9 HOUS. J. HEALTH L & POL'Y 131-156

ISSN 1534-7907

MISSING THE MARK: THE PUBLIC HEALTH EXCEPTION TO THE HIPAA PRIVACY RULE AND ITS IMPACT ON SURVEILLANCE ACTIVITY

Andrea Wilson, J.D.*

I. INTRODUCTION

The evaluation and maintenance of public health has long been recognized as an essential function of government in the United States, even predating the Revolutionary War.[1] Public health

* University of Houston Law Center.

1 Lawrence O. Gostin et al., *The Public Health Information Infrastructure: A National Review of the Law on Health Information Privacy*, 275 JAMA 1921, 1921-22 (1996).

agencies' essential functions focus on the general health of the population to protect against epidemics, environmental risks, the effects of natural disasters, and insufficient accessibility to adequate health services.[2] Surveillance, defined as "the systematic observation of a population to identify the causes, prevalence, incidence, and health effects of injury or disease," is accomplished by the accumulation, compilation, and use of information about the health of individuals.[3] It is one of the primary means by which public health officials are able to foster and support these needed functions, enabling agencies to develop policy that will reduce risk to the public's health.[4] Surveillance involves "disease reporting, anonymous serological surveys, and other epidemiological investigation" to gather information "on both communicable and noncommunicable diseases."[5] Properly utilized, surveillance is a fundamental government activity, indispensable in nature.[6]

Notwithstanding this recognition, maintaining and perhaps enhancing the privacy of individual health information is of central importance, particularly in light of the current social atmosphere.[7]

The Supreme Court has recognized a general, though narrowly constrained, right to the privacy of medical information:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files . . . The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. [We] [r]ecogniz[e] that in some

---

2 Lawrence O. Gostin, *A Theory and Definition of Public Health Law*, *in* Public HEALTH LAW: POWER, DUTY, RESTRAINT 3, 12, 16-17 (2000).

3 Lawrence O. Gostin et al., *The Law and the Public's Health: A Study of Infectious Disease Law in the United States*, 99 COLUM. L. REV. 59, 82 (1999).

4 Gostin et al., *supra* note 1, at 1921-22.

5 Gostin et al., *supra* note 3, at 82.

6 *Id*.

7 James G. Hodge, Jr. & Kieran Gostin, *Challenging Themes in American Health Information Privacy and the Public's Health: Historical and Modern Assessments*, 32 J.L. MED. & ETHICS 670, 671 (2004) ("Historically, balancing was about recognizing the societal value of information collection (e.g., disease surveillance, epidemiological investigation), as contrasted with the individual's benefits of privacy. The factors of balancing may be the same, but the emphasis on the community versus the individual has reversed.").

circumstances that duty arguably has its roots in the Constitution. . . .[8]

Although the Court in *Whalen* declined to invalidate the New York statute in question, the Stevens opinion marked the first occasion on which the Court analyzed public health policy in terms of a balance between the public interest in collection of information and the privacy rights of the individual.[9]

Though seemingly at odds with one another, surveillance and the protection of health information privacy can also be consistent goals.[10] A public perception that privacy is protected is likely to "encourag[e] individuals to fully utilize health services and cooperate with health agencies."[11] Finding the optimum balance between public health activities and privacy is key to protecting the well-being of the community, and yet the enactment and enforcement of current legislation threatens to disrupt this balance. In particular, the public health exception to the Health Insurance Portability and Accountability Act's Privacy (HIPAA) Rule[12] has put this balance in jeopardy because it is drafted in such a way as to cause confusion and a recognized reluctance to provide information to state and local public health agencies. Though well-intentioned, the exception ambiguously defines the role of public health authorities in maintaining the privacy of personally identifiable health information.

---

8 Whalen v. Roe, 429 U.S. 589, 605 (1977) (upholding a New York statute which required centralized computer records to document the issuance of prescriptions for specified drugs for which there was potential for sale on the illegal market on the basis of sufficient privacy protections built into the computer database and a corresponding minimal risk to individuals).

9 Peter H.W. Van Der Goes, Jr., *Opportunity Lost: Why and How to Improve the HHS-Proposed Legislation Governing Law Enforcement Access to Medical Records*, 147 U. PA. L. REV. 1009, 1033 (1999). The article also acknowledges reluctance by the lower courts to extend this privacy right with an increasing "level of deference" afforded to government agencies. Id. at 1034-35 (citing Doe v. Se. Pa. Transp. Auth. (SEPTA), 72 F.3d 1133, 1135 (3d Cir. 1995); United States v. Westinghouse, 638 F.2d 570, 580 (3d Cir. 1980)); *see also* Lawrence O. Gostin, Health Information Privacy, 80 CORNELL L. REV. 451, 498 (1995) (citing Doe v. Borough of Barrington, 729 F. Supp. 376 (D.N.J. 1990); Woods v. White, 689 F. Supp. 874 (W.D. Wis. 1988); and Carter v. Broadlawns Med. Ctr., 667 F. Supp. 1269 (S.D. Iowa 1987)).

10 Lawrence O. Gostin et al., *The Nationalization of Health Information Privacy Protections*, 37 TORT & INS. L.J. 1113, 1119 (2002).

11 *Id.*

12 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., and 42 U.S.C.).

This is a problem particularly because "a lack of statutory guidance may lead public health officials either to overuse or to underuse coercive powers," possibly resulting in "discriminatory use [of power] against stigmatized or marginalized groups . . . even when health officials have no malevolent intentions."[13] The broad public health exception to the HIPAA Privacy Rule inadequately protects the personal health information of individuals and insufficiently defines the criteria by which public health officials may obtain such data, necessitating an amendment to current policy in the form of a heightened statutory minimum for state and local agency compliance.

This paper will explore the ambiguities and recognized problems with HIPAA's public health exception, as well as suggest additional criteria to improve privacy protections and the ability of public health officials to efficiently obtain and utilize personal medical information. Part II of the paper will explain the legislative history and regulatory provisions of the HIPAA Privacy Rule, as well as the specific terms of the public health exception. Part III includes criticism of the exception in its current form, detailing ambiguities and interpretation discrepancies. Part IV examines proposed legislation for further privacy protections and suggests amendments to improve current regulations. These provisions would include stronger requirements for justification, freedom of access, and secondary disclosure for both research and governmental use. Finally, Part V advocates broadening the terms of the federal standards for privacy given the vast array of state laws, which provide disparate protections for identifiable medical records. The goal of this paper is to explore current issues with the public health exception to the HIPAA Privacy Rule and identify potential solutions that will improve both personal health information privacy and public health practice, striking a balance between the needs of individuals and public health officials.

II. THE LEGAL LANDSCAPE

Congress enacted the Health Insurance Portability and

[13] Gostin et al., *supra* note 3, at 116.

Accountability Act of 1996[14] (HIPAA) in an effort to improve continuity of insurance coverage for individuals changing employers and to ensure privacy of health records.[15] Congress recognized and hoped to encourage the already-expanding use of electronic record-keeping methods in health care to facilitate efficient, high-quality treatment by enacting standardized regulations to maintain the privacy of individuals and their personal and medical information.[16] The legislature allotted itself three years in which to finalize the necessary comprehensive privacy regulations. When the legislature failed to meet this deadline, the Secretary of the Department of Health and Human Services (HHS) assumed the process of promulgating a federal privacy rule as required by the terms of HIPAA.[17] A proposed rule was presented in October 1999, drawing 53,000 public comments.[18] HHS issued the final rule in December 2000, and after a thirty-day comment period, President Bush and HHS Secretary Tommy Thompson announced that the rule would go into effect with a compliance deadline of April 2003. [19]

The HIPAA Privacy Rule standardizes forms and requirements for disclosures of individually identifiable protected health information (PHI).[20] Under the regulations, health care providers,

---

14 *Id*.

15 Centers for Disease Control and Prevention (CDC), *HIPAA Privacy Rule and Public Health: Guidance from CDC and the U.S. Department of Health and Human Services*, 52 MORBIDITY & MORTALITY WEEKLY REPORT 1 (Apr. 11, 2003), *available* at http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm (last visited Mar. 26, 2008).

16 *Id*.

17 Sharon J. Hussong, *Medical Records and Your Privacy: Developing Federal Legislation to Protect Patient Privacy Rights*, 26 AM. J.L. & MED. 453, 453-54 (2000).

18 Peter B. Swire & Lauren B. Steinfeld, *Security and Privacy After September 11: The Health Care Example*, 86 MINN. L. REV. 1515, 1524 (2002); Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14,776, 14,799 (Mar. 27, 2002).

19 Dep't of Health & Human Servs., *Protecting the Privacy of Patients' Health Information*, HHS FACT SHEET (May 9, 2001), http://aspe.hhs.gov/admnsimp/final/pvcfact2.htm.

20 CDC, *supra* note 15. PHI includes: "names; geographic subdivisions smaller than a state, including county, city, street address, precinct, zip code, and their equivalent geocodes; all elements of dates (except year) directly related to an individual; all ages <89 and all elements of dates (including year) indicative of such age (except for an aggregate into a single category of age >90); telephone numbers; fax numbers; electronic mail addresses; Social Security numbers; medical record numbers; health-plan beneficiary numbers; account

health insurance plans, and health care clearinghouses, collectively designated as covered entities, are required to obtain patient consent, subject to limited exceptions, before releasing PHI to third parties.[21] The HIPAA Privacy Rule does not preempt state medical record privacy statutes.[22] The Rule and its exceptions are minimum criteria, and state legislatures maintain discretion to expand upon the terms of the regulations.[23] Patients are afforded certain fair information rights including the ability to review and make amendments to their records, receive notice of a covered entity's PHI practices, and request an accounting of all disclosures.[24]

There are, however, a number of general exceptions to the consent requirements, permitting covered entities to release PHI without obtaining patient approval. These include disclosures: (1) as required by law; (2) for public health purposes; (3) for health research subject to prior approval by an institutional review board (IRB) or privacy board; (4) for purposes of reporting abuse, neglect, or domestic violence; (5) for law enforcement purposes; (6) in judicial and administrative proceedings; (7) for cadaveric organ, eye, or tissue donation purposes; (8) for health oversight activities; and (9) for worker's compensation.[25]

---

numbers; certificate and license numbers; vehicle identifiers and serial numbers, including license plate numbers; medical device identifiers and serial numbers; Internet universal resource locators (URLs) [sic]; Internet protocol (IP) addresses; biometric identifiers including fingerprints and voice prints; full-face photographic images and any comparable images; and any other unique identifying number, characteristic, or code, except that covered identities may, under certain circumstances, assign a code or other means of record identification that allows de-identified information to be re-identified." *Id.*

21 CDC, *supra* note 15; 45 C.F.R. § 164.508 (2008). On February 17, 2009, President Obama signed the American Recovery & Reinvestment Act of 2009 (ARRA) into law, further expanding the regulations on privacy of electronic health records (EHR). Though beyond the scope of this paper, a review of the requirements of ARRA is beneficial for a comprehensive understanding of federal health information privacy law. The Act extends privacy protection to EHRs received and retained by business associates of covered entities. *See* Am. Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, §§ 13401, 13402, 123 Stat. 115.

22 45 C.F.R. § 160.202 (2008).

23 *Id.*

24 Lawrence O. Gostin et al., *Balancing Communal Goods and Personal Privacy Under a National Health Informational Privacy Rule*, 46 ST. LOUIS U. L.J. 5, 6-7 (2002).

25 45 C.F.R. § 164.512 (2008).

In the process of promulgating the Privacy Rule, HHS recognized the need to carve out an exception for public health purposes in order to allow authorities at all levels of government to continue to collect, analyze, and use health information that would otherwise be unavailable without prior patient consent.[26] More specifically, a covered entity:

> [M]ay disclose PHI to a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority.[27]

A public health authority is broadly defined by the Rule as any federal, state, tribal, or local agency responsible for the public's health under an official mandate.[28] The agency may be collecting PHI pursuant to a specific statute or regulation, though this is not required as long as the agency is authorized by law.[29] By drafting the exception in such expansive terms, HHS indicated its recognition that public health authorities often "operate under broad mandates to protect the health of their constituent populations."[30]

Notably, covered entities are merely permitted to make such disclosures to public health authorities; the exception provides no requirement for the release of information.[31] Additionally, if the covered entity elects to disclose PHI to a public health authority who submits a request, the entity is still required to record all such disclosures and make an accounting available to those patients who request it.[32]

---

26 CDC, *supra* note 15.

27 See 45 C.F.R. § 164.512(b)(i)(2008).

28 CDC, *supra* note 15.

29 Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,929 (Nov. 3, 1999). HHS defines "authorized by law" as a "term of art" denoting both permitted and mandated activity. Id.

30 CDC, *supra* note 15.

31 45 C.F.R. § 164.512 (2008).

32 CDC, *supra* note 15.

Despite the apparent permissive nature of the public health exception, considerable issues remain. Literally read, the regulations are broad and inclusive, yet they give rise to considerable confusion. The ultimate result of this uncertainty is a significant reluctance to provide public health authorities with needed information. As will be shown below, HHS provided little guidance in drafting the exception, but much of the ambiguity could be relieved by revisiting the regulations and clarifying their terms.

III. THE ABSENCE OF CLEAR STANDARDS FOR PHI COLLECTION

Public health surveillance, defined as "the continuing scrutiny of all aspects of occurrence and spread of a disease that are pertinent to effective control,"[33] is the primary means by which public health authorities build the "basic infrastructure necessary to effect many of the common goods of community health."[34] Surveillance frequently involves physician reporting of certain identified diseases or, alternatively, a request by a public health authority for physician or health care facility records on a patient or group of patients.[35]

Recent years have witnessed growth in the use of electronic health records and coordinated surveillance programs, and yet "clinical reporting remains a critical element in public health surveillance"[36] because it "allows [for] immediate public health response, including case investigation, contact prophylaxis, and outbreak control."[37] Unfortunately, obligations to report or turn over records "create tensions between physicians whose primary role is to protect their patients' interests and public health authorities, whose

---

33 Daniel M. Fox, *From TB to AIDS: Value Conflicts in Reporting Disease*, in PUBLIC HEALTH LAW AND ETHICS: A READER 300, 300 (Lawrence O. Gostin ed., 2002).

34 PUBLIC HEALTH LAW AND ETHICS: A READER 295, 295 (Lawrence O. Gostin ed., 2002).

35 *See* Fox, *supra* note 33; Sandra Roush et al., *Mandatory Reporting of Diseases and Conditions by Health Care Providers and Laboratories*, *in* PUBLIC HEALTH LAW AND ETHICS, *supra* note 34, at 300, 306 ("Historically in the United States, infectious disease surveillance has relied primarily on case reports from physicians and other health care professionals.").

36 PUBLIC HEALTH LAW AND ETHICS, *supra* note 34, at 299.

37 Roush et al., *supra* note 35, at 306.

primary role is to protect the population's interests."[38] Further, the information most useful to public health authorities is quite often the information with the most potential for causing embarrassment or a notion that privacy has been infringed upon.[39] "Data may reveal a person's lifestyle (e.g., sexual orientation), health status (e.g., mental illness, breast cancer, HIV), behaviors (e.g., unsafe sex or needle sharing), and familial health (e.g., genetics)."[40] Though there are clear and apparent tensions, if surveillance is not properly and consistently conducted, our "ability to detect and monitor infectious disease threats to health" is jeopardized.[41]

Public health officials have always faced obstacles in the collection of data needed for evaluating public health concerns and developing effective policy.[42] Agencies frequently suffer from a lack of funding at the state level, resulting in a loss of personnel for surveillance efforts.[43] Public health law aims to improve the health of the population as a whole by implementing policies, which require the cooperation of individual members of society.[44] However, citizens rarely see direct personal benefits from public health efforts because these activities are designed for aggregate well-being, as opposed to medical treatment which focuses on the individual patient.[45] The public does not perceive substantial gain from surveillance, though it can clearly see that such activities require an inquiry into personal medical histories.[46] As a result, patients and their health care

---

38 PUBLIC HEALTH LAW AND ETHICS, *supra* note 34, at 299; Fox, *supra* note 33, at 300 (discussing the history of doctors' struggles with surveillance policy, particularly in light of the AIDS epidemic).

39 *See* PUBLIC HEALTH LAW AND ETHICS, *supra* note 34, at 295.

40 *Id.*

41 Ruth L. Berkelman et al., *Infectious Disease Surveillance: A Crumbling Foundation, in* PUBLIC HEALTH LAW AND ETHICS, *supra* note 34, at 296-97.

42 PUBLIC HEALTH LAW AND ETHICS, *supra* note 34, at 12-14.

43 Berkelman et al., *supra* note 41, at 368 (noting public health agencies have reported a reluctance to add diseases to their mandatory reporting lists because of a lack of capacity for conducting surveillance on these diseases).

44 *Id.*

45 Gostin, *supra* note 2, at 7.

46 *See* PUBLIC HEALTH LAW AND ETHICS, *supra* note 34.

providers are reluctant to release private information.[47] Thus, there was cognizable difficulty in gathering needed surveillance data before the promulgation of HIPAA, and despite HHS's attempts to broaden the means by which public health authorities could access this information, the terms of the regulations have exacerbated the problem.

The implementation of the HIPAA Privacy Rule has had a significant impact on covered entities and the way private health information is managed. Hospitals and physicians, concerned with compliance, have reevaluated the manner in which data is stored and disseminated, resulting in reluctance to release PHI to any third party for any reason. This is true even where HHS included specific exceptions to the rule in furtherance of social policy.

Fear of investigation and penalty by HHS is so palpable that public health officials have encountered this precise issue, finding that "success in gaining access to personal health data has been mixed."[48] Though there is an exception carved out of the Privacy Rule for the release of PHI for public health purposes, the terms for release are unclear and leave significant room for interpretation.[49] The "regulations are drawn in complex and ambiguous terms, inviting future questions or controversies as to whether specific disclosures made without the individual's consent or authorization were, in fact, permitted by the regulations."[50] Because authorities are not required to be acting pursuant to a specific statute or as part of a known surveillance project, covered entities are left with uncertainty

---

47 *Id*.

48 Michael A. Stoto, *Public Health Surveillance in the Twenty-First Century: Achieving Population Health Goals While Protecting Individuals' Privacy and Confidentiality*, 96 GEO. L.J. 703, 713 (2008) ("Varying interpretations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule are at the heart of the problem.").

49 *Id*. at 714.

50 Andrew S. Krulwich & Bruce L. McDonald, *The Vulnerability of HIPAA Regulations to First and Fourth Amendment Attack: An Addendum to "Evolving Constitutional Privacy Doctrines Affecting Healthcare Enterprises,"* 56 FOOD & DRUG L.J. 281, 286 (2001). Notably, two such "controversies" over the constitutionality of disclosures pursuant to the Privacy Rule's exceptions arose even before implementation of the Rule. *See* Ass'n of Am. Physicians & Surgeons v. U.S. Dep't of Health & Human Servs.,224 F. Supp. 2d 1115 (S.D. Tex. 2002), *aff'd*, 67 Fed. Appx. 253 (5th Cir. Tex. 2003). However, the case was dismissed for lack of ripeness because the Rule was in a pre-enforcement stage.

and unanswered questions when asked to turn over the records of their patients and customers.[51] Coupled with the caveat that release of PHI under the public health exception is merely permitted and not mandatory,[52] many covered entities and their attorneys make the decision not to release the requested information.[53] Though they are certainly aware of the importance of the work done by public health agencies, there is strong concern for confidentiality between health care provider and patient, and many covered entities choose to err on the side of caution.[54]

When presented with a request for PHI by a public health official, many covered entities have adopted a standard response: "when in doubt, just say no."[55] Decisions on HIPAA compliance are largely made by a covered entity's legal representation, and given the potential risk for accusations of violation, public health officials are far more likely to be turned away.[56] Authorities have been faced with instances where "covered entities cite the rule in refusing to provide data to researchers and health departments."[57] The permissive nature of the exception is most certainly favorable because it allows covered entities to provide their patients with greater privacy if they so desire. This documented unwillingness to release data could be easily overcome by building stronger privacy protections into the public health exception, ultimately encouraging the exchange of information without resorting to coercion.

The continued use and current interpretation of the Privacy Rule for guidance may have negative implications for public health efforts. "Data that is important, that was provided for decades, and that has

---

51 Standards for Privacy of Individually Identifiable Health Information, *supra* note 29.

52 See 45 C.F.R. § 164.512 (2008).

53 Myra Moran et al., *Applying Law to Front-Burner Issues: Living With the HIPAA Privacy Rule*, 32 J.L. MED. & ETHICS 73, 76 (2004) ("The providers' decisions are made by lawyers, whose job it is to minimize their clients' risk, not to improve public health.").

54 *Id*.

55 *Id*.

56 Stoto, *supra* note 48, at 713.

57 Stoto, *supra* note 48, at 713-14; *see also* Daniel Drociuk et al., *Health Information Privacy and Syndromic Surveillance Systems*, 53 MORBIDITY & MORTALITY WKLY. REP. (SUPP.) 221 (Sept. 24, 2004), *available at* http://www.cdc.gov/mmwr/preview/mmwrhtml/su5301a40.htm (last visited Mar. 26, 2008).

always been treated with respect, is now at a premium."[58] The ambiguous terms of the public health exception as currently written, then, present a serious problem for three groups: (1) covered entities focused on minimizing risk of violation; (2) public health officials struggling to obtain necessary data; and (3) the public which relies on state and local public health agencies to identify and control health hazards to the population.

The solution to the concerns of all three of these interests is to provide clearer, stronger protocol for the release of PHI to public health officials.[59] Though the regulations were drafted with the opposite intent, the minimal standards in their present form pose a potential hindrance to the work of public health agencies.[60] Given definitive, unambiguous requirements for dissemination, the interests of covered entities, public health officials, and the general public stand to benefit. Covered entities would feel secure in sharing information with state and local authorities, public health officials would be able to obtain vital data for surveillance and intervention efforts, and the public could feel safe in knowing that its privacy was respected while the general health of the population was protected. Simply put, the addition of further standards to the public health exception is a necessary step in striking the balance between privacy concerns and the maintenance of public health.

IV. PROPOSED AMENDMENTS

Finding the balance between patient privacy and the needs of public health authorities will require significant changes to the public health exception to the Privacy Rule. Though HHS intended to provide a broad, workable exception to public health agencies, the

---

58 Moran et al., *supra* note 53, at 76.

59 Gostin et al., *supra* note 10, at 1118-19 ("[P]rotecting the privacy of individually identifiable health information is important to achieving benefits for the population such as public health surveillance and longitudinal health research. As we (and others) have stated, protecting health information privacy (e.g., by providing individuals some control over their health data without severely restricting warranted uses of the data) directly improves the quality of health care and public health data (e.g., by encouraging individuals to fully utilize health services and cooperate with health agencies).").

60 Moran et al., *supra* note 53, at 76.

interpretation of such ambiguous regulations has led to uncertainty and a recognized reluctance to release PHI.[61]

Over the course of the last decade, leading public health authorities and scholars have collaborated to develop model legislation for public health activities and privacy practices.[62] These efforts have resulted in the Model State Public Health Privacy Act and the Turning Point Model State Public Health Act.[63] Together, these documents provide prototypes upon which state legislatures and public health departments can base legislation and policy.[64] Stronger privacy protections and justification requirements are at the heart of these rules, but they rely on state legislatures to enact their provisions in full in order to provide the optimum level of data security.[65] However, they do present sound designs for public health legislation, which could be substantially replicated for use in strengthening the terms of the Privacy Rule's public health exception.

Proposed changes to the exception presented in this paper will not alter the basic premise of the HHS regulations. The central goal will continue to be to allow public health authorities to obtain the information necessary to protect the population's well-being. However, further requirements for gaining access to this information should be added. These additions can be categorized into three classes: justification requirements, freedom of access, and disclosure requirements. As discussed below, these proposed amendments to the Privacy Rule will ensure the ability of authorities to conduct public health functions without unnecessarily infringing on the privacy of the individual.

---

61 *Id*.

62 MODEL STATE PUBLIC HEALTH PRIVACY ACT (1999), *available at* http://www.publichealthlaw.net/Resources/ResourcesPDFs/modelprivact.pdf (last visited Mar. 26, 2008); TURNING POINT MODEL STATE PUBLIC HEALTH ACT (2003), *available at* http://www.hss.state.ak.us/dph/improving/turningpoint/PDFs/MSPHAweb.pdf (last visited Mar. 26, 2008).

63 *Id*.

64 *Id*.

65 *Id*.

A. Justification Requirements

Criticisms of the ambiguity of the Privacy Rule's public health exception largely revolve around the lack of need for authorization or justification in obtaining vast amounts of personal health data. The exception as currently drawn allows public health officials to collect PHI without working under a specific statute or mandate and without a particular surveillance activity in mind.[66] Further, the covered entity asked to provide this information is left to rely solely on the word of the requesting official that the PHI is the minimum necessary.[67] Although the agencies are assuredly working to protect the public's health in the most effective way possible, the exception should require officials to present further justification and documentation before obtaining an individual's private medical history.

Upon requesting access to PHI, authorities should be required to establish a particular public health activity for which the information will be used and provide public notice of intent to collect the data for this purpose.[68] This purpose may include preventing a significant public health risk, a likely benefit for the individual subject or subjects, or conducting a specific epidemiological survey.[69] Further, this identified purpose should be authorized by the agency and presented to the covered entity upon the initial request.

This specific purpose should, of course, include the minimum amount of PHI necessary to meet the needs of the study.[70] A great deal of surveillance and epidemiological investigation can be successfully completed without personally identifiable information, but for those projects which necessitate the use of more patient-specific data, officials should seek review by the agency to gain assurance that minimal PHI will be requested.[71] With this added

---

66 CDC, *supra* note 15.

67 *Id*.

68 TURNING POINT MODEL STATE PUBLIC HEALTH Act § 7-101(a)-(b); Gostin et al., *supra* note 1, at 1926; MODEL STATE PUBLIC HEALTH PRIVACY ACT § 2-101(a),(c).

69 TURNING POINT MODEL STATE PUBLIC HEALTH ACT § 7-101(a)(1)-(3).

70 *Id*. at § 7-102(c); MODEL STATE PUBLIC HEALTH PRIVACY ACT § 3-102(b).

71 *Id*.

security, covered entities and the public may more reasonably rely on the requesting official, resulting in greater willingness to release patient records.

These requirements should, of course, be flexible in the face of a public health emergency. In the event that a public health crisis were to arise, covered entities should demonstrate a greater willingness to cooperate with public health authorities who have limited time and resources to gather needed information, and this may mean providing PHI without the justification that would otherwise be required as above.

The Model State Emergency Health Powers Act[72] provides a helpful framework for these situations. This model act restricts access to PHI during an emergency to those with a "legitimate need to acquire or use the information to: (1) provide treatment to the individual who is the subject of the health information; (2) conduct epidemiological research; or (3) investigate the causes of transmission."[73] Though the formalities of PHI collection may not be followed as usual, these limitations should control the flow of information during the period of a declared public health emergency. And because declared public health emergencies should last for only a brief period of time while authorities work to bring the crisis under control, the expanded access to PHI should only be temporary.

Because public health agencies work under general mandates to protect the population's health by whatever means are appropriate based on the threat presented, it would be ineffective and likely undesirable to require authorities to be working in accordance with a specific statute. However, establishing and gaining authorization for a definitive prevention or surveillance effort based on the minimum amount of PHI possible is a simple step that would provide covered entities assurance that disclosures will not violate the terms of the exception or the trust of their patients.

B. Freedom of Access

To provide further assurances of individual privacy in the work

---

72 MODEL STATE EMERGENCY HEALTH POWERS ACT (2001), *available at* http://www.aapsonline.org/legis/msehpa2.pdf (last visited May 5, 2008).

73 *Id*. at § 607(a).

of public health officials, the conditions of maintenance of PHI must be considered once the records are in the possession of the public health agency.[74] The current terms of the public health exception contain no provision regarding access to one's own PHI held by an agency, nor does it place limitations on the time period for which PHI can be stored and utilized by the collecting agency.[75] The public has a great interest in such details given that personal medical records are in question, and "subjects should have access to information about themselves with identifiers to other persons deleted," as well as "access to just procedures for correcting and amending their personal records."[76]

An individual member of the public should have freedom of access to any data about him or herself which is held or disclosed by a public health agency.[77] The Privacy Rule currently requires covered entities to provide such access and accountings to their patients and customers, and the same standards should apply to government agencies.[78] As written, the freedom of information requirements for covered entities allow individuals to obtain copies of the PHI held and amend any records to correct mistakes.[79] It is not unreasonable, then, to require similar accessibility to records held by public health agencies, particularly in a society that values transparency of government.[80] The same exceptions for unreasonable requests would, of course, apply,[81] but public concern for invasions of privacy could be assuaged by allowing individuals to inspect records in agency possession. And if the minimum amount of PHI necessary to complete a project is collected, information about any particular citizen should be nominal, creating only a small burden on the agency.

---

74 Gostin et al., *supra* note 1, at 1926; TURNING POINT MODEL STATE PUBLIC HEALTH ACT § 7-104(a); MODEL STATE PUBLIC HEALTH PRIVACY ACT § 6-101 – 102.

75 45 C.F.R. § 164.512 (2008).

76 Gostin et al., *supra* note 1, at 1926.

77 TURNING POINT MODEL STATE PUBLIC HEALTH ACT § 7-105(a).

78 45 C.F.R. §§ 164.524, 164.528 (2008).

79 *Id*.

80 Gostin et al., *supra* note 1, at 1926.

81 TURNING POINT MODEL STATE PUBLIC HEALTH ACT at § 7-105(b).

Additionally, an amendment to the exception should address the length of time PHI may be reasonably held by a public health agency.[82] PHI may certainly be useful in studying trends in the public's health, but the identifying information is generally useful only for the initial period of investigation. The comments to § 3-104 of the Model State Public Health Privacy Act reflect this view. Its framers reject the argument "that there is an inherent value to having identifiable information when the use of the information no longer serves a legitimate public health purpose," concluding that the PHI "must be permanently destroyed, deleted, or made non-identifiable" upon completion of the authorized use.[83] After the completion of the previously identified purpose, officials should be required to expunge records of any and all personal identifiers.[84] Aggregate data compiled based on obtained PHI may certainly continue to be useful and should be maintained, but personal identifiers should be properly disposed of when no longer in use.

C. Disclosure Requirements

A final necessary change to the Privacy Rule's public health exception arises with the issue of propriety or secondary disclosure of PHI once in the hands of public health officials. Though public health agencies certainly have a vested interest in the collection and use of PHI,[85] there remains a concern as to the possibility of secondary uses not contemplated at the time of collection, as well as third party access to the information.[86]

The exception currently provides no directives to public health agencies on proper terms for disclosure of PHI already in possession of public health officials.[87] Once an agency receives the requested PHI from a covered entity, officials seemingly have complete discretion as to when and how the data will be used or disseminated in the future,

---

82 *Id*. at § 7-102(g); MODEL STATE PUBLIC HEALTH PRIVACY ACT § 3-104.

83 MODEL STATE PUBLIC HEALTH PRIVACY ACT at § 3-104.

84 *Id*.

85 James G. Hodge, Jr., *Health Information Privacy and Public Health*, 31 J.L. MED. & ETHICS 663, 663 (2003) (describing PHI as the "lifeblood of public health practice").

86 TURNING POINT MODEL STATE PUBLIC HEALTH ACT, supra note 62, at § 7-103(e).

87 *See* 45 C.F.R. § 164.512 (2008).

subject, of course, to state law.[88] "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."[89] As long as state law allows "the sharing of data by public health authorities across state boundaries, or among agencies within the state, these exchanges may continue unabated by the Privacy Rule."[90] Public agencies are not covered entities and are thus exempt from the requirements of the Privacy Rule.[91] As a result, private citizens are left with little assurance that their personal medical histories will be kept confidential and used solely for the purpose of protecting public health.

As previously discussed, the rationale behind HHS' decision to carve out an exception for public health purposes was in recognition that agencies would be unable to conduct classic surveillance and investigative activities if covered entities were restricted from disclosing PHI for use in these efforts.[92] The exception does not contemplate utilization of this information for purposes not related to the protection of the population's well-being; nevertheless, unintended secondary use is a possibility.[93] "In light of the liberal rules for supplying public health information to the agencies, the biggest privacy and security issues going forward are likely to arise in the largely unregulated instances once the public health agencies have received the data."[94]

In addition to the requirement that PHI be collected only for a specified public health activity with the narrowest information possible, an amendment to the public health exception should prohibit secondary uses. Any and all uses of the data not related to the purpose of original collection should be restricted. The only exception would be in the event that a public health official wanted

---

88 Hodge, *supra* note 85, at 669.

89 *Id*.

90 *Id*.

91 *Id*. at 668; see also Diana M. Bonta et al., *The HIPAA Privacy Rule: Reviewing the Post-Compliance Impact on Public Health Practice and Research*, 31 J.L. MED. & ETHICS 70, 71 (2003).

92 CDC, *supra* note 15.

93 45 C.F.R. § 164.512 (2008); Hussong, *supra* note 17, at 472.

94 Swire & Steinfeld, *supra* note 18, at 1529.

to utilize previously collected PHI for another narrowly-tailored public health purpose duly authorized by the agency.[95] Under these circumstances, the continued use of PHI already in the possession of the agency could minimize any further collection of private medical records and is desirable as such. For any other purpose, however, the disclosure of PHI in the hands of public health officials should be specifically prohibited without the informed consent of the individual.[96] Without this caveat, the policy rationale behind the public health exception breaks down, allowing for exactly the type of invasion of privacy the Privacy Rule purports to eliminate.

Secondary disclosures[97] are worrisome in two primary contexts. First, there is the potential for internal or external use of previously collected PHI in later studies or even human subjects research.[98] Second, PHI originally collected by public health officials is subject to disclosure to external third parties who would otherwise have no access to such data.[99] Of particular concern are other government agencies whose use of the information likely has little or no relation to the purpose for which the PHI was originally collected. As discussed below, these secondary uses should be regulated within the terms of the public health exception. Without further guidance, there is a substantial risk of unnecessary infringement of personal privacy as well as violation of the public's trust.

1. Human Subjects Research

Public health agencies act in a number of capacities in an effort to identify risks and improve current conditions.[100] Classic public health activities are essential to society and are often specifically authorized

---

95 MODEL STATE PUBLIC HEALTH PRIVACY ACT § 3-101(b)-(c)(1999).

96 *Id*. at § 4-101.

97 Secondary disclosure is defined as any "disclosure of data for purposes beyond those used to justify the original collection." Gostin et al., *supra* note 1, at 1925.

98 James G. Hodge, Jr., *An Enhanced Approach to Distinguishing Public Health Practice and Human Subjects Research*, 33 J.L. MED. & ETHICS 125, 125 (2005); Gostin et al., *supra* note 1, at 1925, 1927.

99 Gostin et al., *supra* note 1, at 1926-27.

100 Hodge, *supra* note 98, at 125.

by law.[101] However, a risk to personal privacy arises when authorities engage in extended use of PHI, which may "resemble, include, or constitute human subjects research."[102] Human subjects research "is legally defined as 'a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge' that involves living human subjects (or their identifiable private data)."[103] This category of research is differentiated from classic public health activities in that it generally requires the informed consent of the individual subjects as well as approval by an institutional review board (IRB).[104] Unfortunately, "a host of public health activities that are not neatly characterized as either practice or research" are "[l]ost in a legal and ethical gray zone."[105]

In order to preserve the privacy of individuals and their PHI, authorities must ensure that any extended use of data already in possession does not cross the line between authorized public health activities and human subjects research.[106] "If the primary intent changes, what is initially deemed public health practice can become public health research."[107] In the case that a question arises as to how a particular activity is to be categorized, authorities should err on the side of caution and obtain IRB approval.[108] Further, an amendment to the public health exception should specify that any human subjects research intended or later conducted by the agency or any third party is prohibited unless consent is obtained from the subjects involved. There is currently a separate exception to the Privacy Rule designed to assist researchers in obtaining needed data, subject to prior approval by an IRB or privacy board.[109] Without these added conditions to the public health exception, the requirements of the

101 *Id*.

102 *Id*.

103 *Id*.

104 *Id*. at 125-26.

105 Hodge, *supra* note 98.

106 *Id*.

107 *Id*. at 128.

108 TURNING POINT MODEL STATE PUBLIC HEALTH ACT § 7-102(f)(1)-(6)(2003).

109 45 C.F.R. § 164.512 (2008).

research exception are essentially undermined. Public health authorities or third party researchers could simply obtain the desired PHI under the guise of the public health exception to avoid IRB review and conduct human subjects research without the subjects' knowledge or approval. Such unethical conduct is counter to the purpose of the Privacy Rule, and it erodes any assurances of confidentiality provided by covered entities to their patients.

2. Government Agency Access

Another concern for secondary use of PHI after collection under the public health exception is disclosure to other government agencies.[110] Because no restrictions on dissemination to non-public health agencies are included in the exception, there remains a strong possibility that state and local authorities not engaged in public health practice could obtain and make use of personal medical data, with potential for "negatively affect[ing] an individual's job status or opportunities, insurability, and social status."[111] This possibility undermines the public's trust as well as the reason for the exception because "providing access to protected health information to any person other than a public health agency or public health official is not a use" within the meaning of the regulations.[112] When approached by public health authorities, covered entities may take into account potential "downstream" uses of the PHI, considering the ways in which disclosed information will be subsequently used by the public entity."[113] If a covered entity perceives that the PHI will be utilized in investigations or studies beyond public health purposes, there may be added reluctance to provide requested records. Further, had HHS intended for other government agencies to be given access to PHI, separate exceptions arguably would have been written into the Rule.

---

110 Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439, 1470 (2002).

111 *Id.* at 1470, 1475 (also noting "DHHS's privacy regulations arguably make it too easy for unauthorized disclosures to police to take place."); *see also* Van Der Goes, Jr., *supra* note 9 (discussing the relationship between the Privacy Rule and the Fourth Amendment).

112 MODEL STATE PUBLIC HEALTH PRIVACY ACT § 3-101(a)(1999).

113 Bonta et al., *supra* note 91, at 72.

As currently drawn, the exchange of PHI between government agencies is entirely plausible, subject to state law restrictions.[114] Exchanges between state and local public health agencies are desirable inasmuch as there is great potential for benefits to public well-being.[115] Disclosure of PHI to other types of agencies, however, is beyond the scope of the intended purposes for collection and should be prohibited.[116] PHI is sensitive, potentially embarrassing information, and government agencies not involved in the maintenance and protection of public health should not have access to the information collected by public health authorities.[117] It is certainly possible that federal agencies, law enforcement officials, or judicial or administrative proceedings may take an interest in such information, but HHS included specific exceptions to allow those entities access to PHI under certain conditions.[118] Other government agencies should not be permitted to undercut the requirements for disclosure by covered entities by encroaching on public health data.

The public health exception was designed to allow public health authorities to continue their work as it had been conducted before the Privacy Rule was enacted, and disclosures for "law enforcement [and] judicial and administrative proceedings . . . do not serve to improve individual and public health outcomes."[119] HHS did not contemplate secondary disclosure for research or alternative government use when it drafted the public health exception, so these activities should be explicitly prohibited. The public's trust and reliance on public health officials rests on the assumption that obtained PHI will be kept confidential and used only for public health activities. The possibility that the exception could be used for other purposes undermines that trust and erodes the willingness of individuals and covered entities to permit the disclosure of PHI.

---

114 Swire & Steinfeld, *supra* note 18, at 1529; Gostin et al., *supra* note 110, at 1470.

115 Gostin et al., *supra* note 1, at 1925; MODEL STATE PUBLIC HEALTH PRIVACY ACT § 2-102.

116 MODEL STATE PUBLIC HEALTH PRIVACY ACT § 4-101.

117 Gostin & Hodge, *supra* note 110, at 1470.

118 MODEL STATE PUBLIC HEALTH PRIVACY ACT § 4-104-105.

119 Gostin et al., *supra* note 24, at 28.

V. CREATION OF A CLEARER, STRONGER FEDERAL STANDARD

The HIPAA Privacy Rule has been described as a "floor" for privacy protections,[120] which HHS believes "balance[s] the needs of the individual with the needs of the society."[121] State law is not preempted, and state legislatures are free to implement measures to provide further requirements for disclosure of PHI by covered entities.[122] This is an especially desirable aspect of the Privacy Rule because it allows citizens to control how much or how little of their private medical information is available and allows state and local agencies to "address a population's specific needs."[123]

State law, however, is so widely varied in terms of privacy protections currently in place[124] that "some public health officials support federal preemption, claiming that uniformity is necessary and that federal law should provide strong patient protection."[125] How much privacy an individual has depends largely on his state of residence, and "the legal protection of health privacy is uneven, not simply across state lines, but within them."[126] Though state control is an advantageous approach, weak federal guidelines do a disservice to the nation's population:

> Independent evolution of state law has produced considerable variation and inconsistency. Variability, of course, can be a strength in a federal system of government, allowing state experimentation with complex issues. Variability in surveillance and privacy protection, however, creates problems in an increasingly mobile society in which disease outbreaks may erupt rapidly in several states, requiring

120 Gostin & Hodge, *supra* note 110, at 1441.

121 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000).

122 45 C.F.R. § 160.202-.203 (2008).

123 Hussong, *supra* note 17, at 469.

124 Gostin et al., *supra* note 3, at 111 ("States generally provide some protection to health data collected for public health purposes, though the grading of the offense varies greatly. Most states treat violations as a misdemeanor, while a few punish official violators by dismissal, and some provide no penalty at all.").

125 Hussong, *supra* note 17, at 469.

126 Gostin et al., *supra* note 3, at 111.

systematic and consistent collection of comparable data sets.[127]

Due to this incongruent accumulation of legislation, the privacy an individual enjoys in one state may be entirely altered if he moves to another state or simply crosses state lines to seek medical treatment.[128] Thus, there is an identifiable need for a raising of the "floor" in the public health exception.

The exception in its current form provides only ambiguous terms and no guidance as to the use of PHI once in the possession of public health authorities. Model rules for privacy protection and the suggestions for amendment discussed in this paper will have little to no impact if not uniformly adopted and implemented in every jurisdiction. As one scholar noted, "When the law is comprehensive and well-considered, it can provide substantial protections."[129] However, when it "fail[s] to provide clear criteria and useful sanctions," it has the potential to "hamper public health work in a variety of ways."[130] In order to ensure that basic privacy protections are uniform in every state, regulations for justification, access, and disclosure must be added to the HIPAA public health exception as standardized national criteria in the form of a "single, strong federal law."[131]

There has been some suggestion that HHS lacked the authority needed to implement such regulations at the time of drafting the original Rule.[132] Accordingly, Congressional authorization may be necessary before clearer guidelines for public health agencies could be promulgated. "Despite the virtues of state privacy laws, the public is calling for Congress to take action. The 'patchwork system' of state privacy laws does not afford comprehensive privacy protection, and so Congress must provide additional protection through

---

127 Gostin et al., *supra* note 1, at 1925.

128 *Id.* ("Data sent from state to state do not receive reliable privacy and security protection. Moreover, individuals who relocate across state lines cannot expect continuity in privacy protections of publicly held health information.").

129 Van Der Goes, Jr., *supra* note 9, at 1047.

130 Gostin et al., *supra* note 3, at 116.

131 Van Der Goes, Jr., *supra* note 9, at 1012.

132 Gostin et al., *supra* note 3, at 125-26.

comprehensive federal legislation."[133]

State law preemption for privacy regulations should remain the standard for PHI disclosures. However, the only way to ensure the privacy of personal medical records in the hands of public health authorities is to strengthen the existing regulations. Without further standards at the national level, the individual is left with incomplete and inadequate protections, and public health officials will continue to encounter reluctance when soliciting PHI.

VI. CONCLUSION

In promulgating and implementing the HIPAA Privacy Rule, HHS intended to provide patients with the greatest level of privacy protection possible while allowing government agencies to continue to function for the benefit of the population. Though well-intentioned, the attempt fell short of optimal design. Covered entities received clear guidelines as to dissemination of records in the private sector, but the protocol regarding release to public health officials were drafted in a way which has great potential for causing confusion. Public health officials faced significant obstacles in gathering needed data before the introduction of HIPAA, and, unfortunately, the Privacy Rule has only created an additional barrier. When HHS constructed the terms of the public health exception, it had an opportunity to both ensure privacy and ease the burden of public health authorities. Unfortunately, the agency missed the mark. In creating broad and seemingly permissive regulations, HHS actually added to the difficulties faced in gathering public health data. Had the Rule given stronger, clearer protocol for public health officials and covered entities to work from, HIPAA may have improved health conditions on an aggregate, rather than individual, level.

In its current state, the public health exception to the Privacy Rule lays the groundwork for an ideal federal privacy rule, but in order to strike a balance between privacy and public health needs, Congress and HHS must revisit the regulations and formulate clearer guidance. Improved regulations should include requirements for

---

[133] Gostin et al., *supra* note 24, at 14.

justification of PHI collection, freedom of access by individual citizens, and restrictions on secondary disclosure. If these terms can be added to the exception in the form of strong federal legislation to harmonize protections nationwide, all interests involved stand to benefit. Covered entities could release data to public health officials free from fear of liability, and public health agencies could collect essential information. Most importantly, the nation's population would have improved privacy assurances in addition to well-equipped public health departments. Though it may seem counter-intuitive, more stringent protocol for collection of personal medical information actually has the potential for improving overall health conditions.

As noted by one scholar,

> Perhaps what the public desires is not absolute privacy, but reasonable assurances that when personal information is collected, public health authorities will treat the information with respect, store it in an orderly and secure manner, and disclose it only for important health purposes and in accordance with publicly accountable principles of fairness.[134]

If a balance can be struck with these principles in mind, we may find a way to protect the integrity of each individual, both physically and psychologically.

---

[134] Gostin et al., *supra* note 1, at 1927.