Old before its time: HIPAA and e-health policy

R Cunningham

Health Affairs 19, no.6 (2000):231-238
doi: 10.1377/hlthaff.19.6.231

The online version of this article, along with updated information and services, is available at:
http://content.healthaffairs.org/content/19/6/231.citation

For Reprints, Links & Permissions : http://content.healthaffairs.org/1340_reprints.php

Email Alertings : http://content.healthaffairs.org/subscriptions/etoc.dtl

To Subscribe : https://fulfillment.healthaffairs.org
Old Before Its Time: HIPAA And E-Health Policy

A law that predates the Internet explosion needs retrofitting to serve as a foundation for standardized data exchange.

by Rob Cunningham

The cornerstone of federal policy on information technology (IT) in health care is an ambitious law that by a twist of fate was conceived just before network computing and the World Wide Web revealed themselves as the building blocks of a new electronic marketplace. As a result, federal policy making remains locked in a framework that does not properly fit the realities of current IT and the challenges that the emerging electronic marketplace pose for the health system. At the same time, the slow pace and crowded agenda of the health policy process have been aggravated by delays in the rule-making process and jurisdictional fragmentation in Congress that is even more acute than usual because of the high stakes and keen interest that e-commerce arouses. Despite the extravagant claims that are now routinely made about the potential impact of the Internet on health care, only a minimum of effective focus on these issues has been discernible on Capitol Hill in the year 2000.

Several factors slowed regulation writing for the IT provisions of the Health Insurance Portability and Accountability Act (HIPPA) of 1996, including the priority given to the act’s insurance-reform titles, the preoccupation of Congress and the Department of Health and Human Services (HHS) with the Balanced Budget Act, and a long timeout at HHS to cope with the year 2000 transition. Final rules on HIPAA’s Administrative Simplification provisions were not expected to appear until the end of summer 2000. One such rule was issued in August that defines standards for financial and administrative transactions, including required data elements and their code sets; these rules, effective after a twenty-four-month period for industry to gear up, are an important step toward achieving “interoperability” of health system information platforms. But many stakeholders and policy experts have already declared inadequate the crucial privacy rule also finalized in late summer 2000 and called for Congress to remodel the privacy legislation.

Rule making is in progress to implement further provisions of HIPAA on security and additional standardization measures for electronic health information. However, the technical obstacles to meeting the act’s security standards in a network computing environment are formidable, and the challenges to achieving some of the law’s standardization requirements may be even more difficult. An HHS study panel also has made a preliminary report on the issues likely to be involved in creating federal standards for the electronic medical record (EMR), a further step in the administrative simplification process envisaged, but not mandated, by HIPAA.

In the meantime, the explosive growth of the Internet not only has threatened to make

Rob Cunningham was writer and editor of Medicine and Health Perspectives from 1995 until March 2000, when he joined the staff of Health Affairs as a senior editor. He coauthored The Blues: A History of the Blue Cross and Blue Shield System (Northern Illinois University Press, 1997) with his father, the late Robert M. Cunningham Jr.
some of HIPAA’s IT provisions obsolete before they become operational, it also has entangled the policy questions about electronic commerce in health in a larger political struggle for which no end is in sight. There is huge pressure on Congress not to write rules on e-commerce that will kill the golden goose, but lawmakers risk undermining consumers’ confidence in the virtual marketplace if they leave advertisers and information brokers free to exploit the gold mine of data on Web surfers’ personal preferences that are now readily accessible in unregulated cyberspace. Free-market champions give lip service to the principle that sensitive personal information about health as well as finances needs stronger protection than routine shopper-surfing patterns do, but the distinction may be difficult to draw in practice. “While governments should not intervene excessively in this area, neither should they simply be spectators,” warned a 1999 report of the Organization for Economic Cooperation and Development.

**Born Too Soon**

Notwithstanding the general debate about whether more or less regulation is best for the future of e-commerce, or corollary differences of opinion about whether HHS exceeded its authority with the HIPAA privacy regulation or did not go far enough, the 600-plus pages of the rule suffer unmistakably from the antediluvian origins of the underlying statute. HIPAA’s IT provisions are “based on the wrong technology model,” says one HHS official—an early-1990s world in which electronic health information was stored in large, centralized payer and provider legacy systems, before network service providers and browser technology achieved the capability of marshalling huge fields of data in a common cyberspace accessible to anyone with a telephone line.

**Covered entities problem.** The HIPAA privacy regulation reflects many tough decisions and controversial choices, but none better illustrates the difficulties created by this essential anachronism than the law’s definition of “covered entities,” including plans, providers, and data clearinghouses. The Internet service providers (ISPs) and application service providers (ASPs) that came to dominate the electronic landscape in the late 1990s—and whose central role in managing the flow of networked information must be addressed to create meaningful privacy protection or broader IT policies—are not contemplated by the 1996 law. Regulation writers at HHS get credit for creativity for inventing the concept of “business partners” to extend the reach of the privacy regulation beyond the covered entities defined in statute. However this artifice—which makes the covered entities responsible for the conduct of ASPs, ISPs, and others with whom they contract—is “a Rube Goldberg kind of response” that may create as many problems as it solves.

The Joint Commission on Accreditation of Healthcare Organizations (JCAHO), for example, estimated that it would take about 20,000 separate contracts for it to conduct the business of accrediting providers under the regulation. The Health Insurance Association of America (HIAA) said that the rules “would force insurers to renegotiate hundreds of thousands of contracts.” Opposition came from across stakeholder groups, with health plans and employer and physician groups among those urging HHS to drop the business partner approach. Nor did the 52,000 comment letters seem to represent a mere knee-jerk reaction to regulation per se by entrenched interests: The Workgroup for Electronic Data Interchange, a large constellation of insurers, providers, government agencies, and vendors established during the Bush administration, was among those arguing for the scope of the rule to be expanded, suggesting that “all entities involved in electronic exchange of individually identifiable health information should be included in the rule as health care clearinghouses.”

Indeed, the established stakeholder groups that are usually the most vigorous upholders of the status quo have been curiously heterodox in their responses to the proposed HIPAA privacy rule. The regulation is “better than we expected,” said an employer representative.
“Insurers got what they wanted,” she said, because the “standing authorization” provision allows covered entities to share individually identifiable information for routine treatment and payment purposes without obtaining explicit patient consent—a formulation decried by patient advocates as overly broad.6 Some of the more powerful stakeholder groups, though, especially large businesses with regional or national operations (health plans, employers, and health information clearinghouses), called for a stronger federal privacy law that would preempt more-stringent state regulations. The HIPAA statute expressly stops short of preemption. “Many commentators cited the need for Congress to act” on various shortcomings of the underlying legislation, said a U.S. General Accounting Office (GAO) official summarizing responses to the proposed rule for the Senate Health, Education, Labor, and Pensions (HELP) Committee in April 2000.7 The National Committee on Vital and Health Statistics (NCVHS), a broad-based expert panel charged by HIPAA with advising Congress on information policy, concurred: “There is a need for comprehensive federal legislation...The proposed rule is limited in scope and does not cover all records or all entities...The definition of protected health information raises serious problems.”8

Security standards protested. The closely related HIPAA regulation detailing security standards for electronic patient information, also expected to appear in final form this year, are similarly problematic for stakeholders and seen by some as likely to create additional pressure for congressional intervention. Both the American Hospital Association and the American Medical Association called for immediate withdrawal of the rule when it was first proposed in 1998, and in this case the HIAA joined with the provider lobbies to protest the rule, claiming that the insurance industry was already held to rigorous computer security standards under state law.9 “Even the most sophisticated medical centers are unlikely to come close to meeting HIPAA’s security standards,” the chairman of the American Bar Association’s computer law division wrote recently. “HIPAA requires the health care industry to begin treating medical records in the same way that the federal government treats national defense secrets—as a form of classified information.” The security standards will in many cases require health care institutions still reeling from the disruptions of the Y2K transition to overhaul data systems yet again, if not replace them—at enormous expense, of course. “HHS’s proposed privacy and security standards will impose burdens so substantial that new efforts to convince Congress to amend HIPAA are inevitable,” wrote the official. “In 2001...expect an intense political debate about the nature and extent of security regulation needed to achieve an adequate, cost-effective, sensible level of privacy for medical records.”10

Further Frontiers

The task of implementing HIPAA’s privacy and security standards pales beside the challenge of realizing the law’s further goal: the linking of financial and clinical data with a “unique patient identifier.” The identifier is “an essential component of administrative simplification,” according to a 1998 NCVHS white paper, and “is necessary because the constellation of personal attributes commonly used to identify an individual...is rarely captured in the same manner by each entity in the diverse system of health care. Yet, good care depends on the provider’s ability to synthesize information from a variety of sources.”11 The Clinton administration issued a stop-work order to HHS on implementing the unique identifier in 1998 until privacy standards could be put in place to protect...
such a comprehensive, individually identifiable form of electronic record. Congress followed suit by attaching a ban on funding for such efforts in its fiscal year 2000 budget authorization. The patient identifier, as one member of the NCVHS put it, is “the mother of all privacy issues.”

In the environment of centralized, legacy data systems that were in place when HIPAA was conceived, the kinds of access control and system security that would be necessary to make the public comfortable with unique identifiers were conceivable, although modern access allowed skilled hackers to routinely penetrate even supposedly secure systems in this bygone era. In the past year, though, since the profiling practices of network ad brokers like DoubleClick began to make headlines and Internet privacy took off as a hot political issue, the notion of a unique identifier has acquired the aura of a third rail. “Dead on arrival,” said an HHS official, reflecting a concern that if the mechanisms of administrative simplification are not refashioned, federal policy will fall further behind events.

Standardization, after all, was to be the payoff for all of HIPAA’s arduous IT requirements, promising not only improved care but relief from the health system’s nightmarish administrative inefficiencies, with huge savings to boot, through the free flow of information. “We are pleased to see administrative simplification being done at the national level, and believe that these efforts will create significant cost savings in the health care marketplace,” said a Healtheon spokesperson, for example, in comments on HIPAA rules on standards for electronic transactions and code sets proposed in 1998. Yet, Healtheon stumbled in some of its first crucial contracts with physicians because of a lack of standardized, “interoperable” data systems. Even if new-economy ventures like Healtheon fail to transform the health system, administrative simplification could give the old system the tools to transform itself, many still hope.

The premature obsolescence of the policy set forth in the 1996 law, however, seems to have cut the system adrift in heavy seas. “Although the use of EDI [electronic data interchange] to support administrative transactions in health care has been increasing for several years, concerns about the century date change and other issues may have diverted attention from the HIPAA effort, and base line levels of EDI use in claims and related transactions vary decidedly among types of providers and health care organizations,” said the NCVHS in its Third Annual Report to Congress. “Because of the complexity of the standards, almost two years have passed without the issuance of a final rule. The NCVHS detects a growing industry concern about a loss of momentum. Further delay in issuing final rules for standards raises the possibility that industry resources committed to implementing the HIPAA standards may be diverted to other priorities. Moreover, delays in implementation translate into the loss of economic benefits from administrative simplification.”

Is HELP On The Way?

The policy process, too, has lost momentum, especially since a shift in the locus of responsibility for leadership that occurred in 1999, when Congress failed to meet HIPAA’s August deadline for enacting comprehensive privacy legislation for electronic medical records and the duty to create new protections through regulation devolved to HHS secretary Donna Shalala. The Senate HELP Committee spent nearly two years laying the groundwork for such a bill before the effort broke down in mid-1999 under the weight of unresolved issues in Sen. Jim Jeffords’ (R-VT) proposed bill and the committee’s increasing preoccupation with managed care legislation.

Jeffords’ “chairman’s mark” was scheduled for committee action five times in May and June 1999, but the markup was cancelled every time. Sticking points included the issue of preemption of more-stringent state laws, an amendment allowing parents access to information about minors’ abortions, and liability for disclosure of protected information. With Congress still polarized over the right-to-sue issue in managed care legislation also pending at the time, the liability question...
resonated insidiously. Rep. James Greenwood (R-PA) introduced a privacy bill in the House Commerce Committee in July to forestall congressional default on the HIPAA mandate, but the measure stalled without receiving serious consideration. Then Congress adjourned for its August recess, and the HIPAA deadline passed.

When HHS released its proposed privacy rule in October 1999, Jeffords declared that the regulation highlighted the need for congressional action because of gaps such as the limitations on covered entities and the rule’s failure to cover paper as well as electronic records. But the onset of the regulatory process, along with managed care, helped to push further consideration of confidentiality legislation off the committee’s agenda for the duration of the 106th Congress.

**Explosion of political interest.** To complicate matters further, the HELP Committee soon began to lose exclusive ownership of the issue as Internet privacy suddenly began to blossom as a hot political controversy. In November 1999 the Federal Trade Commission (FTC) attracted media attention with an all-day public workshop on the consumer-profiling practices of networking advertising brokers, piquing public curiosity with the provocative details about “cookie” technology and the powerful logic of targeted Internet advertising strategies based on collection of individualized data on Web users’ surfing habits. Then in February 2000, after the Y2K fixation finally released its grip on the planet’s technological imagination, the California HealthCare Foundation received prominent play in major national media with a detailed report on the large gaps between the declared privacy policies of major Internet health sites and the actual vulnerability of visitors to the sites to third-party collection of intimate, individually identifiable health-related information about them. Noting the limitations on covered entities in the proposed HIPAA rule, the report drew the obvious conclusion: “Many of the new e-health companies and services now proliferating on the Web are outside this definition, yet they collect and store vast amounts of personal health information.”

Alarming anecdotes about privacy violations on the Internet quickly became a staple of the daily news. Congressional interest in the privacy issue intensified rapidly, stoked by the inescapable conflict between aroused consumer advocates and the many champions of laissez-faire e-commerce policy in Congress and the Clinton administration. In the Senate, interest was stirred on the Commerce and Judiciary Committees with Sen. Patrick Leahy (D-VT) having led a series of efforts to develop privacy rules without impeding freedom of innovation. Multiple House Commerce subcommittees had putative interests at stake, as did the House committees on Government Reform, Science, and the Judiciary. The Banking Committees in both chambers had already weighed in with new standards protecting the confidentiality of financial records in the 1999 Gramm-Leach-Bliley Financial Services Modernization Act.

**Jurisdiction diffuses.** The action had moved decisively away from the traditional committees of jurisdiction in health. The House Commerce Subcommittee on Health held hearings on Internet prescription drug sales but remained focused on conference negotiations over managed care and the Medicare prescription drug issue. Renewal of the Internet tax moratorium in the House limited the interest of the House Ways and Means Committee, although its Health Subcommittee had a major role in HIPAA and held hearings on confidentiality in 1999 and again in February 2000, to explore “whether the regulation will ultimately prove to be workable or whether legislation might be necessary,” in the words of chairman Bill Thomas (R-CA).

The Senate Commerce Committee, where the FTC declared its dramatic about-face on privacy regulation, came close to but did not enter the specific realm of health data confidentiality. FTC chairman Robert Pitofsky acknowledged the need for a higher standard of protection for sensitive health and financial data than for other consumer information collected on the Web after explaining to the
committee in May why the FTC had decided that self-regulation was not progressing rapidly enough to be an adequate answer to consumers’ privacy concerns. However, the FTC did not make specific recommendations for health data protection, nor did the stronger legislative proposals under consideration in Commerce, such as the Consumer Privacy Protection Act proposed in May by Sens. Conrad Burns (R-MT) and Ernest Hollings (D-SC). The well-organized Congressional Internet Caucus, an industry-friendly alliance with active members on all involved committees in both chambers, was just one manifestation of a strong inclination in Congress to minimize Internet regulation.

■ Strong bill unlikely. The only legislative proposals that appeared to have fair chances of passage in 2000 were minimalist measures such as a requirement that sites post privacy policies, empowering the FTC to enforce self-regulatory efforts under its fair trade powers; or creation of a study commission on the privacy issue, as Rep. Asa Hutchinson (R-AR) proposed. Sen. Joseph Lieberman (D-CT) introduced a bill in the Senate Governmental Affairs Committee in May to encourage voluntary standards for health information on the Internet as a way of letting e-commerce ventures in health know that Congress was watching their conduct.

But the bill did not reach toward the tough questions on privacy, over which the Governmental Affairs Committee had no jurisdiction in any case. “People really look to the Senate HELP Committee,” said Ticia Gerber, manager of public policy for the Washington Business Group on Health. But the message that lobbyists were getting from the committee as the year wore on was that Jeffords was no longer interested in comprehensive health confidentiality legislation, other than a possible effort to “fill in the gaps” in HIPAA—a dubious proposition given the law’s underlying disconnection from the Internet context. “They’re backtracking,” Gerber said.

■ HIPAA not at fault. Despite the law’s pardonable shortcomings and frustration over delays in its implementation, HIPAA itself can hardly be blamed for the lack of cogent federal policy on e-health. The world has changed too rapidly, and a divided government moves too slowly, to have kept up. The challenge moving forward, as a new Congress and new administration begin their work, will be to fashion coherent and constructive federal policies that enhance the use of new information technologies in health across a confusing welter of competing viewpoints, interests, agency turf, and committee jurisdictions. The privacy issue will likely be the first

The Call For Leadership

Although they constituted a very forward-looking piece of legislation, HIPAA’s IT provisions are now cast in a doubly problematic light, simultaneously behind the times and crowding the road ahead with mandates. Stakeholders from across the spectrum, as well as disinterested parties such as the NCVHS—with its statutory authority to advise Congress and the HHS secretary on HIPAA—have called on Congress to revisit the issues, and the Senate HELP Committee will likely do its best to reassert leadership next year. Senator Jeffords has “made it clear that confidentiality standards will be a high priority for the Committee during the 107th Congress,” said a HELP staff member in July 2000, noting also that the HIPAA regulations do not become effective until twenty-four months after final rules are issued and that the statute allows for the updating of regulations as often as every twelve months. Final rules on transaction standards and code sets were published in August, clearing the way for covered entities and vendors to begin with the costly process of gearing up for implementation. Even in the absence of a viable rule for the unique patient identifier, these rules will help to create a foundation for increased electronic data exchange.

“HIPAA itself can hardly be blamed for the lack of cogent federal policy on e-health.”
such leadership test in 2001, but others soon will follow, both within the HIPAA context and beyond it. In the past, for example, Senators Jeffords and Leahy have worked to coordinate efforts on EMR confidentiality in the HELP and Judiciary committees. But broader questions about Internet privacy in general engage the Senate Commerce Committee as well, which is bent on nurturing e-commerce. For these panels to craft strong patient-record protections while minimizing perceived threats to commercial and technological innovation will not be easy. HELP staffers have “an appreciation of the need to be extremely careful.”

Further standardization. Beyond privacy, security, and the preliminary steps toward standardization mandated by HIPAA, the NCVHS in July 2000 released a report also required by the law on further steps needed to standardize not only transaction formats but patient medical records as well—“holy grail stuff,” in the words of one technology vendor. “Caregivers...need comparable PMRI [patient medical record information] seamlessly integrated from all sources to treat patients, ensure continuity of care, measure performance, and improve quality and productivity,” the report argued. “The lack of complete and comprehensive PMRI standards is a major constraint on the ability of our healthcare delivery system to enhance quality, improve productivity, manage costs, and safeguard data.” Even such confirmed free-marketeers as Newt Gingrich and Ira Magaziner, elsewhere in this volume, agree that government must establish these standards for the promise of IT in health to be realized.

Potential for patchwork solutions. Standardizing patients’ medical records will entail enormous cost, inconvenience, and resistance and will require an unusual mustering of political will to enact. Outside of the sweeping agenda envisaged in HIPAA lie a host of ancillary e-health issues crying out for policymakers’ attention: the quality of online health information; the regulation of online prescription drug sales; barriers to online care coordination created by existing Stark and anti-kickback laws; Food and Drug Administration regulation of electronic decision-support devices; and reimbursement for telemedicine and physician/patient e-mail contacts, to name a few. The fragmentation of congressional jurisdictions around the diverse domains subsumed under the rubric of e-health almost certainly will result in a patchwork of ad hoc and inconsistent measures if the need for coordinated policy is not successfully asserted.

“Government leadership is essential to effectively address the issues of interoperability, comparability, and data quality, as well as the related issues of protecting the confidentiality of PMRI, reducing ineffective diversity in state laws, and building a national health information infrastructure,” the July report from the NCVHS found. Similar conclusions were reached in a report earlier in the year from an expert panel of the National Research Council convened at the request of the National Library of Medicine: “The concerns and needs of the health community must be reflected in efforts to resolve national policy issues such as intellectual property protection, privacy, and access to information infrastructure, and specific efforts are needed to ensure that policy issues of concern only to the health community, such as licensure of care providers, reimbursement policies, federal funding for health informatics research, and the supply of health information technology workers, are addressed...Strong, stable leadership is essential to keep these policy-related activities focused and sustained,” the report found, and “DHHS should assert itself more aggressively in this arena.” The NRC panel cited the expanded role of the NCVHS as an example of agency leadership to build upon.

The appeal for more leadership from HHS is an opportunity for a new secretary to seize. Congress, too, has a clean slate in a postelection year and would do well to make a place at the high table for credible and disinterested voices from the science and research communities who can help to minimize the risk of counterproductive policies and maximize information-based advances in quality and efficiency.
NOTES

17. NCVHS, Third Annual Report to Congress, 2.
20. Senate HELP staff interview.
27. Senate HELP staff interview.
32. NCVHS, Report on Uniform Data Standards, 41.