American Medical Association Journal of Ethics

March 2016, Volume 18, Number 3: 288-298

POLICY FORUM

Federal Privacy Protections: Ethical Foundations, Sources of Confusion in Clinical Medicine, and Controversies in Biomedical Research

Mary Anderlik Majumder, JD, PhD, and Christi J. Guerrini, JD

The privacy of patient information is protected by the US Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPAA) [1] and other laws, including the Basic HHS Policy for Protection of Human Research Subjects (often referred to as the "Common Rule") [2]. Although the term "privacy" does not appear in HIPAA's title, attention to privacy is critical to achieving its goals, which include facilitating coordination of care as people change insurance plans and providers and promoting electronic exchange of information within the health care system. Further, HIPAA and the Common Rule exist within a broader biomedical context in which data sharing is increasingly recognized as critical to both clinical care and research. A National Research Council report on sharing biomedical information identifies "careful handling of policies to ensure privacy as *the central issue* in its entire vision" of accelerating innovation [3].

The aim of this essay is threefold. We first describe the ethical foundations for HIPAA and other privacy laws. We then suggest that, contrary to claims that HIPAA is ethically questionable because it obstructs coordinated clinical care, *confusion* about HIPAA is sometimes, perhaps even frequently, the barrier to high-quality care. Finally, we raise some questions about the ethical status of proposed changes to the Common Rule that concern privacy in the context of medical research.

Ethical Foundations of Privacy Law

Privacy is defined broadly, encompassing the right to be free of unwarranted surveillance and interference and the right to control sharing of personal information [4]. Under the umbrella of privacy, *confidentiality* concerns the protection against unauthorized disclosure of patient or client information obtained within the context of a professional relationship [4].

The importance of privacy and confidentiality to the practice of medicine has been recognized from ancient times to the present. For example, the Hippocratic Oath commits the oath taker to keep all information obtained about patients' lives secret [5]. Opinion 5.05 of the current AMA *Code of Ethics* states that the patient should be able to "make a full disclosure of information" secure in the knowledge that "the physician will respect the confidential nature of the communication" [6]. Revealing confidential

information without express patient consent is only permitted when "ethically justified because of overriding considerations" [6].

What are the ethical considerations supporting these strong endorsements of privacy and confidentiality?

Trust. Opinion 5.05 of the AMA *Code of Ethics* implies that trust—the bedrock of the patient-physician relationship—requires privacy protections. A person's level of trust in health care professionals is likely to affect his or her willingness to seek professional help, reveal relevant information, adhere to a treatment plan, return for further care, and participate in research. Trust is built and preserved by consistent, reliable privacy protection practices within and across professions and institutions engaged in the provision of health care and the conduct of research.

Beneficence and fiduciary responsibility. Beneficence and the health care professional's fiduciary responsibility to patients entail not only commitments to protect and promote patients' health-related and other interests, but also commitments to avoid causing loss or harm to one's patients. Disclosure of patients' private information can cause harms including: (1) economic harm, such as employment discrimination (if diagnostic or health risk data are not properly protected) or identity theft; (2) social harm, such as stigmatization or damage to family relationships (e.g., from disclosure of an HIV diagnosis or misattributed parentage revealed by genetic testing); and (3) legal harm, such as prosecution for drug-related offenses of a patient seeking treatment for a substance use disorder.

Respect for autonomy and for patients. Respect for autonomy includes respect for a patient's right to decide with whom to share his or her personal information. AMA *Code of Ethics* Opinion 5.05 appeals to this consideration by treating disclosures to which the patient has expressly consented differently than disclosures without patient endorsement [6]. Related to respect for autonomy is the more encompassing principle of respect for persons, which entails recognition of and sensitivity to patient vulnerability, efforts to preserve and restore patient dignity, and protection of patients from exploitation. This ethical consideration translates into efforts to screen patients' bodies from view and restrictions on the ability of health care professionals to use patient information for purposes unrelated to the care of the patient (e.g., fundraising and selling that information to third parties).

Fidelity. There are generally recognized exceptions to the duty to maintain confidentiality (discussed below) and the existence of legal obligations to disclose information in some circumstances (for example, reporting cases of communicable disease to public health authorities and cases of suspected child abuse to child protection agencies). Even given these, however, a health care professional's implicit or explicit promises to a patient of

confidentiality regarding a particular encounter or disclosure must be factored in when evaluating whether the ethical considerations supporting an exception to confidentiality are "overriding."

Clearing Up Confusion about HIPAA

HIPAA's strong commitment to privacy is in keeping with the ethical considerations reviewed above [7]. It restricts uses and disclosures of individually identifiable protected health information (PHI) by covered entities (i.e., most health care providers, health plans, and health care clearinghouses) without patient authorization, but allows exceptions to facilitate the delivery of care. Three major categories of exceptions are disclosure for treatment, payment, and health care operations purposes [8].

Assigning to the patient the role of gatekeeper to his or her personal information is consistent with the principle of respect for autonomy. So is enshrining patients' rights to receive a notice of their privacy rights, to access and amend their PHI held by health care professionals and institutions, and to receive an accounting of disclosures. The exceptions for payment and health care operations (but not for treatment purposes) are subject to a "minimum necessary" standard that reflects awareness that, even when disclosure is justified, it exposes patients to risks and so should be tailored to need [9].

Despite the existence of these exceptions, HIPAA is often invoked as a frustrating barrier to coordinated delivery of care and appropriate sharing of information (i.e., to promote patient well-being). A 2015 report to Congress from the Health Information Technology Policy Committee found, however, that it is not the provisions of HIPAA but *misunderstandings* of privacy laws by health care providers (both institutions and individual clinicians) that impede the legitimate flow of useful information. The report refers to "many examples where misinterpretations" have inhibited information exchanges permitted under HIPAA [10].

Such provider misunderstandings include the following:

- The belief that HIPAA requires patients to provide authorization before information can be shared for treatment purposes between physicians and other health professionals, hospitals, ambulance companies, health information exchange organizations, and others involved in providing or coordinating care (potentially generating inefficiencies such as delays and unnecessary paperwork burden and inhibiting coordination of care);
- The belief that HIPAA forbids appropriate communication with patients' families, friends, and the clergy (potentially isolating patients and depriving them of support); and
- The belief that HIPAA restricts appropriate use of electronic technologies for communication (potentially depriving providers, patients, and the larger health

care system of the capacities of these technologies to facilitate communication and make the transfer of information more efficient).

All of these misunderstandings were labeled as such in a 2004 HHS Office for Civil Rights (OCR) letter to health care providers [11], among other sources [12-14]. Yet the myths persist [10, 15]. What follows is accurate information about HIPAA's provisions.

Information sharing among treating entities. As noted above, HIPAA permits sharing of information among those treating the patient without separate authorizations. The OCR letter states: "Providers can freely share information with other providers where treatment is concerned, without getting a signed patient authorization or jumping through other hoops" [16]. Further, as noted above, such sharing is not subject to the "minimum necessary" standard, which requires reasonable steps to limit uses and disclosures to the minimum necessary for accomplishing the intended purpose [9].

Disclosure of information to patients' family, friends, and clergy. Disclosure of information is permitted when others are in the room with the patient, and a patient's location and general condition information can generally be shared with loved ones. The OCR letter states: "Doctors and other providers covered by HIPAA can share needed information with family, friends—or even with anyone else a patient identifies as involved in his or her care—as long as the patient does not object" [16]. In addition, when a patient is incapacitated, it is permissible to share information so long as the health care professional believes that doing so is in the patient's best interests [11-14, 17].

Use of electronic technologies. In the words of former OCR director Richard Campanelli, "HIPAA is not anti-electronic" [16]. The HIPAA regulations neither privilege paper communication nor restrict particular modes of electronic communication. Further, facilitating health information exchange using electronic technologies remains a top national policy priority, with policymakers embracing these methods' potential to promote patient access to information and make sharing among providers more efficient [18]. It would be incorrect to state, for example, that HIPAA requires written authorizations from patients before information can be transmitted via a health information exchange for treatment purposes, or that it prohibits participation in such an exchange. Such statements reflect confusion about HIPAA and perhaps also the desire to avoid the technological, financial, and policy challenges associated with using electronic technologies to share information in an ethically responsible, secure manner.

The HIPAA regulations do require systematic attention to privacy and security concerns across all modes of documentation and communication, and they also permit providers to impose some requirements for tracking and identity verification purposes [11, 17]. When physicians or other clinicians encounter an institutional policy related to information access or sharing that they believe is creating inefficiencies, impeding coordination of care, or causing other problems affecting quality of care, the ideal next

step is an inquiry to determine whether the policy is truly mandated by HIPAA or another law. If not, a critical assessment of its justification is warranted.

We have argued that the provisions of HIPAA governing protection of patients' information are, in general, consistent with ethical norms, although we would certainly not endorse every detail. Further, we believe that clearing away confusion about what HIPAA requires is important from an ethics perspective and should serve to improve health care quality and promote patient well-being.

Privacy Law and Research

Although the HIPAA framework is consistent with ethical norms governing patient care, its application to modern medical research raises several ethical concerns. In recent years, the landscape of medical research has undergone a dramatic transformation as a result of the explosion in number and scale of clinical trials, the development of increasingly sophisticated techniques for analyzing biospecimens, and the escalation of efforts to store and combine large datasets for analysis. Together, these changes have brought into sharp focus questions about identity, consent, and commercialization that have important privacy implications.

The relationship between HIPAA and the Common Rule. In the context of medical research, there are two main sources of federal privacy protections. The first is HIPAA, which applies to medical research in which (1) the researcher is providing medical care in the course of research and transmits any health information in electronic form, or (2) the researcher is employed by a covered entity, such as a hospital, or a hybrid entity, such as an academic medical center providing medical care in addition to noncovered functions [19]. As described below, the 21st Century Cures legislation, which was approved by the House of Representatives in July 2015 and is currently pending in the Senate, would make several important changes relevant to HIPAA's application to medical research [20].

The second major source of federal privacy protections in medical research is the Common Rule, which applies when a researcher obtains either identifiable private information or data about an individual through an intervention or interaction with that individual [2]. In September of 2015, HHS proposed sweeping changes to the Common Rule that, if adopted, would have important privacy-related implications for researchers [21].

In their current forms, HIPAA and the Common Rule are aligned on several key issues, such as allowing research subjects' broad consent to secondary research use of data and biospecimens. However, the laws differ in important ways, such as the mechanisms they provide for removing identifiers from research data and the specific activities that they exclude and exempt.

The conflicting requirements of these two laws have been perceived by some to add unnecessary complexity to the conduct of medical research [22]. A proposed amendment to the Common Rule is intended to reduce some of this complexity by excluding certain data also protected by HIPAA from protection under the Common Rule [21]. Another amendment to the Common Rule would require researchers to adopt safeguards to protect the security of data and biospecimens used in research, but this requirement could be satisfied by complying with HIPAA's security provisions [21]. Although these proposals, if enacted, would alleviate some administrative burdens associated with satisfying two sets of legal requirements, they also generate new ethical questions.

Do biospecimens have different ethical claims in research than data? Both HIPAA and the Common Rule exclude from protection data and biospecimens that are not identifiable—i.e., they cannot be traced back to individual sources [1, 2]. If one of the major amendments to the Common Rule is adopted, however, any secondary research involving biospecimens would be subject to the protections required by the Common Rule regardless of whether the biospecimens or the information they generate are identifiable [21]. (If the secondary research involves only data, the usual rules would apply, with coverage under the Common Rule turning on the identifiability of the data.)

The change is justified on two ethical grounds. First, it is asserted that the principle of beneficence supports the change because sophisticated analytical techniques, including whole-genome sequencing, have made it possible to re-identify nonidentified biospecimens using publicly available information and free web-based tools [23], although the likelihood of re-identification is widely recognized to be remote. The new rule is intended to minimize the risks of and harms resulting from inappropriate disclosure of information generated from biospecimens. Second, in light of new participatory models of research in which subjects want and expect to be consulted regarding the disposition and use of their biospecimens, respect for persons is claimed to support the change [21].

The question remains, however, whether biospecimens should be treated differently from data in the legal arena. The controversy surrounding the HeLa cell line, which was derived from tumor cells taken from Henrietta Lacks and used in research without her consent, is a poignant reminder of the harms to dignity that can result from unknowing research use of biospecimens [24]. But in that case, researchers made little attempt to hide Ms. Lacks as the source of the cell line, whereas today both HIPAA and the Common Rule provide standards for de-identifying both biospecimens and data [1, 2]. Although reidentification has been shown to be possible in an academic proof-of-concept study [23], even the commentary to the proposed Common Rule amendments acknowledges that the risk of reidentification is not unique to biospecimens but also exists for

information, like whole-genome sequencing data, that is extracted from them [21]. Yet the amendments take the position that such data is not inherently identifiable, while the biospecimens from which the data is generated *are*. The ethical basis for treating these two forms of research (that in which genetic sequencing data is generated and that only involving analysis of the data) differently is unclear and has led to claims of unjustified "biospecimen exceptionalism" [25]. The practical result of this exceptionalism will be to encourage medical researchers to avoid using biospecimens in their studies, even when biospecimen analysis is most suited to their particular research questions.

Is "broad consent" ethically defensible? Another lingering ethical question concerns broad consent to storage and secondary research use of biospecimens and data obtained during research. There is a range of available options for obtaining consent for secondary research use [26], and both HIPAA and the Common Rule have been interpreted to permit broad consent when the secondary research is adequately described. Specifically, HIPAA allows subjects to give informed consent to secondary research use of data [27], and the Common Rule allows subjects to consent to secondary research use of data and biospecimens when they are given a reasonable idea of the types of research that might be conducted in the future and associated risks [28]. But can broad consent ever be truly informed—and therefore ethically acceptable—given that the contexts in which research subjects' biospecimens and private information will be analyzed are not yet known?

If the ethical aim is to respect persons as autonomous agents by consulting them about the future use of their biological samples and private information, it is debatable whether that aim can be achieved when persons are not and cannot be told when, why, or how that future use will occur or what the results will mean for them, their families, or society. Moreover, there is a real possibility that, over time, changed life circumstances and values could cause some persons to weigh their participation in future research studies differently than they did initially [29]. On the other hand, it might demonstrate lack of respect for autonomy to deny people the opportunity to provide broad consent when they comprehend and are comfortable with the attendant uncertainties [30].

Moreover, research on complex diseases involving multiple factors cannot reach statistically significant conclusions without the participation of large numbers of people. To improve health, biospecimens and data must therefore be accessible to as many researchers as possible for use in as many future studies as possible, not all of which can be specified or even predicted at the time of initial consent [31]. In the end, societal interest in promoting public health may trump any ethical claim that private persons should be allowed to participate in only those existing research studies that are known and well defined.

Is it ethical to permit the sale of subjects' health data? Finally, unresolved ethical concerns surround the commercialization of research subjects' biospecimens and private information. The Common Rule does not forbid the sale of these raw research materials [2], although proposed amendments would require consent to research involving biospecimens to include, where applicable, a statement that the biospecimens may be used for commercial profit [21]. HIPAA does prohibit the sale of private health information for most purposes without prior authorization [7], but amendments proposed by the 21st Century Cures legislation would permit it for research purposes [20].

The principle of respect for persons provides reason to question the propriety of allowing such profiteering when research subjects are not notified of the possibility of its occurrence, particularly in light of consistent evidence that patients and the public are distrustful of a major category of potential purchasers and resellers—for-profit entities—in genomic research contexts [30, 32]. The amendments to the Common Rule begin to address this issue by requiring researchers to inform subjects of their intentions to profit from subjects' biospecimens [21]. The reason for declining to extend this requirement to researchers who intend to profit from subjects' private information, however, is unclear. The principle of respect for persons suggests that research subjects should at least be notified of the possibility that their biospecimens *or* personal data could be sold by researchers for profit.

Conclusion

Federal privacy laws describe overlapping but not identical requirements that impact medical practice and research. Although the ethical bases of these laws are sound, their application to particular circumstances sometimes breeds confusion. Moreover, pending amendments to these laws generate difficult ethical questions. A goal of this essay has been to illuminate some of the intersections between privacy law, ethics, and current policy debates.

References

1. Health Insurance Portability and Accountability Act of 1996, Pub Law No. 104-191, 110 Stat 1936. https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf. Accessed February 2, 2016.
2. Protection of human subjects, 45 CFR sec 46.101-46.505 (2016).
3. National Research Council Committee on a Framework for Developing a New Taxonomy of Disease. *Toward Precision Medicine: Building a Knowledge Network for Biomedical Research and a New Taxonomy of Disease*. Washington, DC: National Academies Press; 2011:51.
4. Harman LB, Flite CA, Bond K. Electronic health records: privacy, confidentiality, and security. *Virtual Mentor*. 2012;14(9):712-719.

5. National Library of Medicine History of Medicine Division. Greek medicine. https://www.nlm.nih.gov/hmd/greek/greek_oath.html. Accessed December 21, 2015.
6. American Medical Association. Opinion 5.05 Confidentiality. *Code of Medical Ethics*. http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion505.page?. Accessed December 21, 2015.
7. Standards for privacy of individually identifiable health information. *Fed Regist*. 2002;67(157):53182-53273. Codified at 45 CFR sec 160, 164. https://www.gpo.gov/fdsys/pkg/FR-2002-08-14/pdf/02-20554.pdf. Accessed February 2, 2016.
8. US Department of Health and Human Services. Uses and disclosures for treatment, payment, and health care operations. http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html. Accessed December 21, 2015.
9. US Department of Health and Human Services. Minimum necessary requirement. http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html. Accessed December 21, 2015.
10. Health Information Technology Policy Committee. Report to Congress: challenges and barriers to interoperability. December 2015:9. https://www.healthit.gov/facas/sites/faca/files/HITPC_Final_ITF_Report_2015-12-16%20v3.pdf. Accessed December 21, 2015.
11. Campanelli RM. Letter to health care providers. US Department of Health and Human Services; May 17, 2004:1. http://archive.hhs.gov/ocr/Health care-Provider-letter.pdf. Accessed February 2, 2016.
12. Span P. HIPAA's use as code of silence often misinterprets the law. *New York Times*. July 17, 2015. http://www.nytimes.com/2015/07/21/health/hipaas-use-as-code-of-silence-often-misinterprets-the-law.html. Accessed December 21, 2015.
13. McGee MK. How HIPAA myths block data exchange. *GovInfoSecurity*. October 28, 2015. http://www.govinfosecurity.com/interviews/how-hipaa-myths-block-data-exchange-i-2967. Accessed February 1, 2016.
14. Fisher M. HIPAA myths. *HIE News*. April 30, 2014. http://www.hitechanswers.net/hipaa-myths/. Accessed February 1, 2016.
15. Whaley MP. The 3 biggest HIPAA myths debunked. *KevinMD*. July 17, 2013. http://www.kevinmd.com/blog/2013/07/3-biggest-hipaa-myths-debunked.html. Accessed February 1, 2016.
16. Campanelli, 2.
17. US Department of Health and Human Services. Individuals' right under HIPAA to access their health information: 45 CFR sec164.524. http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html. Accessed January 7, 2016.

18. Senate discussion draft: a bill to improve federal requirements relating to the development and use of electronic health records technology, 114th Cong, 2nd Sess (2016). http://www.help.senate.gov/imo/media/doc/HELP%20Health%20IT%20Bipartisan%20Staff%20Discussion%20Draft.pdf. Accessed February 1, 2016. The bill contains provisions addressing patient empowerment as well as topics such as certification criteria for health information technology and interoperability.
19. National Institutes of Health. Health services research and the HIPAA Privacy Rule. May 20, 2005. https://privacyruleandresearch.nih.gov/healthservicesprivacy.asp. Accessed December 25, 2015.
20. 21st Century Cures Act, HR 6, 114th Cong, 1st Sess (2015). https://www.congress.gov/bill/114th-congress/house-bill/6. Accessed February 2, 1016.
21. Federal policy for the protection of human subjects; notice of proposed rulemaking. *Fed Regist*. 2015;80(173): 53933-54061. To be codified at 6 CFR sec 46; 7 CFR sec 1c; 10 CFR sec 745; 14 CFR sec 1230; 15 CFR sec 27; 20 CFR sec 431; 22 CFR sec 225; 28 CFR sec 46; 29 CFR sec 21; 32 CFR sec 219; 34 CFR sec 97; 38 CFR sec 16; 40 CFR sec 26; 45 CFR sec 46, 690; 49 CFR sec 11. https://www.gpo.gov/fdsys/pkg/FR-2015-09-08/pdf/2015-21756.pdf. Accessed December 23, 2015.
22. Skloot R. Your cells. Their research. Your permission? *New York Times*. December 30, 2015. http://www.nytimes.com/2015/12/30/opinion/your-cells-their-research-your-permission.html. Accessed January 24, 2016.
23. Gymrek M, McGuire AL, Golan D, Halperin E, Erlich Y. Identifying personal genomes by surname inference. *Science.* 2013;339(6117):321-324.
24. Skloot R. *The Immortal Life of Henrietta Lacks*. New York, NY: Crown Publishers; 2010.
25. Emanuel EJ. Reform of clinical research regulations, finally. *N Engl J Med.* 2015;373(24):2299.
26. Grady C, Eckstein L, Berkman B, et al. Broad consent for research with biological samples: workshop conclusions. *Am J Bioeth.* 2015;15(9):34-42.
27. 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. *Fed Regist*. 2013;78(17):5566-5702. Codified at 45 CFR sec 160, 164. https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Accessed December 23, 2015.
28. Secretary's Advisory Committee on Human Research Protections. FAQs, terms and recommendations on informed consent and research use of biospecimens. Department of Health and Human Services; July 20, 2011.

http://www.hhs.gov/ohrp/sachrp/commsec/attachmentdfaq'stermsandrecommendations.pdf.pdf. Accessed December 23, 2015.
29. Trinidad SB, Fullerton SM, Bares JM, Jarvik GP, Larson EB, Burke W. Informed consent in genome-scale research: what do prospective participants think? *AJOB Prim Res*. 2012;3(3):3-11.
30. Spellecy R. Facilitating autonomy with broad consent. *Am J Bioeth.* 2015;15(9):43-75.
31. Husedzinovic A, Ose D, Schickhardt C, Fröhling S, Winkler EC. Stakeholders' perspectives on biobank-based genomic research: systematic review of the literature. *Eur J Hum Genet*. 2015;23(12):1607-1614.
32. Garrison NA, Sathe NA, Antommaria SH, et al. A systematic literature review of individuals' perspectives on broad consent and data sharing in the United States [published online ahead of print November 19, 2015]. *Genet Med.* doi:10.1038/gim.2015.138.

Mary Anderlik Majumder, JD, PhD, is an associate professor of medicine at the Center for Medical Ethics and Health Policy at Baylor College of Medicine in Houston, Texas. Her research focuses on the ethical and social implications of new genomic technologies and ethical and policy questions related to problems of cost, quality, and access in health care.

Christi J. Guerrini, JD, is a research instructor at the Center for Medical Ethics and Health Policy at Baylor College of Medicine in Houston, Texas, and a graduate student at University of Texas School of Public Health. Her research focuses on health privacy, human research subject protections, and the intersection of intellectual property law and genomics.

Acknowledgement
We would like to acknowledge our debt to our colleague, Amy McGuire, whose lectures on privacy and confidentiality have provided the framework for our section on the ethical foundations of privacy law.

Related in the *AMA Journal of Ethics*
New Developments in Human Subjects Protections: Proposed Updates to the Common Rule, December 2015
The Evolution of Confidentiality in the United Kingdom and the West, September 2012
Would Patient Ownership of Health Data Improve Confidentiality? September 2012
Privacy Protection in Billing and Health Insurance Communications, March 2016
Shedding Privacy Along With Our Genetic Material: What Constitutes Adequate Legal Protection Against Harms of Surreptitious Genetic Testing? March 2016