal issues concerning public health disclosures pursuant to proposed administrative regulations re: the Family Education Rights and Privacy Act (FERPA), Atlanta: Council of State and Territorial Epidemiologists, May 1, 2008; 1-13. Available at http://www.cste.org/dnn/LinkClick.aspx?fileticket=KzpIyCJDDmI%3D&tabid=184&mid=733 (accessed March 30, 2009); Gostin LO, Hodge JG. Personal privacy and common goods: a framework for balancing under the national health information privacy rule. Minn L Rev 2002;86:1439–80.

[2] Great Lakes Inter-Tribal Epidemiology Center. Community Health Profile: Minnesota, Wisconsin, & Michigan tribal communities, 2007. Lac du Flambeau, WI: Great Lakes Inter-Tribal Council, Inc., 2008. Available at http://www.glitc.org/epicenter/programs.html (accessed March 30, 2009).

[3] Indian Health Service. Trends in Indian Health 1998–99. Rockville, MD: US Department of Health and Human Services, Indian Health Service, 2001.

[4] Hodge JG, Harris ME. International genetics research and issues of group privacy. Journal of Biolaw and Business 2001; Suppl):15-21.

[5] Government Accountability Office. Information security: protecting personally identifiable information, United States General Accountability Office, GAO-08-343, January 2008. Available at http://www.gao.gov/new.items/d08343.pdf (accessed August 28, 2008), citing Committee on Government Reform, Staff Report: Agency Data Breaches Since January 1, 2003 (Washington, DC, October 13, 2006).

[6] Privacy Rights Clearinghouse. Available at http://www.privacyrights.org/ar/ChronDataBreaches.htm (accessed October 4, 2011).

[7] Goodman B. Georgia patients' records exposed on Web for weeks, Baltimore Sun, April 11, 2008.

[8] Augé K. Financial, medical data found on Net. Denver Post, May 24, 2007. Available at http://www.denverpost.com/headlines/ci_5971015 (accessed November 15, 2011)

[9] Bole K. UCSF alerts patients about a security breach. University of San Francisco, May 28, 2008. Available at http://pub.ucsf.edu/newsservices/releases/200805283/ (accessed August 28, 2008).

[10] In 2006, a class action lawsuit was filed against the federal Veterans Administration after the theft of personal data on 26.5 million military personnel. The stolen information included names, birthdates, Social Security numbers, and disability codes of veterans and active duty personnel. FoxNews.com, June 6, 2006. Available at http://www.foxnews.com/printer_friendly_story/0,3566,198372,00.html (accessed August 28, 2008).

[11] Dimitropoulos LL. International privacy and security solutions for interoperable health information exchange: nationwide summary, July 20, 2007. Available at http://www.rti.org/pubs/nationwide_summary.pdf (accessed March 30, 2009).

[12] 45 C.F.R. § 164.514(a)(b).

[13] Dunkel YF. Medical privacy rights in anonymous data: discussion of rights in the United Kingdom and the United States in light of the source informatics cases, Loy LA Int'l & Comp L Rev 2001; 23:41.

[14] Health Privacy Project, Best principles for health privacy. A report of the Health Privacy Working Group [cited August 28, 2008]. Available athttp://www.healthprivacy.org/usr_doc/33807.pdf http://www.cdt.org/files/file/33807.pdf (accessed March 30, 2009).

[15] Centers for Disease Control and Prevention. HIPAA Privacy Rule and public health: guidance from the Centers for Disease Control and the Department of Health and Human Services. MMWR 2003;52(Suppl):1-12.

[16] 32 C.F.R. 219 (1991).

[17] Hodge JG, Gostin LO. Public health practice vs. research: a report for public health practitioners including case studies and guidance. Report for the Council of State and Territorial Epidemiologists, May 17, 2004. Available at http://www.cste.org/pdffiles/newpdffiles/CSTEPHResRptHodgeFinal.5.24.04.pdf. (accessed March 30, 2009).

[18] Hodge JG. An enhanced approach to distinguishing public health practice and human subjects research. J Law Med Ethics 2005;33:125–41.

[19] Hodge JG. Health information privacy and public health. J Law Med Ethics 2004;31: 663–71.

[20] Hodge JG. The intersection of federal health information privacy and state administrative law: the protection of individual health data and worker's compensation. Admin L R 1999;51:117, 128.

[21] Gostin LO. Health information privacy. Cornell L Rev 1995;80:451, 495.

[22] *Whalen v. Roe*, 429 U.S. 589 (1977).

[23] In *United States v Westinghouse Electric Corp.*, 638 F.2d 570, 578 (3d Cir. 1980), the Third Circuit enunciated five factors to be balanced in determining the scope of the constitutional right to informational privacy: (1) the type of record and the information it contains, (2) the potential for harm in any unauthorized disclosure, (3) the injury from disclosure to the relationship in which the record was generated, (4) the adequacy of safeguards to prevent nonconsensual disclosure, and (5) the degree of need for access—i.e., a recognizable public interest.

[24] *Doe v Borough of Barrington*, 729 F. Supp. 376 (D.N.J. 1990) (holding that police officer violated constitutional right to privacy by disclosing that a person was infected with HIV); Woods v White, 689 F. Supp. 874 (W.D. Wis. 1988) (extending constitutional right to privacy to disclosure of prisoner's HIV status by prison medical service personnel), aff'd, 899 F.2d 17 (7th Cir. 1990); Carter v Broadlawns Medical Ctr., 667 F. Supp. 1269 (S.D. Iowa 1987) (holding that giving chaplains open access to patient medical records violated privacy rights of patients), cert. denied, 489 U.S. 1096 (1989).

[25] 5 U.S.C. 552 (1988).

[26] 5 U.S.C. 552(a) (1988).

[27] 45 C.F.R. § 160.103

[28] 45 C.F.R. §§ 164.524, 164.526.

[29] Nass SJ, Levit LA, Gostin LO, eds. Beyond the HIPAA Privacy Rule: improving health through research. Washington, DC: National Academies Press; 2009.

[30] Gostin LO, Hodge JG, Valdiserri RO. Informational privacy and the public's health: the model state public health privacy act. Am J Public Health 2001;91:1388-–92.

[31] 105 Code of Mass. Reg. 300.120.

[32] Gostin LO, Lazzarini Z, Neslund V, Osterholm M. The public health information infrastructure. JAMA. 1996;275:1921–7.