VIEWPOINT

How HIPAA Harms Care, and How to Stop It

Donald M. Berwick, MD, MPP
Institute for Healthcare Improvement, Boston, Massachusetts.

Martha E. Gaines, JD, LLM
Center for Patient Partnerships, University of Wisconsin Law School, Madison.

Viewpoint pages 231 and 233

"Knock, knock."

"Who's there?"

"HIPAA."

"HIPAA, who?"

"I'm sorry, but I cannot disclose that."

Clinicians and patients alike will laugh at this, but behind the laughter are anger and frustration. The Health Insurance Portability and Accountability Act (HIPAA), a law created to protect patients, has borne with it serious obstacles to effective care. How did this happen? What went wrong on the road to protecting privacy?

Passed in 1996, HIPAA was not originally a privacy law at all. Its primary intent was to assure "portability": continuity of health insurance coverage as individuals changed jobs. In fact, the privacy part of the law was very brief. Congress had been debating a Patients' Bill of Rights for some time, which was to include privacy rights as well as the right to sue insurers for wrongful denial of coverage; but Congress failed to pass such legislation. This prompted the Department of Health and Human Services (HHS) to create the privacy regulations governing transfer of records (paper or electronic) containing personal health information (PHI), designed to ensure patient safety and prevent insurance companies from using that information to manipulate coverage.

> Privacy of [personal health information] is crucial, but ill- conceived policies and behaviors that have emerged based on misinterpretations about HIPAA are not the way to get there.

The regulations that compose the HIPAA Privacy Rule are complex and voluminous. (The 2013 update alone, regarding electronic medical records and e-health, is 563 pages long.[1]) However, these regulations coalesce around one simple rule: clinicians and health care organizations may not disclose PHI without patient permission unless that information is being used for treatment, payment, or health care operations. For these purposes, patient permission is assumed. In addition, organizations must release records to patients who ask for them and to HHS for enforcement purposes.

The law levies significant penalties for wrongful release of PHI and for the failure to timely release to the patient or HHS, but it has no penalties for unreasonably delayed or wrongful refusal to release information to other clinicians for treatment purposes. This imbalance has led to a knee-jerk bias against releasing information, as well as to a culture of complex paperwork to double and triple document the purpose before releasing information. Compounded by increased enforcement activity and higher fines over the last several years, the organizational policies intended to protect patients' privacy may too often compromise their health care.[2,3]

In too many cases, these policies do not reflect HIPAA requirements. Rather they are grounded in "HIPAA myths": misapplications based on misunderstandings about what the law requires. The policies needlessly cast a confusing shadow over nearly every aspect of clinical care, health care information management, patient and family services, and even building design.[4,5]

The myths abound. Every day, patients seeking second opinions or transferring to new clinicians experience treatment delays when wrongly conceived procedural hurdles prevent their physicians from talking to previous clinicians and obtaining timely access to test results and treatment histories. Family members seeking information about a loved one involved in a motor vehicle crash are wrongly told that HIPAA prevents even a confirmation of whether their family member is at that facility.

Both the need for privacy and the toxicity of HIPAA myths have increased with the spread of electronic medical records. Privacy practices prior to electronic medical records were dismal. Many physicians remember disorderly piles of medical records spread across desktops in hospital nurses' stations, abusive husbands easily locating their terrified wives in the emergency department, and curious employees reading about their neighbors' illnesses. That certainly was not private enough. Compounding those original problems is the new threat of having medical records stored in the cloud, with the possibility that those records could be hacked. Stricter standards seem logical to make clear who has viewed a patient's record so that improper access can be addressed.

Privacy of PHI is crucial, but ill-conceived policies and behaviors that have emerged based on misinterpretations about HIPAA are not the way to get there. The test of the wisdom of a policy is not whether it protects privacy absolutely (that would be easy: just forgo communication altogether), and absolute privacy is not what HIPAA requires. Rather, a well-designed policy strikes the best balance between protecting patients' privacy and enhancing their health, ensuring that the records necessary to their care can be provided where they are needed promptly and without needless expense.

When a clinician or clerk feels compelled to say, "I wish I could tell you but HIPAA won't let me," that is usually an indication of a misguided organizational policy or insufficient employee training. Some legitimate differences of opinion can, of course, arise about how HIPAA regulations resolve some ethical or legal issues.

Corresponding Author: Donald M. Berwick, MD, MPP, Institute for Healthcare Improvement, 53 State St, 19th Floor, Boston, MA 02109 (donberwick@gmail.com).

But most pain caused to clinicians and patients through the overzealous pursuit of privacy comes from misinterpretations of the regulations, and not from their actual substance.

Common misguided administrative provisions are many. They include restrictions on the exchange of clinical information between treating clinicians, rules against posting patients' names in clinical areas to facilitate finding or identifying the patient, and rules against family members or loved ones reviewing medical records and clinical information even with the patient's permission. At best, confronting or circumventing such unnecessary policies takes precious time and energy, already in short supply for clinicians and patients. At worst, such policies and restrictions can force wasteful and sometimes harmful repetition of diagnostic tests, and even cause potentially devastating delays to needed care.[6]

For patients, families, and clinicians, health care is complex and precarious enough to warrant removal of every unnecessary bureaucratic barrier to coordination and the mission-critical exchange of information. The widespread confusion about what HIPAA requires is harmful. The proper, but daunting, goal is to ensure accurate, uniform, sensible, and understandable policies and procedures for the efficient transfer of information and the appropriate protection of patient privacy. Getting that right will require leadership and real effort at the highest levels. At the moment, the balance is wrong.

The following are possible corrective steps:

1. HHS should commission and support immediate research studies on the magnitude, frequency, patterns, and consequences for patients of restrictive misinterpretations of the HIPAA Privacy Rule in the treatment context, similar to the 2009 Institute of Medicine study of the effects of HIPAA on research,[7] which concluded that the rule inhibited research and failed to protect patients.
2. The Office for Civil Rights at HHS should promulgate model policies and procedures that can be adapted locally as necessary to comply with state laws, to promote consistency and compliance with the letter and the spirit of HIPAA privacy regulations, and to reduce perilous, over-restrictive, and misguided practices.
3. HHS should consider creating and enforcing penalties for failure to release all relevant clinical information to treating clinicians in a timely fashion. While this may require congressional action, it would encourage health care organizations to root out HIPAA myths and countermand them. In addition, HHS should create a website listing hospitals and other health care organizations that repeatedly deny clinicians, patients, or families needed information, akin to the existing "Wall of Shame" listing organizations that are under investigation for breaches of unsecured protected health information.[8]
4. Professional societies and patients' rights organizations should mount concerted campaigns to inform patients and clinicians about common barriers to information exchange that represent erroneous interpretations of HIPAA, and about how to assert their rights to information.[9]

HIPAA regulations were promulgated to address serious breaches of patient privacy, an undeniably noble intention. But, as the adage states, the road to hell is paved with good intentions, and, similarly, the implementation of those regulations via erratic, bureaucratic, and misguided policies has led too often to a veritable HIPAA hell. The promise of electronic medical records to facilitate the transfer of clinical information where and when it is needed is all for naught if ill-conceived policies pour virtual molasses on the process. Through HIPAA, Congress has properly tried to protect patients' privacy. Those who implement the law should act wisely to protect patients' care as well.

ARTICLE INFORMATION

Published Online: June 20, 2018. doi:10.1001/jama.2018.8829

Conflict of Interest Disclosures: All authors have completed and submitted the ICMJE Form for Disclosure of Potential Conflicts of Interest and none were reported.

Additional Contributions: We thank Corinna Parisi, BA (Institute for Healthcare Improvement), for providing research support for this work, for which she did not receive extra compensation.

REFERENCES

1. 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. https://s3.amazonaws.com/public-inspection.federalregister.gov/2013-01073.pdf. Accessed June 13, 2018.
2. Gray R. How HIPAA is harming patient care. *MD Magazine*. http://www.mdmag.com/contributor/ryan-gray-md/2016/02/how-hipaa-is-harming-patient-care. Published February 10, 2016. Accessed June 13, 2018.
3. De M. Understanding HIPAA, and how it can hurt health care. US Annenberg Center for Health Journalism. https://www.centerforhealthjournalism.org/2016/03/29/when-misuse-hippa-hurts-health-care. Published April 9, 2016. Accessed June 13, 2018.
4. Span P. HIPAA's use as a code of silence often misinterprets the law. *The New York Times*. https://www.nytimes.com/2015/07/21/health/hipaas-use-as-code-of-silence-often-misinterprets-the-law.html. Published July 17, 2015. Accessed June 13, 2018.
5. Pines J, Gray E, Thorpe JH. 10 times HIPAA may not apply. *Emergency Physicians Monthly*. http://epmonthly.com/article/10-times-hipaa-may-not-apply/. Published September 1, 2015. Accessed June 13, 2018.
6. Salem DN, Pauker SG. The adverse effects of HIPAA on patient care. *N Engl J Med*. 2003;349(3):309. doi:10.1056/NEJM20030717349032
7. Nass SJ, Levit LA, Gostin LO, eds; Institute of Medicine Committee on Health Research and the Privacy of Health Information. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. Washington, DC: National Academies Press; 2009.
8. Department of Health and Human Services. Breach report: notice to the Secretary of HHS breach of unsecured protected health information. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Accessed June 13, 2018.
9. Health Information & The Law Project. Health information & the law. http://www.healthinfolaw.org/search/apachesolr_search?filters=type%3Aarticle%20tid%3A122. Accessed June 13, 2018.