24. Link BG, Phelan JC. Social conditions as fundamental causes of disease. *J Health Soc Behav.* 1995;(extra issue): 80–94.

25. Loue S. *Gender, Ethnicity, and Health Research.* New York, NY: Kluwer Academic/Plenum Publishers; 1999.

26. *Report of the Secretary's Task Force on Black and Minority Health.* Washington, DC: US Dept of Health and Human Services; 1985.

27. Gamble VN, Blustein BE. Racial differentials in medical care: implications for research on women. In: Mastroianni AC, Faden R, Federman D, eds. *Women and Health Research; Ethical and Legal Issues of Including Women in Clinical Studies.* Vol 2. Washington, DC: National Academy Press; 1994: 174–191.

28. Yu ESH. Ethical and legal issues relating to the inclusion of Asian/Pacific Islanders in clinical studies. In: Mastroianni AC, Faden R, Federman D, eds. *Women and Health Research; Ethical and Legal Issues of Including Women in Clinical Studies.* Vol 2. Washington, DC: National Academy Press; 1994: 216–231.

29. Gamble VN. Under the shadow of Tuskegee: African Americans and health care. *Am J Public Health.* 1997; 87:1773–1778.

30. Holtzman NA, Marteau TM. Will genetics revolutionize medicine? *N Engl J Med.* 2000;343:141–144.

31. Pollard KM, O'Hare WP. America's racial and ethnic minorities. *Popul Bull.* 1999;53. Available at: http://www.prb.org/pubs/population_bulletin/bu54-3/54_3_intro.htm. Accessed November 3, 2000.

32. LaVeist TA. Why we should continue to study race—but do a better job: an essay on race, racism and health. *Ethn Dis.* 1996;6:21–29.

33. Kumanyika SK, Golden PM. Cross-sectional differences in health status in US racial/ethnic minority groups: potential influence of temporal changes, disease, and life-style transitions. *Ethn Dis.* 1991;1:50–59.

34. Call to action; eliminating racial and ethnic disparities in health. In: Proceedings of the National Leadership Conference; September 11, 1998; Potomac, Md. Available at: http://raceandhealth.hhs.gov/sidebars/report.htm. Accessed June 13, 2001.

35. Council on Economic Advisers for the President's Initiative on Race. Changing America. Indicators of social and economic well-being by race and Hispanic origin. 1998. Available at: http://www.access.gpo.gov/eop/ca/index.html. Accessed November 3, 2000.

36. Walsh SJ, Algert C, Gregorio DI, Reisine ST, Rothfield NF. Divergent racial trends in mortality from systemic lupus erythematosus. *J Rheumatol.* 1995;22:1663–1668.

37. McAlindon T. Update on the epidemiology of systemic lupus erythematosus: new spins on old ideas. *Curr Opinion Rheumatol.* 2000;12:104–112.

38. Lin SS, Kelsey JL. Use of race and ethnicity in epidemiologic research. Concepts, methodological issues and suggestions for research. *Epidemiol Rev.* 2000;22:187–202.

Informational Privacy and the Public's Health: The Model State Public Health Privacy Act

Protecting public health requires the acquisition, use, and storage of extensive health-related information about individuals. The electronic accumulation and exchange of personal data promises significant public health benefits but also threatens individual privacy; breaches of privacy can lead to individual discrimination in employment, insurance, and government programs. Individuals concerned about privacy invasions may avoid clinical or public health tests, treatments, or research.

Although individual privacy protections are critical, comprehensive federal privacy protections do not adequately protect public health data, and existing state privacy laws are inconsistent and fragmented. The Model State Public Health Privacy Act provides strong privacy safeguards for public health data while preserving the ability of state and local public health departments to act for the common good.

Lawrence O. Gostin, JD, LLD (Hon), James G. Hodge Jr, JD, LLM, and Ronald O. Valdiserri, MD, MPH

ASSESSING POPULATIONAL health is a core function of state and local public health departments that requires the acquisition, use, and storage of health-related information about individuals.[1,2] National, regional, and statewide governmental public health systems collect vast amounts of public health data regarding communicable (e.g., sexually transmitted diseases [STDs], HIV, tuberculosis), genetic (e.g., newborn metabolic conditions, birth defects), behavioral (e.g., use of drugs, alcohol, and tobacco), and environmental (e.g., pediatric blood lead levels) diseases, conditions, and risks to reduce morbidity and excess mortality.[3]

The accumulation and exchange of these personal data within an increasingly automated public health information infrastructure promises significant public health benefits. Well-planned surveillance helps to identify health problems, target interventions, and influence funding decisions.[4] Health information databases facilitate existing and future epidemiologic investigations and research studies. These essential public health functions rely on the quality and reliability of identifiable health information (i.e., any health-related information that reveals, or could reveal under certain circumstances, the identity of the individual who is the subject of the information).[5]

As increasing amounts of identifiable health data are gathered, stored, and exchanged,[6] personal privacy is threatened. Many Americans distrust government agencies[7] and believe that the collection of personal data without their explicit permission is morally wrong.[8] If public health authorities disclose intimate information, individuals may suffer embarrassment, stigma, and discrimination in employment, insurance, and government programs.[3,9] Persons who fear invasions of privacy may avoid clinical tests and treatments, withdraw from research, or provide inaccurate or incomplete health information.[10]

Congress has unsuccessfully pursued comprehensive health information privacy legislation,[11] but the Department of Health and Human Services recently issued final regulations pursuant to the Health Insurance Portability and Accountability Act of 1996.[12] However, these federal initiatives do not regulate government collection of state public health in-

formation. Since public health is quintessentially a state function, federal privacy rules defer to state public health law under principles of federalism.

Although state public health agencies have an excellent track record of safeguarding public health data, extant state laws concerning public health information privacy are inconsistent, fragmented, and inadequate.[2] These laws differ significantly in the degree of privacy protection afforded, give varying rights to access identifiable data, and allow multiple exceptions to disclosure prohibitions outside public health agencies.[2] Some states' laws declare that public health records are private, but they are silent about the degree of protection of privacy. Laws often fail to narrowly define who may have access to such data and to require persons to demonstrate why they need access. Statutes often lack specificity about when disclosures may be made, permissively allow disclosures to persons or for purposes that are inconsistent with those of public health (e.g., disclosure in legal settings through court orders or subpoenas), or fail to address secondary disclosures of information beyond those used to justify the original collection. In some states, disclosure provisions are too strict, interfering with legitimate public health exchanges of identifiable data among in-state and out-of-state public health agencies.

Current law and policy often fail to reconcile individual privacy interests with collective public health interests in identifiable health data. Civil libertarians and consumers see informational privacy as a fundamental right and stress the importance of stronger legal safeguards. Public health professionals, on the other hand, strongly assert the need to use data to achieve important public health purposes. To reconcile these 2 divergent approaches, the Georgetown/Johns Hopkins Program on Law and Public Health convened a multidisciplinary team of privacy, public health, and legislative experts to propose a model public health information privacy statute.[13] The Model Act would provide, for the first time, strong and consistent privacy safeguards for public health data, while still preserving the ability of state and local health departments to act for the common good. The Centers for Disease Control and Prevention recommends that states consider adopting the model legislation to "strengthen the current level of protection of public health data."[14] In this commentary, we explain the Model Act and the principles that underlie its protections.

RECONCILING PUBLIC HEALTH AND PRIVACY INTERESTS

Some scholars perceive a conflict between individual privacy interests (which seek strict limits on data uses) and public health interests (which seek more expansive data uses for the common good).[15,16] This conflict, while complex and difficult, often can be resolved. The Model Act's approach is to maximize privacy safeguards where they matter most to individuals and facilitate data uses where they are necessary to promote the public's health. This accommodation between privacy and public health balances individual and collective interests.

Consider the sequence of events when a government agency collects public health data through, for example, reporting or other forms of surveillance. First, the agency *acquires* the data, typically after the patient has given informed consent (usually to a medical care provider) to provide a biologic sample (e.g., blood or urine) or health-related behavioral information (e.g., sexual history or drug use practices). Given that there is a strong public health interest, most people believe that patients should accept this invasion of privacy for the collective good. Next, the agency *uses* the data strictly within the confines of the health department. Again, if the agency has a strong public health interest and the data are shared only with agency officials who have a need to know, data uses should prevail over privacy. When public health authorities acquire and use data strictly within the agency, public health benefits are at their highest and risks to privacy are at their lowest. The agency needs the freedom to use the data to monitor and prevent health risks. If public health authorities do not disclose the identifiable data outside the agency, patients face few social risks.

Finally, the agency may be asked or, under unusual circumstances, may seek to *disclose* personally identifiable information to persons outside the agency—for example, to employers, insurers, commercial marketers, family, or friends. These kinds of disclosures are not very important for the public's health, but they do place patients at considerable risk of embarrassment, stigma, and discrimination. For these reasons, the law ought to provide maximum protection of privacy. The Model Act's approach, therefore, is to give government flexibility to acquire and use data strictly within the mission of the public health agency, providing it can demonstrate an important public health purpose. However, the Model Act affords public health authorities very little discretion to release personally identifiable data outside the agency and imposes serious penalties for disclosures without the patient's informed consent.

THE MODEL STATE PUBLIC HEALTH PRIVACY ACT

The Model Act is structured to protect privacy and security interests without thwarting public health goals underlying the acquisition, use, disclosure, and storage of identifiable health data at the state and local levels. Figure 1 provides a flowchart image of the Model Act, the design of which is based on several core assumptions.

Public health and privacy are synergistic. The debate surrounding public uses of identifiable data and individual privacy assumes that these interests are mutually exclusive. This is not invariably the case, however. Public health agencies have significant interests in protecting the privacy of health-related information. Protecting individual privacy encourages individuals to voluntarily participate in public health and individual health care programs and to freely divulge personal information, thus improving the reliability and quality of data.[4] Privacy advocates (and others) benefit from a well-functioning, efficient public health system that works to improve population health outcomes. In these ways, public health and privacy are synergistic, thus suggesting that the Model Act, if passed, would actually im-

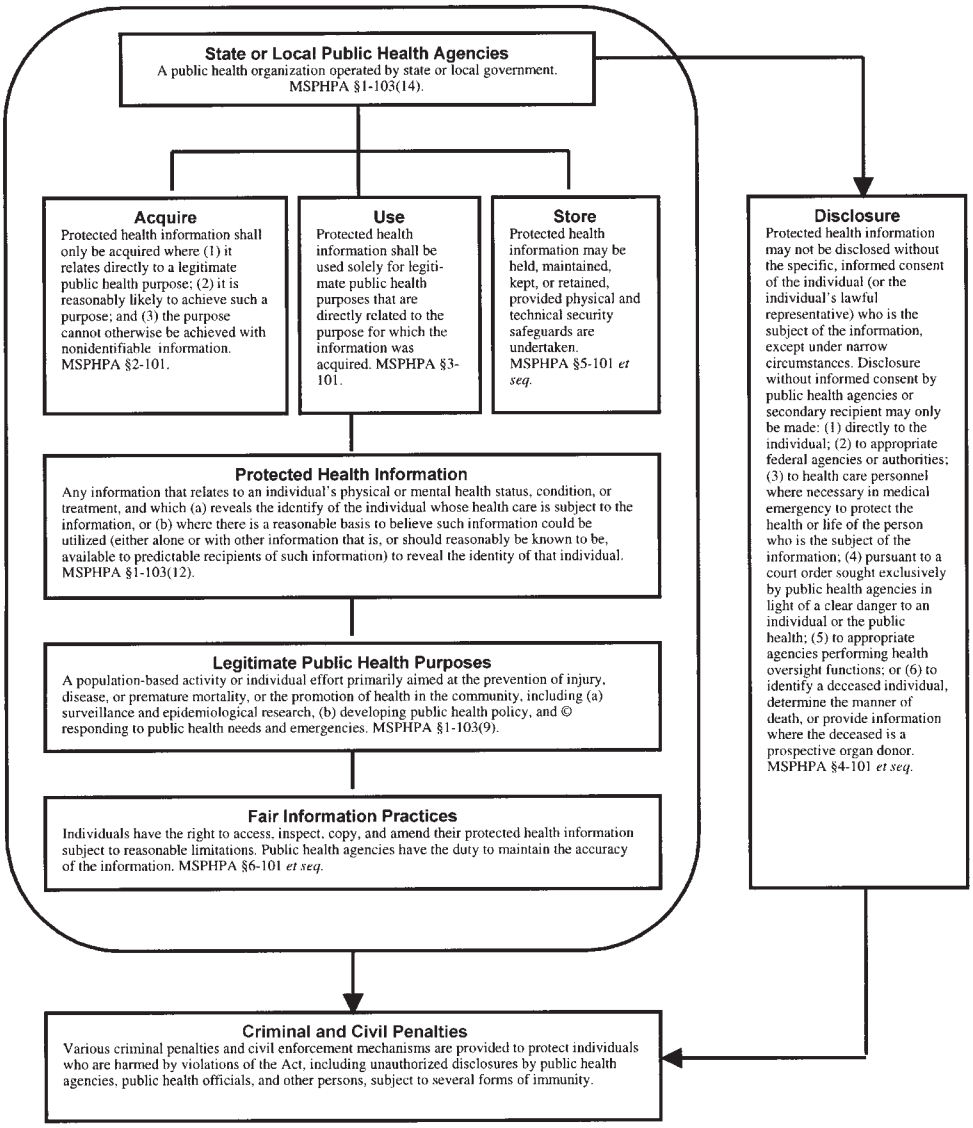

FIGURE 1—The Model State Public Health Privacy Act.

prove public health outcomes, not thwart them.

All identifiable health information deserves legal protection. The Model Act applies to all "protected health information" held by public health agencies. This includes any public health information, whether oral, written, electronic, or visual, that relates to an individual's past, present, or future physical or mental health status, condition, treatment, service, product purchases, or provision of care. This broad definition of protected health information recognizes that any identifiable data (e.g., HIV, STD, or immunization status) can be sensitive.

Nonidentifiable health information requires no protection. The definition of "protected health information" specifically incorporates another core assumption: nonidentifiable health data do not merit privacy protection. Where health data are truly nonidentifiable, individual privacy interests are not threatened. Notwithstanding the interests of societal groups (e.g., ethnic, racial, or religious minorities) in the protection of some nonidentifiable information, the Model Act only regulates in favor of individual privacy interests. Protected health information includes only health information (1) that reveals the identity of the individual whose health care is the subject of the information (e.g., health data that refer to the name, social security number, or any other information about the person who is the subject of the data) or (2) that, in cases where there is a reasonable basis to believe, could be used (either alone or with other information that is known to be available to predictable recipients of such information) to reveal the identity of that individual. Under this latter category of protected health information, even aggregate statistical data may be identifiable. Consider, for example, statistical data that reveal that a Native American female in a small county is infected with HIV. If this information can be used to identify this individual because the ethnic group membership is sufficiently small in the county, the data are individually identifiable under the Model Act. Since nonidentifiable information cannot infringe individual privacy, the act requires public health agencies, whenever possible, to use data stripped of personal identifiers.

Acquisition and use are contingent upon legitimate public health purposes. The Model Act regulates the ways in which public health agencies acquire, use, disclose, and store protected health information. It safeguards privacy, in part, by requiring public health authorities to demonstrate a legitimate public health purpose for the acquisition and use of data. The act defines "legitimate public

health purpose" to mean a population-based activity or individual effort primarily aimed at the prevention of injury, disease, or premature mortality, or the promotion of health in the community (see Figure 1). Such efforts include carrying out public health surveillance, conducting epidemiologic research, developing public health policy, and responding to public health needs and emergencies. While interpretation of a legitimate public health purpose may admittedly narrow or broaden the scope of the act, it allows flexibility in prioritizing various state public health activities across jurisdictions.

In addition to imposing a requirement to justify data acquisition, the Model Act limits the use of identifiable information within the agency. In particular, it specifies that (1) nonidentifiable data must be used whenever possible, (2) the sharing of identifiable data among public health officials must be limited to the minimum amount necessary, (3) public health officials may have access to identifiable data only if they have a demonstrable need to know, and (4) agencies must protect security by maintaining the data in a physically and technologically secure environment.

Disclosures must be strictly limited. While the Model Act affords public health agencies the power to acquire and use health data for important public health purposes, it grants very little authority to disclose identifiable data outside the public health system. The act clarifies that protected health information is not subject to public review (e.g., inspection, dissemination, or investigation by members of the public) and may not be disclosed without the specific informed consent of the individual who is the subject of the information (or the individual's lawful representative), except under narrow circumstances.

Disclosures without informed consent may only be made as follows.

1. Directly to the individual. For example, a public health agency may contact an individual about identifiable health information it has about the individual without that person's consent.
2. To appropriate federal agencies or authorities. As a model *state* law, the Model Act cannot restrict federal demands for identifiable information under constitutional principles.
3. To health care personnel where necessary in a medical emergency to protect the health or life of the person who is the subject of the information from serious, imminent harm. This exception is exceedingly narrow. It would not allow, for example, a disclosure to protect the health of a person who is not the subject of the information, such as a health care worker who was injured by a needle that may have been used by an individual infected with HIV.
4. Pursuant to a court order sought exclusively by public health agencies in light of a clear danger to an individual or to the public health that can be averted or mitigated only through a disclosure by the agency. This is the only exception for the disclosure of protected health information pursuant to a court order.
5. To appropriate public or private agencies performing health oversight functions relating to the public health agency as authorized by law.
6. To identify a deceased individual, determine the manner of death, or provide information in cases where the deceased is a prospective organ donor.

Secondary disclosures by recipients of protected health information from public health agencies are specifically prohibited without individual informed consent or authorization under the narrow exceptions. Naturally, this prohibition does not apply to the (a) individual subject of the information, (b) persons authorized to make health care decisions for the individual, or (c) any person who is specifically required by federal or other state law to disclose the information.

Finally, the Model Act permits the exchange of data among public health agencies within and outside the state. These information exchanges are viewed as data *acquisitions* or *uses*, not *disclosures*. As such, public health agencies may exchange identifiable health data with other state or local agencies provided the exchanges are necessary for the public's health. For example, comparing HIV and tuberculosis registries among state and local health agencies is an important public health function, given the strong relationship between these two diseases.

FAIR INFORMATION PRACTICES

Safeguarding privacy requires data holders to engage in a range of fair information practices. These practices ensure strong security and privacy of public health information, but they do not unreasonably burden public health authorities. The act incorporates the following fair information practices.

Justifying the Need for Data Collection

Acquiring identifiable data is not an inherent good. Rather, public health authorities must substantiate the need for identifiable data. As discussed above, the Model Act affirms that public health agencies shall only acquire identifiable health information that (a) relates directly to a legitimate public health purpose and (b) is reasonably likely to achieve such a purpose. When information is no longer needed to fulfill the purpose for which it is acquired, it must be expunged or made nonidentifiable.

Informing Data Subjects

The act acknowledges that individuals are entitled to know how information about them is being used. Public health agencies may not acquire identifiable data without public knowledge. Before acquiring such data, public health agencies must provide public notice (through written information distributed in such a way as to reasonably inform the public) concerning their intentions to acquire the data and the purposes for which the data will be used. Individuals are entitled to view records of disclosures of their protected health information, which public health agencies are required to maintain.

Access to One's Own Data

Subject to reasonable limitations, individuals are entitled to access, inspect, and copy their health data. Public health agencies are required to explain to individuals any code, abbreviation, notation, or other marks appearing in the information, as well as to ensure the accuracy of such data and amend any errors.

Ensuring Privacy and Security

Public health agencies have a duty to adhere to privacy and security safeguards. Specific protections are administered by a designated health information officer appointed by each public health agency and enforced through significant administrative, criminal, and civil penalties. These protections apply to identifiable health data, regardless of their holder, through various provisions of the act that (a) require an affirmative statement of privacy protections to accompany the disclosure of protected health information and (b) apply similar criminal and civil sanctions for unlawful disclosures to public health officials as well as secondary recipients.

CONCLUSION

The Model State Public Health Privacy Act is a product of consensus-building among nationally prominent experts in privacy and public health.[12] The National Conference of State Legislatures plans to make the act available to state legislators interested in promoting health information privacy.[17] At least one state legislature, Texas, has introduced a version of the Model Act to date.[18] Proposed legislation concerning health information privacy in New York has incorporated some of the language and principles embodied in the act.[19]

Although not perfect, the act provides a balance between the social good of data collection (recognizing its substantial value to community health) and the individual good of privacy (recognizing the normative value of respect for persons). It authorizes public health agencies to acquire, use, and store identifiable health data for public health purposes while simultaneously requiring them to respect individual privacy and imposing stiff penalties for failure to comply. Individuals are empowered with various privacy rights and remedies for breaches of these duties. The community generally is sympathetic to data collection for public health purposes, but it seeks strong legal protection against potentially harmful uses of personal information. States that adopt the act or laws consistent with its structure can stabilize and modernize public health information practices. If the act serves as a model across multiple jurisdictions, it could reduce the variability of existing protections among states, allow for the responsible exchange of health data within a national public health information infrastructure, and ultimately improve public health outcomes. ■

About the Authors

Lawrence O. Gostin is with Georgetown University Law Center, Washington, DC, and the Center for Law and the Public's Health, Baltimore, Md, and Washington, DC. James G. Hodge Jr is with the Johns Hopkins Bloomberg School of Public Health, Baltimore, Md, and the Center for Law and the Public's Health, Baltimore, Md, and Washington, DC. Ronald O. Valdiserri is with the Centers for Disease Control and Prevention, Atlanta, Ga.

Requests for reprints should be sent to James G. Hodge Jr, JD, LLM, Center for Law and the Public's Health, Johns Hopkins Bloomberg School of Public Health, 624 N Broadway, Room 582, Baltimore, MD 21205-1996 (e-mail: hodgej@erols.com).

This commentary was accepted March 19, 2001.

Contributors

L.O. Gostin convened and chaired the panel (of which J.G. Hodge and R.O. Valdiserri were members) to develop the Model State Public Health Privacy Act. L.O. Gostin and J.G. Hodge drafted the act with the assistance of the panel. All 3 persons contributed to the writing of the commentary.

Acknowledgments

This project was supported by the Centers for Disease Control and Prevention, the Council of State and Territorial Epidemiologists, the Association of State and Territorial Health Officers, and the National Conference of State Legislatures.

The authors are grateful for the contributions of the following individuals who served as consultants in the drafting and review of the Model Act: Julio C. Abreu, Christopher E. Anders, Cornelius Baker, Gus Birkhead, K. King Burnett, Scott Burris, J. Richard Ciccone, Jeffrey S. Crowley, Kevin DeCock, Ruth R. Faden, John P. Fanning, Chai Feldblum, Helen Fox Fields, Patricia Fleming, Robert Gellman, Eric P. Goosby, Richard N. Gottfried, Paula C. Hollinger, Tracey Hooker, John F. Hybarger, Michael T. Isbell, Rob Janssen, Derek Link, Glen Maxey, Kristine Moore, Verla S. Neslund, James L. Pearson, Steven B. Powell, Kevin Quinn, Marc Rotenberg, Steve Scarborough, Julie Scofield, Susan K. Steeg, Robert E. Stein, John W. Ward, David Webber, and Timothy Westmoreland.

References

1. Institute of Medicine. *The Future of Public Health.* Washington, DC: National Academy Press; 1988.

2. Gostin LO. *Public Health Law: Power, Duty, Restraint.* Berkeley: University of California Press; 2000.

3. Gostin LO, Lazzarini Z, Neslund V, Osterholm M. The public health information infrastructure. *JAMA.* 1996; 275:1921–1927.

4. Gostin LO, Hodge JG. The "names debate": the case for national HIV reporting in the United States. *Albany Law Rev.* 1998;61:679–743.

5. Hodge JG, Gostin LO, Jacobson PD. Legal issues concerning electronic health information. *JAMA.* 1999;282: 1466–1471.

6. National Research Council, Committee on Maintaining Privacy and Security in Health Care Applications for the National Information Infrastructure. *For the Record: Protecting Electronic Health Information.* Washington, DC: National Academy Press; 1997.

7. Wills G. *A Necessary Evil: A History of American Distrust of Government.* New York, NY: Simon & Schuster; 1999.

8. Beauchamp TL, Childress JF. *Principles of Biomedical Ethics.* New York, NY: Oxford University Press; 1994.

9. Blum BM, Crooks GM. Designing solutions for securing patient privacy—meeting the demands of health care in the 21st century. *J Am Pharm Assoc.* 1999;390:402–407.

10. Goldman J. Protecting privacy to improve health care. *Health Aff.* 1998; 17:47–60.

11. Pear R. Clinton to unveil rules to protect medical privacy. *New York Times.* October 27, 1999:A1.

12. *Standards for Privacy of Individually Identifiable Health Information: Final Rule, 45 CFR Part 160–164.* Washington, DC: Dept of Health and Human Services; 1999.

13. Gostin LO, Hodge JG. Model State Public Health Privacy Act. 1999. Available at: http://www.critpath.org/msphpa/privacy.htm. Accessed June 15, 2001.

14. CDC guidelines for national human immunodeficiency virus case surveillance. *MMWR Morb Mortal Wkly Rep.* 1999;48:1–27.

15. Gostin LO. Health information privacy. *Cornell Law Rev.* 1995;80: 101–184.

16. Etzioni A. *The Limits of Privacy.* New York, NY: Basic Books; 1998.

17. Model state law on privacy of medical records sets strict protections for identifiable information. *State Health Watch.* 1999;6:3.

18. HR 3254, 76 Leg. Reg Sess (Tx 1999).

19. Assemb 4473, 223rd Leg, Reg Sess (NY 1999); Assemb 11242, 223rd Leg, Reg Sess (NY 1999); S 8127, 223rd Leg, Reg Sess (NY 1999).