HIPAA: a flawed piece of legislation

Allen B. Weisse, MD

A physician who always insisted that, as a sign of respect, his office staff address patients by their surnames arrives one morning to find that, to conceal identities, someone like “Mr. or Mrs. so-and so” is now being greeted as “Harry” or “Mary” or, worse, “Grandpa” and “Granny.”

A physician well known to the local pharmacy writes a prescription for his wife, who drops it off on her way to work. Shortly thereafter, the pharmacy calls about a problem concerning it. The physician, who is home alone at the time of the call, offers to resolve the problem. Despite the fact that he had written the prescription, he is informed that the pharmacy will speak to no one but his wife.

A neurologist arrives on a medical ward to perform a consultation. All the charts on the chart rack are turned facing the wall so that no names are visible on viewing it. He must then remove each one individually until he finds the name of the patient on the proper chart.

A physician has brought his pet dog to the local veterinary hospital to have certain blood work performed. The next day he calls to determine the results of this testing, but they will not be revealed to him unless he appears at the hospital with proof that he is, indeed, owner of the “patient.”

In collecting these bizarre vignettes occurring after the 1996 passing of Public Law 104-191, better known as the Health Insurance Portability and Accountability Act (HIPAA), and then complaining about it, I thought that the least I should do was to read it. And, even more importantly, since I planned to comment upon its outsized successor, the Omnibus Final Rule of 2013, a similar chore would be required. The original HIPAA, as suggested by its title, was concerned mainly with insurance matters, although in its preamble it promised a lot more:

To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud and abuse in health insurance and *health care delivery* [italics added], to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and *for other purposes* [italics added].

Much of the 167 pages of legislative gobbledygook about health insurance was pretty much unintelligible to one without the proper background in these matters, but despite such

shortcomings, the general impression received was that some positive measures were in the offing regarding the workings of the medical insurance system and related issues. As for patients’ privacy rights, only about a single page *in toto* was included and, in this respect, the content of the message was crystal clear. Under the subtitle concerning data collection, the secretary of the Department of Health and Human Services (HHS) would include procedures to ensure the privacy of individuals receiving health care services. And under the section regarding “wrongful disclosure of individually identifiable health information,” any person knowingly violating the law using a unique health identifier might be liable for fines up to \$50,000 and 1 year in prison or both. If the offense was committed under false pretenses, the fine might be as high as \$100,000 with up to 5 years in prison. If such an offense was committed for some commercial advantage, personal gain, or malicious harm, the penalties could rise to \$250,000 with 10 years in prison or both. What constituted an illegal breach of confidential information was simply what the secretary of HHS said it was. Given the vagueness of this criterion and such potentially draconian punishments for any breach in confidentiality, it is no wonder that many health care providers were driven by paranoia to the kinds of absurdities in behavior described above.

Between 1996 and 2013, supplementary regulations broadening and attempting to explain the law have been issued. Prominent among them was one defining the role of the Office of Civil Rights in assuming responsibility for the privacy provisions under HIPAA. A record of the number of possible breaches reported between 2004 and 2012 can be obtained over the Internet (1). The totals have nearly doubled during this time period. There were 4799 in 2004; 5683 in 2005; 8363 in 2011; and 9411 in 2012. Although these numbers may not seem excessively high for the entire country, each breach can involve many individuals. The 9411 number registered in 2012 actually represents the involvement of 6.7 million individuals.

What of the Omnibus Final Rule of 2013? To further educate myself on the subject, I sought assistance from governmental

From the Department of Medicine (retired), Rutgers–New Jersey Medical School, Newark, NJ.

Corresponding author: Allen B. Weisse, MD, 164 Hillside Avenue, Springfield, NJ 07081 (e-mail: allenweisse@gmail.com).

sources. The Congressional Research Service (CRS) is an independent part of the Library of Congress. It provides excellent reports on a variety of questions received from congressmen and their offices. Ordinarily, this service is not available to the public. However, as an academician engaged in a scholarly endeavor, I wrote to the director of the CRS asking for an exemption. My request was never answered. Similarly, a letter to the director of the Office of Civil Rights at HHS received no reply. Fortunately, I was able to obtain a number of useful CRS reports through a friendly connection to Congress. Another individual I knew to be professionally involved with the system gave me further access to important information. A copy of the new rule was obtainable over the Internet (2).

In a preamble to the rule that went into effect in March 2013, the stated aims of this new version of HIPAA include, among others, making business associates of covered doctors and other entities such as medical practices and hospitals directly liable for compliance with HIPAA rules and regulations; strengthening limitations on the use of protected patient information; expanding individuals' rights to access of electronic information; requiring changes and redistribution of notices of privacy practices by physicians and hospitals; implementing more objective standards defining "harms" when privacy is breached; and prohibiting most hospital plans from using genetic information for underwriting purposes. No priority was given to means of improving cooperation and understanding between patients and their physicians.

Confronting the Omnibus Final Rule of 2013 was daunting, and not only because of its 563-page length. The routine use of impenetrable legalistic jargon jarred the mind. Adding to the bulk of material to be reviewed was the practice of printing an initially proposed version of a provision of the rule; this was followed by public commenters' input, often a response to the commenters' suggestions or objections, and then the final version of the rule.

Since the new law incorporates portions of previous laws still in effect, reference to these pepper the pages. These include the Health Information Technology for Economic and Clinical Health Act of 2009, the Social Security Act, the Patient Safety and Quality Improvement Act of 2005, and the Genetic Information Non-Discrimination Act of 2008, among others. At every point I wished to examine and enlighten myself, I found references to previous acts that were in effect, some identified only by number and sections. An example on page 35: 164.504(c)(4)(ic)(B). I began to feel the same way I did when I examined my first matryoshka doll, opening it up to reveal its essence only to find a smaller but otherwise identical doll, containing a still smaller one, and so on, all smiling inscrutably in colorful lacquered dress. If I was really to make a legitimate study of the law, I would be compelled to open up all the previously referred to laws now included in the 2013 document. This would no doubt take many months rather than the several weeks I planned to devote to the project, and I seriously doubted whether, given the character of such legislative documents—assuming I could acquire them—I would emerge any better informed. I therefore settled on limiting the project

to extracting whatever few pieces of information I could that might prove to be of some value to physicians and other so-called "entities" reading the law.

What about privacy? The ability of individuals to completely control access to their personal medical records is the Holy Grail of privacy rights advocates. The possibility of actually achieving this is as much a myth as the Holy Grail itself. Were it seriously attempted, the whole machinery of medical care administration would come to a screeching halt. Insurance companies and billing services require such information to process charges. Institutions such as Medicare and Medicaid need this information to audit their operations and plan for the future. Certain diseases are classified as "reportable" in the interests of public health. Immunization records are often required by school districts to ensure protection of the children attending their schools. Such requirements are actually recognized by the new law. Perhaps the only type of care that may effectively adhere to the ideal of personal privacy is psychiatric treatment, since this is so often paid out of pocket directly to the psychologist or psychiatrist.

What about genetic information? This is a major component within the 2013 rule, taking up almost 100 pages, about a fifth of the document. With the recent advances in the field, this is a highly charged, newly recognized element of medical care now being given its proper due. Mercifully, this section contains much writing that actually could pass muster in English 101. The rule prohibits "using or disclosing protected health information that is genetic information for underwriting purposes in all plans covered in the HIPAA privacy rule." It also distinguishes between "manifest disease" (symptoms and physical findings characteristic of a particular genetically based disease) and the finding of a genetic component that may or may not coexist (a genetic abnormality). This section would make worthwhile reading for anyone practicing medicine where genetics is emerging as a primary factor.

What about decedent information? Knowledge about cause of death and its relationship to various patient characteristics has been critical in advancing the quality of medical care. The new rule sets 50 years after demise as an appropriate period of protection before postmortem information might be obtained without permission from survivors of the deceased. While some medical historians might find this satisfactory, with new diagnostic modalities and treatments occurring at a rapidly advancing rate and the need for their evaluation urgent, practitioners and medical researchers might find this rule overly restrictive. Those empowered to make disclosures about decedents are defined as those with first to fourth degrees of familial relationship. The marital bond appears to be given equal recognition. No mention is made of civil unions, gay or lesbian, but those primarily responsible for the decedent's health concerns prior to death appear to be given some consideration. Issues such as removal from artificial life support systems, organ donation, and permission for autopsy are not covered.

How much will the activation and continued support of these new regulations cost? The estimate for the first year of operation was \$114 to \$225 million, with an estimate of \$14.5 million annually thereafter.

What are the penalties involved for breaking the law? Four categories are defined reflecting the increased severity of any malfeasance: 1) violations in which the covered entity did not know and, with reasonable diligence, would not have known a violation had occurred; 2) violations due to reasonable cause and not to willful neglect; 3) violations due to willful neglect but corrected in a timely manner; and 4) violations due to willful neglect and not corrected in a timely manner. At the low end, each violation can be met with a fine of \$100 to \$50,000, with \$1.5 million for identical violations within a calendar year. For the most severe category, a minimal penalty of \$50,000 can be levied with an annual maximum of \$1.5 million for repeat offenses. The severity of the penalty will be determined by the nature of the violation and the resulting harm caused. Compared to 1996, the potential financial penalties are appreciably higher, but prison time is no longer mentioned.

Presumably the income generated by violations will meet the costs of conducting the program. Such penalties, even before the 2013 law went into effect, have been considerable. Brach/Eichler, a New Jersey legal firm that is involved in such matters, keeps a tab on such penalties and includes many physicians on their mailing list. Before the new law took effect, they noted a \$1.2 million penalty against Affinity Health Plans and a settlement with WellPoint, Inc. for \$1.7 million as examples of recent actions by the government.

In the end, this legislative voyage of discovery was pretty disappointing. I was left pondering another Russian-related metaphor, that uttered by Winston Churchill regarding his view of the Soviets: “a riddle wrapped in a mystery inside an enigma.” Most laws passed by Congress are flawed to some extent but, once passed, they seem to develop a life of their own, persisting within the body politic. Of course there are some really bad ones, such as that ushering in prohibition, which was passed in 1919 and repealed in 1933. However, for most laws passed by

Congress during the last couple of hundred years, repeal will not happen. There is always some small but powerful constituency that benefits even from a bad law, and congressional inertia can be counted upon to keep it on the books.

James Madison, the father of the Constitution, warned us, “It will be of little avail to the people that the laws are made by men of their own choice if the laws be so voluminous that they cannot be read or so incoherent that they cannot be understood.” Despite his concern at the beginning of the Republic, we continue to witness legislative behemoths like HIPAA and its reincarnations bearing down upon us with little hope for revision or repeal.

Despite the worthy portions of these laws, their emphasis on punishment for breaches only serves to inhibit the flow of information necessary for efficient medical management and erode the bonds of trust so essential to a proper doctor-patient relationship. Stuart Graves, in writing about confidentiality and the effect of electronic health records upon it, commented, “Physicians seem to live interminably hassled lives” (3). How true.

Acknowledgment

Jerilyn Goodman and Kevin Littlefield assisted in the preparation of this paper.

1. US Department of Health and Human Services. *Health information privacy: Enforcement results by year*. Available at <http://www.hhs.gov/oct/privacy/hipaa/enforcement/data/historicalnumbers.html#tenth>.
2. US Department of Health and Human Services. *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules*. Available at <https://s3.amazonaws.com/public-inspection.federalregister.gov/2013-01073.pdf>
3. Graves S. Confidentiality, electronic health records, and the clinician. *Perspect Biol Med* 2013;56(1):105–125.