

University of Michigan Law School
University of Michigan Law School Scholarship Repository

Articles

Faculty Scholarship

2006


HIPAA-Cracy

Carl E. Schneider

University of Michigan Law School, carlschn@umich.edu

Available at: <https://repository.law.umich.edu/articles/1958>

Follow this and additional works at: <https://repository.law.umich.edu/articles>

 Part of the [Health Law and Policy Commons](#), [Legislation Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

Schneider, Carl E. "HIPAA-cracy." *Hastings Center Rep.* 36, no. 1 (2006): 10-1.

This Response or Comment is brought to you for free and open access by the Faculty Scholarship at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in Articles by an authorized administrator of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.

HIPAA-crazy

by Carl E. Schneider

The Department of Health and Human Services has recently been exercising its authority under the (wittily named) “administrative simplification” part of the Health Insurance Portability and Accountability Act to regulate the confidentiality of medical records. I love the goal; I loathe the means. The benefits are obscure; the costs are onerous. Putatively, the regulations protect my autonomy; practically, they ensnarl me in red tape and hijack my money for services I dislike.

HIPAA (a misnomer—HIPAA is the statute, not the regulations) is too lengthy, labile, complex, confused, unfinished, and unclear to be summarized intelligibly or reliably. (*Brevis esse laboro, obscurus fio.*) However, a covered entity is any health plan or “health care provider” that “transmits any health information in electronic form.” If HIPAA has a general rule, it is that (1) a “covered entity may not use or disclose protected health information except as permitted,” (2) the entity must “make reasonable efforts to limit protected health information to the minimum necessary,” and (3) the covered entity must require its “business associates” to “appropriately safeguard the information.” With plentiful exceptions and restrictions, entities *may* use or disclose information “for treatment, payment, or health care operations.”

There is much more. For instance: (1) Information may usually be disclosed for “marketing” only with the patient’s elaborately detailed authorization. (2) An entity may reveal a patient’s

name, room, and general condition to “persons who ask for the individual by name” but “must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information . . . and provide the individual with the opportunity to restrict” the disclosures. (3) Entities may release information with the patient’s consent. If a patient cannot give consent, the “entity may, in the exercise of its professional judgment, determine whether . . . disclosure [to a person taking care of the patient] is in the best interests of the individual and, if so, disclose only the . . . information that is directly relevant to the person’s involvement with the individual’s health care.”

Almost every part of HIPAA instructs the entity to loose rivers of information upon the patient. Entities may do many things without consent, but they must specify these things at punishing length. One example: the notice must describe each purpose “for which the covered entity is permitted or required . . . to use or disclose protected health information without the individual’s written authorization.” This “description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.” Entities may do many things only *with* consent, which must be solicited through another grueling barrage of disclosures.

Why HIPAA? Medical privacy was multiply protected—by ethical codes,

state and federal statutes and administrative regulations, tort law (which, unlike HIPAA, give patients remedies), accrediting organizations, hospital policies, even the market—long before HIPAA gleamed in a bureaucrat’s eye. As Richard Epstein notes, before HIPAA we saw no “explosion of improper disclosures of sensitive information, and no systematic unwillingness to deal with the problems that do arise by private organizations or even by more limited and focused regulatory responses.”

So why HIPAA? HHS presented and justified its basic rules in 400 large pages of small print. First: “Privacy is a fundamental right. . . . [I]t speaks to our individual and collective freedom.” This makes me reach for my Burke. He could not praise “anything which relates to human actions . . . on a simple view of the object . . . in all the nakedness and solitude of metaphysical abstraction. Circumstances (which with some gentlemen pass for nothing) give in reality to every political principle its distinguishing color and discriminating effect.”

“Privacy” means everything and nothing. In law, “privacy” is so protean that it is meaningless without modification. Privacy as “fundamental right” is an idea from constitutional law, but it refers to freedom of choice, not confidentiality of information. The Constitution protects physical privacy only sporadically; for example, only some searches are prohibited. More broadly, I doubt that the interests protected by “privacy” are distinctive or illuminating enough to make up an independent moral category.

And fundamental? Complete privacy is impossible even for a hermit and unhealthy for anyone. Every day we trade privacy for the many things we value more. Privacy itself has costs for individuals and society, as when it makes illness embarrassing. Finally, *many* invasions of medical privacy are unfortunate and wrong but not greatly damaging. When they are damaging, it is often the misuse of the information by a third party, not the breach of privacy itself, that causes the harm.

HHS's rationale for HIPAA quickly descends from the loftily vague to the absurdly narrow: "The health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center. . . ." "An employee of the Tampa, Florida health department took a computer disk containing the names of 4,000 people who had tested positive for HIV. . . ." Sad stories, but HIPAA cannot prevent winds from blowing nor employees from stealing, and state law already provides sanctions for negligence and theft.

HHS concedes that the "costs and benefits of a regulation must, of course, be considered as a means of identifying and weighing options." Does HHS believe this? In the same paragraph it warns cryptically that because privacy is a "fundamental right . . . it must be viewed differently from any ordinary economic good."

However "fundamental" privacy may be, HIPAA is otiose if it promotes it ineffectively. Some privacy is unattainable; HIPAA can do little to reduce the number of people who need to see medical records. Other kinds of privacy cannot be achieved with HIPAA's tools. Consider HIPAA's incessant disclosure requirements. My hospital distributes seven pages of disclosures in print so small I can't read them with my glasses on. One analysis placed these forms at a college reading level. Like this:

Examples of these activities include obtaining accreditation from independent organizations like the Joint Commission for the Accreditation of Healthcare Organizations, the National Committee for Quality Assurance and others, outcomes evaluation and development of clinical guidelines, operation of preventive health, early detection and disease management programs, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives, and related functions; evaluations of health care providers (credentialing and peer review activities) and health plans; operation of educa-

tional programs; underwriting, premium rating and other activities relating to the creation, renewal or replacement of health benefits contracts; obtaining reinsurance, stop-loss and excess loss insurance; conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; business planning and development; and business management and general administrative activities, including data and information systems management, customer service, resolution of internal grievances, and sales, mergers, transfers, or consolidations with other providers or health plans or prospective providers or health plans.

But what does the language matter, since no one reads the forms? One "covered entity" told me that in three years I was the second patient to ask for a copy of his HIPAA disclosure form.

Nor is *any* benefit to confidentiality worth *any* cost. Consider HIPAA's record-keeping requirements. One compels entities to offer patients "an accounting of disclosures of protected health information made . . . in the six years prior" to the request. The accounting must include the disclosure's date, the discloser's name and address, a description of information disclosed, and the reason for the disclosure. The cost of keeping so many records in such detail for so long cannot be small; the people who will request, receive, and benefit from the information must be few. Have we *no* better uses for resources?

Not only does HIPAA impose extravagant costs for exiguous benefits. HIPAA's sour assumptions about human nature work positive harm. For instance, HIPAA assumes people (1) want to keep information from their families and (2) do not want to participate in research, even medical records research whose benefits can be great and whose threat to privacy tiny. HIPAA's rules are structured to serve patients who fit those assumptions.

HIPAA's assumptions are wrong. Most people want their families involved in their medical care. And in one study, 96 percent of the Mayo Clinic patients approached consented to medical records research. Instead of having the few patients who fit HIPAA's assumptions opt in to restrictive privacy rules, HHS requires the huge majority of patients who don't fit the assumptions to opt out of them. This burdens patients. Worse, most patients won't realize they need to act, and few will get around to it.

Most patients, then, will at least be harassed, and their preferences will regularly be thwarted. Patients who would cheerfully have acceded to medical records research may not suffer, but a crucial kind of research will (to say nothing of HIPAA's effect on research generally, a disturbing problem I lack space to consider). Patients who want families involved in their care may directly be harmed, for families are often denied information patients want them to have. Thus prudent patients are saddled with one more chore—having a lawyer draft a HIPAA release form.

The best defense of HIPAA I hear is that, *favorably interpreted*, it *might* not require entities to make overlong disclosures, deny families information, or thwart research. But pity the entities. HIPAA speaks in sweeping, vague, and menacing language. Terms like "reasonable," "minimum necessary," "professional judgment," and "best interest" litter it. It deploys civil *and* criminal penalties. Recall the unspeakable sentence I quoted. You might speak unspeakably too in order to provide descriptions with "sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law." Surely cautious entities will tell patients too much, and everyone else too little.

So I reach again for my Burke. "The science of constructing a commonwealth, or renovating it, or reforming it, is . . . not to be taught *a priori* . . . , [for] very plausible schemes, with very pleasing commencements, have often shameful and lamentable conclusions."