



# Rapid Public Health Policy Response Project

February 2009

School of Public Health and Health Services

## Patient Privacy in the Era of Health Information Technology: Overview of the Issues

THE GEORGE  
WASHINGTON  
UNIVERSITY  
MEDICAL CENTER  
WASHINGTON DC



URL: [www.gwumc.edu/sphhs/about/rapidresponse/index.cfm](http://www.gwumc.edu/sphhs/about/rapidresponse/index.cfm).



## Patient Privacy in the Era of Health Information Technology

---

### About this Paper

Congress is poised to include some \$20 billion for health information technology in the pending economic stimulus package. While sharing patient data electronically has the potential to improve health care quality and save money, it also raises significant concerns about patient privacy.

“No one thinks existing HIPAA privacy rules are fine the way they are, but there is disagreement on what the problems are and how to fix them,” observes Phyllis C. Borzi, JD, MA, research professor at the School of Public Health and Health Services at The George Washington University. “Many consumer groups and patient advocates say the rules are way too lax. The industry people say they are barriers to creating effective health information systems and need to be loosened.”

The Privacy Rule implemented under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides the only national legal standard for protecting the use of health information. This paper reviews the scope of that law, the proposed privacy requirements in the stimulus legislation, and the perspectives of industry and consumer groups on electronic health information privacy.

### For more information about the issues raised in this paper, contact:

Phyllis C. Borzi, JD, MA, Research Professor  
Department of Health Policy  
School of Public Health and Health Services  
The George Washington University  
2021 K Street, N.W., Suite 800  
Washington, DC 20006  
(202) 530-2312  
borziph@gwu.edu

### About the Rapid Health Policy Response Project

The Rapid Health Policy Response Project of the School of Public Health and Health Services at The George Washington University presents data and other background information on breaking public health stories. The goal is to educate the public, policymakers, legislators, health care providers, the media and others in order to promote informed decisionmaking.

Karyn Feiden, an independent consultant who writes about public health and health care, provides editorial support for this project. Financial support comes from the Public Health and Policy Group of Pfizer, Inc., which provides no input into the content of these reports.

# Patient Privacy in the Era of Health Information Technology: Overview of the Issues

The economic stimulus package working its way through Congress allocates some \$20 billion for health information technology (HIT), reflecting the belief that electronic information systems that provide shared access to patient data have the potential to reduce fragmentation in the health care system and improve the quality of care in a cost-effective manner.<sup>1</sup>

But computerized medical information also raises significant concerns about patient privacy. “No one thinks existing HIPAA privacy rules are fine the way they are, but there is disagreement on what the problems are and how to fix them,” observes Phyllis C. Borzi, JD, MA, research professor at the School of Public Health and Health Services at The George Washington University. “Many consumer groups and patient advocates say the rules are way too lax. The industry people say they are barriers to creating effective health information systems and need to be loosened.”

This paper reviews the privacy protections currently applicable to electronic health information, their scope and limitations, and industry and consumer perspectives on proposals for revising them.

## A Primer on Health Information Technology

Health information technology provides opportunities for physicians, hospitals, pharmacists, and other health care providers to share patient information electronically, and makes medical records available to patients themselves.<sup>2</sup>

The Congressional Budget Office describes health information technology as “applications specifically designed for the practice of clinical medicine, including electronic health records, personal health records, health information exchange, computerized physician order entry, clinical decision support systems, and electronic prescribing.”<sup>3</sup> At the heart of HIT is an electronic record capturing critical demographic, health, and health care information on individual patients, the contents of which can be shared.

Beginning with an Executive Order in 2004, the federal government set a goal of having electronic medical records in widespread use by 2014 so that medical information can accompany a patient across providers and the health care system.<sup>4</sup> Such records, coupled with the many other components of a health information infrastructure, offer the promise of generating “richer, cheaper and more relevant clinical information” that can be used to:<sup>5</sup>

- ▶ Promote an evidence base for clinical practice and influence decisionmaking.
- ▶ Improve communication and reduce errors in clinical settings.
- ▶ Streamline administrative processes.
- ▶ Measure performance at the level of the individual health care professional and the health care institution, and by community and geographic location.

- ▶ Increase transparency in the health care system by alerting providers and patients to variations in performance.
- ▶ Give payers far better information on cost and quality in order to introduce greater efficiencies into health care purchasing
- ▶ Shed greater light on racial, ethnic, and socioeconomic disparities in health care population health outcomes.
- ▶ Provide greater integration between health care and public health surveillance and health promotion. For example:
  - State and local health departments can use aggregated data, stripped of information that identifies individuals, to track community health issues, assess the prevalence of chronic diseases, and prepare for emergencies.
  - Patient registries can permit public health agencies to target supportive self-management and health education services to individuals with chronic health problems, such as advanced diabetes, or to parents of children with conditions such as asthma.

A limited number of studies have documented quality improvements and cost savings from health information technology.<sup>6</sup> But widespread HIT adoption still faces significant challenges, particularly at the physician and hospital level, where it may matter most. Only 4 percent of physicians had fully functional electronic medical records systems in 2007, according to a study supported by the Office of the National Coordinator for Health Information Technology, a part of the Department of Health and Human Services (HHS).<sup>7</sup>

The U.S. Government Accountability Office (GAO), which has been tracking the evolution of HIT, reported to a Senate committee in mid-January that progress had been made but that uncompleted efforts could still jeopardize success.<sup>8</sup> In particular, the GAO called for additional emphasis on:

- ▶ Defining, adopting, and implementing standards that allow information to be shared.
- ▶ Strengthening management and planning activities and developing more comprehensive milestones and performance measures.
- ▶ Developing an overall approach to privacy that provides policies and guidance to stakeholders and ensures that all key privacy principles and challenges are addressed.

Limitations of current approaches to health information technology were also highlighted in a recent report by the National Research Council, based on the experiences of eight medical centers considered leaders in the field.<sup>9</sup> The report called for a greater commitment to help clinicians make sense of the vast amounts of raw data becoming available to them, rather than primarily on using the data to comply with regulations and defend against lawsuits.

# Patient Privacy in the Era of Health Information Technology

---

## The Federal Privacy Rule and HIT

Whatever the stumbling blocks, the use of health information technology is clearly growing, and the American public is rightly concerned about who will have access to personal health information.<sup>10</sup>

As the contents of electronic health records are more widely shared, the risk rises that stigmatizing disclosures could impact employment status, access to health insurance and other forms of insurance, participation in community activities, and more. Researchers have also noted that patients may engage in “privacy protective behaviors,” avoiding screening tests, treatment, or participation in research protocols if they are not confident that privacy protections will adequately safeguard their medical information.<sup>11</sup>

The Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides the current national legal standard for protecting the use of health information held by “covered entities,” which are defined as health plans, health care clearinghouses, and health care providers who transmit health information. Researchers from GW’s School of Public Health and Health Services have highlighted several notable features of HIPAA’s privacy framework:<sup>12</sup>

- ▶ The HIPAA Privacy Rule distinguishes between mandatory and permitted disclosures of health information, with health professionals given significant discretion to determine what disclosures are permissible. The only mandates are that patients have access to their own health information and that data are available to the Department of Health and Human Services for compliance and enforcement activities.
- ▶ The remaining “allowable” disclosures divide into those that require patient consent and those that do not. Most importantly, no patient authorization is required for a wide array of health care information exchange related to treatment, payment, and health care operations.
- ▶ Federal standards apply if state laws are “contrary” to HIPAA’s privacy standards, but the states are allowed to establish “more stringent” privacy protections than those recognized under federal law. For example, a state might prohibit the exchange of personal health information for payment purposes without specific consent. The number of states that actually maintain more stringent standards is unclear.
- ▶ State privacy laws vary considerably in their reach and focus. Some state laws are substantially more comprehensive than others, and some apply to a broader set of actors in health care. Different states may have laws targeting specific diseases, types of information, or populations (for example, specific provisions may apply to HIV, sexually transmitted diseases, or substance use).

(For a fuller description of HIPAA, including provisions regarding authorized uses of personal health information, limitations to its use, notification requirements, the right to amend the record, marketing, enforcement, and more, see the Department of Health and Human Services summary.<sup>13</sup>)

## The Continuing Debate

A number of questions have been raised about the reach and structure of the existing HIPAA Privacy Rule, and the need for additional privacy protections. The Health Information Technology for Economic and Clinical Health Act, passed by the U.S. House of Representatives on Jan. 29, 2009 as part of the economic stimulus package, expands on existing protections, as described in the Appendix to this report.<sup>14</sup>

Among the key issues:

- ***Should the federal government preempt the states?*** At present, the HIPAA Privacy Rule provides a federal “floor” on health information privacy, but not a “ceiling.” In general, industry groups favor a uniform national standard, while consumer advocates want states to be able to enact tighter standards if they choose to do so.
  - The Health Care Leadership Council, which represents hospitals, health plans, pharmaceutical companies, and other private sector health entities, argues that a patchwork of state privacy laws complicates compliance.<sup>15</sup> Calling the many state standards “a serious impediment to sharing information in the context of a national health information network,” the Council has urged Congress to preempt state privacy laws.
  - Judicial history suggests that concern may be misplaced. After reviewing 500 HIPAA-related court decisions from 1996 to 2006, GW School of Public Health and Health Services researchers concluded there is “no evidence that allowing more stringent state laws to be enforced impedes providers’ access to essential patient information. Nor does it create obstacles to the use of such information to improve quality ...”<sup>16</sup>
  - The Center for Democracy & Technology’s Health Privacy Project emphasizes that state privacy laws are often enacted to meet specific local needs. Moreover, these laws may be incorporated into broader legislation, such as that guiding HIV testing or public health reporting. “Eliminating only the privacy provisions of such laws would compromise their integrity,” according to analysts.<sup>17</sup>
- ***Who should comply with HIPAA?*** HIPAA applies only to the legally defined covered entities, not to any entity with access to electronic health information. Companies known as “business associates,” which contract with covered entities for tasks that give them access to health data, are not directly subject to federal privacy laws, although they have a contractual obligation to comply.<sup>13</sup>

Google, WebMD, and other vendors that offer commercial services to help consumers consolidate medical information from multiple providers into electronic personal health records fall outside HIPAA’s jurisdiction. Although some have chosen to comply with the Privacy Rule, they are not mandated to do so.<sup>5</sup>

## Patient Privacy in the Era of Health Information Technology

In general, there is agreement that a consistent set of principles must guide privacy and security in electronic health information exchange. In offering guidelines for a “nationwide privacy and security framework,” the Office of the National Coordinator for Health Information Technology has stated: “These principles are expected to guide the actions of all health care-related persons and entities that participate in a network for the purpose of electronic exchange of individually identifiable health information.”<sup>18</sup>

The mechanisms through which this should happen are subject to some debate:

- The Consumer Partnership for eHealth, a coalition of labor and consumer groups, has called for applying HIPAA provisions to business associates.<sup>19</sup> However, an industry privacy expert has argued that HHS itself can not regulate business associates, and that the department’s only enforcement mechanism is to pursue covered entities who do not execute appropriate contracts.<sup>20</sup>
- The Center for Democracy & Technology has recommended that more specific language be written into the pending economic stimulus legislation so that any entity receiving federal funds for health information technology — whether or not it is subject to HIPAA — is held legally accountable for adhering to core privacy protections.<sup>21</sup>

The pending stimulus legislation would broaden the obligations of business associates and move towards greater uniformity in compliance with privacy rules.<sup>1</sup>

- ***Should consumer consent be required?*** Under the HIPAA privacy rule, covered entities can “use and disclose” personal health information without patient authorization for treatment, payment, and health care operations, such as quality assessment, underwriting activities, audits, and business planning. (A significant exception is in place for psychotherapy notes.) Disclosure is also permitted for certain oversight, judicial, and public health purposes, among others.<sup>13</sup>

Industry has generally opposed broader consent requirements for the sharing of health information. The original draft of the HIPAA Privacy Rule would have required prior consent for most uses of patient information, but industry fought successfully to change that, arguing that it “would hinder the delivery of treatment, the processing of payments and other routine activities.”<sup>22</sup> The consent mandates in other pending legislation — including the PRO(TECH) Act of 2008 (HR 6357) and the Health Information Privacy and Security Act (SB 1814) — have generated similar concerns.<sup>23</sup>

Privacy-focused consumer groups differ on the priority they place on consent:

- The Center for Democracy & Technology supports a strategy that enables information-sharing without consent for a defined set of core activities, while requiring consent beyond that core. “Consent is not the *sine qua non* of privacy protection,” notes the center, because it “relieves the holders of patient data of the responsibility for adopting comprehensive privacy protections” and places undue burdens on individuals.<sup>22</sup>

- The Coalition for Patient Privacy, a 35-member organization that includes the ACLU, the National Association of Social Workers, Consumer Action, and the Government Accountability Project, leans more towards consent requirements, emphasizing “an individual’s right to control how their personal information is used.” The coalition has called for a “federal right to health information privacy” and urged that “personal health information obtained for one purpose [not] be used for other purposes without informed consent.”<sup>24</sup>
- **Should other privacy standards be strengthened?**
  - **Marketing restrictions:** HIPAA currently prohibits disclosure for most marketing purposes without explicit consent, although significant exceptions exist to allow health plans to provide patient education and describe certain health-related products and services. Consumer groups support efforts to tighten the definition of marketing and to prohibit the sale of an individual’s health information without authorization.<sup>21,22,19</sup> (The pending stimulus legislation takes several steps in that direction.<sup>1</sup>)
  - **Notification of a security breach:** Consumer groups favor requirements that patients be notified if their health information has been breached.<sup>21,19</sup> The industry generally believes that a “risk-based standard” should apply such that notification would be required only where there is a “reasonable risk of substantial harm.”<sup>25</sup> (The pending stimulus legislation establishes a notification requirement in the event of a breach.<sup>1</sup>)
  - **Mandating an audit trail:** Consumer groups want expanded accounting so that patients can learn what health information about them has been disclosed, and to whom.<sup>21,19</sup> The industry has asserted that “even the most sophisticated health providers would struggle to maintain compliance with this costly and bureaucratic requirement.”<sup>25</sup> (The pending stimulus legislation requires entities using electronic records to track disclosures and make them available to patients.<sup>1</sup>)
  - **Enforcement and penalties:** Consumers groups have called for strengthening the enforcement provisions of privacy rules, and making more resources available to ensure compliance.<sup>21,19</sup> Industry has expressed particular concern about allowing an individual right of action, and giving state attorneys general increased jurisdiction over federal privacy laws.<sup>25</sup> (The pending stimulus legislation expands enforcement, and provides additional resources for it.<sup>1</sup>)

Industry and consumer groups both promote health information technology as a valuable tool for streamlining the health care system, improving quality, and controlling costs, and they agree that patient privacy is a legitimate concern. But as HIT gains traction, the best approaches to privacy protections remain contentious. The privacy provisions in the economic stimulus legislation pending before Congress add to the existing framework, but they are surely not the final word on this evolving subject.

### Appendix:

#### Privacy Protections in the Economic Stimulus Legislation

The Health Information Technology for Economic and Clinical Health Act, passed by the U.S. House of Representatives on Jan. 29, 2009 as part of the economic stimulus package, includes the following privacy protections, according to senior congressional staff:<sup>14</sup>

- ▶ Establishes a federal breach notification requirement for health information that is not encrypted or otherwise made indecipherable. It requires that an individual be notified if there is an unauthorized disclosure or use of their health information.
- ▶ Ensures that new entities that were not contemplated when the federal privacy rules were written, as well as those entities that do work on behalf of providers and insurers, are subject to the same privacy and security rules as providers and health insurers.
- ▶ Provides transparency to patients by allowing them to request an audit trail showing all disclosures of their health information made through an electronic record.
- ▶ Shuts down the secondary market that has emerged around the sale and mining of patient health information by prohibiting the sale of an individual's health information without the individual's authorization.
- ▶ Requires that providers secure authorization from patients in order to use their health information for marketing and fundraising activities.
- ▶ Strengthens enforcement of federal privacy and security laws by increasing penalties for violations and providing greater resources for enforcement and oversight activities.

### Endnotes

1. Title IV — Health Information Technology for Economic and Clinical Health Act.
2. See the [Health Information Technology Web site](#) of the Department of Health and Human Services.
3. Congressional Budget Office [letter](#) to Congressman Henry A. Waxman, Jan. 21, 2008 [*sic*; the letter was actually sent on Jan. 21, 2009].
4. Executive Order 13335. [Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator](#). *Federal Register* 2004 April 30; 69 (84).
5. [Health Information Technology in the United States: Where We Stand, 2008](#). Executive Summary. Produced by The Robert Wood Johnson Foundation, The George Washington University Medical Center and the Institute for Health Policy. 2008.
6. See, for example: Chaudhry B, Wang J, Wu S., Maglione M., et al. “[Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care](#).” *Annals of Internal Medicine* 2006;144:742-52. Amarasingham R., Plantinga L, Diener-West M, Gaskin DJ, Powe NR. “[Clinical Information Technologies and Inpatient Outcomes: A Multiple Hospital Study](#).” *Archives of Internal Medicine* 2009;169(2):108-14.
7. DesRoches CM, Campbell EG, Rao SR, Donelan K, et al. “[Electronic Health Records on Ambulatory Care – A National Survey of Physicians](#).” *New England Journal of Medicine* 2008;359:50-60.
8. U.S. Government Accountability Office. “[Health Information Technology: Federal Agencies’ Experiences Demonstrate Challenges to Successful Implementation](#).” Testimony before the U.S. Senate Committee on Health, Education, Labor and Pensions, Jan. 15, 2009. A series of earlier GAO reports has monitored the evolution of federal efforts to develop health information technology: “[Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy](#),” January 2007 (GAO-07-238). “[Health Information Technology: Efforts Continue but Comprehensive Privacy Approach Needed for National Strategy](#),” June 19, 2007 (GAO-07-988T). “[Health Information Technology: HHS is Pursuing Efforts to Advance Nationwide Implementation, but Has Not Yet Completed a National Strategy](#),” Feb. 14, 2008 (GAO-08-499T).

9. National Research Council. “Current Approaches to U.S. Health Care Information Technology are Insufficient.” Press release, Jan. 9, 2009. The full report is: Stead WW, Lin HS, eds. *Computational Technology for Effective Health Care: Immediate Steps and Strategic Directions*. Washington, DC: Committee on Engaging the Computer Science Research Community in Health Care Informatics, National Research Council 2009.
10. Markle Foundation. “Americans Overwhelmingly Believe Electronic Personal Health Records Could Improve their Health.” June 2008. Survey developed Professor Alan F. Westin, Professor of Public Law & Government Emeritus at Columbia University, and administered by Knowledge Networks.
11. Goldman J. “Protecting Privacy to Improve Health Care.” *Health Affairs* 1998 November/December; 17; (6):47-60. Privacy-protective behavior is not unique to electronic records, which is why special and highly protective rules have applied to information on addiction and mental illness for many years, as documented in Beckerman JZ, Pritts J, Goplerud E., Leifer JC, Borzi PC, Rosenbaum S. “Health Information Privacy, Patient Safety, and Health Care Quality: Issues and Challenges in the Context of Treatment for Mental Health and Substance Use.” *BNA’s Health Care Policy Report*, 16(2), Jan. 14, 2008.
12. Goldstein M, Repasch L, Rosenbaum S. “Emerging Privacy Issues in Health Information Technology.” In: *Health Information Technology in the United States: Where We Stand, 2008*. Produced by The Robert Wood Johnson Foundation, The George Washington University Medical Center, and the Institute for Health Policy at Massachusetts General Hospital. 2008.
13. Office of Civil Rights. “Summary of the HIPAA Privacy Rule.” Privacy Brief. Accessed Feb. 1, 2009.
14. Title IV — Health Information Technology for Economic and Clinical Health Act. Summary of privacy protections in the legislation, prepared by senior staff of the U.S. House Committees on Energy and Commerce; Ways and Means; and Science and Technology, Jan. 16, 2009.
15. Health Leadership Council. *HLC Outlook: Confidentiality of Patient Information*. Oct.10, 2008.
16. Rosenbaum S, Borzi PC, Burke T, Nath SW. “Does HIPAA Preemption Pose a Legal Barrier to Health Information Transparency and Interoperability?” *BNA’s Health Care Policy Report* 2007 March 19;15 (11). This analysis was conducted as part of The Robert Wood Johnson Foundation’s Legal Barriers to Health Information project.

17. Center for Democracy & Technology. Issue Brief: [HIPAA and Health Privacy: Myths and Facts: Part 2](#). Jan. 2009.
18. Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services [Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information](#), Dec. 15, 2008.
19. Consumer Partnership for eHealth letter to Secretary of Health and Human Services, Jan. 26, 2009.
20. Nahra KJ. “[Are Troublesome HIPAA Changes on the Way?](#)” *Privacy & Data Security Law Journal* 2008 July.
21. McGraw D. “[Health IT: Protecting Americans’ Privacy in the Digital Age.](#)” Center for Democracy & Technology statement before the U.S. Senate Judiciary Committee, Jan. 27, 2009.
22. Center for Democracy & Technology. “[Rethinking the Role of Consent in Protecting Health Information Privacy.](#)” Jan. 2009.
23. See, for example, Confidentiality Coalition [letter](#) to the House Subcommittee on Health, Committee on Energy and Commerce, June 24, 2008, arguing that under the terms of the PRO(TECH) Act, “physicians, hospitals, pharmacists, and other providers would be unable to perform vital functions within health care operations.”
24. Coalition for Patient Privacy [letter](#) to Representative Nancy Pelosi and Senator Harry Reid, Jan. 14, 2009. See also Patient Privacy Rights [Web site](#).
25. Confidentiality Coalition [letter](#) to Senator Harry Reid and Representative Nancy Pelosi, Dec. 19, 2008.