The editors of the Case Studies in Social Medicine are Scott D. Stonington, M.D., Ph.D., Seth M. Holmes, Ph.D., M.D., Helena Hansen, M.D., Ph.D., Jeremy A. Greene, M.D., Ph.D., Keith A. Wailoo, Ph.D., Debra Malina, Ph.D., Stephen Morrissey, Ph.D., Paul E. Farmer, M.D., Ph.D., and Michael G. Marmot, M.B., B.S., Ph.D.

Disclosure forms provided by the authors are available at NEJM.org.

From Rush Medical College (K.P., D.A.A.), DePaul University (F.D.M.), and Metropolitan Chicago Breast Cancer Taskforce (D.A.A.) — all in Chicago.

1. Ansell D, Grabler P, Whitman S, et al. A community effort to reduce the black/white breast cancer mortality disparity in Chicago. Cancer Causes Control 2009;20:1681-8.
2. Rauscher GH, Khan JA, Berbaum ML, Conant EF. Potentially missed detection with screening mammography: does the quality of radiologist's interpretation vary by patient socioeconomic advantage/disadvantage? Ann Epidemiol 2013;23:210-4.
3. Bailey ZD, Krieger N, Agénor M, Graves J, Linos N, Bassett MT. Structural racism and health inequities in the USA: evidence and interventions. Lancet 2017;389:1453-63.
4. Geronimus AT. To mitigate, resist, or undo: addressing structural influences on the health of urban populations. Am J Public Health 2000;90:867-72.
5. Sighoko D, Murphy AM, Irizarry B, Rauscher G, Ferrans C, Ansell D. Changes in the racial disparity in breast cancer mortality in the ten US cities with the largest African American populations from 1999 to 2013: the reduction in breast cancer mortality disparity in Chicago. Cancer Causes Control 2017;28:563-8.

DOI: 10.1056/NEJMp1811499

A Belmont Report for Health Data

Efthimios Parasidis, J.D., M.B.E., Elizabeth Pike, J.D., LL.M., and Deven McGraw, J.D., M.P.H., LL.M.

Legal safeguards for health data are limited in scope in the United States. The Health Insurance Portability and Accountability Act (HIPAA) covers identifiable health information held or transmitted by health plans, health care providers and clearinghouses, and their business associates. However, HIPAA doesn't apply to various other companies or products that regularly store and handle customer health information, including social-media platforms, health and wellness apps, smartphones, life insurers, retailers, credit-card companies, and Internet search engines; HIPAA also places no limits on the use of deidentified data, regardless of who controls the information.[1] Beyond coverage limitations, HIPAA doesn't mandate ethics review for data collection or downstream use. Rather, ethics review is required only if other laws are triggered — specifically, in cases of research on living humans that falls under the Common Rule or research intended to support medical product applications to the Food and Drug Administration. Yet much of contemporary data analytics falls outside these areas — and thus outside mandatory ethical oversight.

The large swaths of data held by digital health pioneers raise a host of ethical concerns related to the reporting of incidental findings, misuse of private information, reidentification of deidentified data, discrimination, and health profiling. Last year, Facebook sought to purchase deidentified patient records, match the records with its identifiable user data, and create digital health profiles of Facebook users — a practice not precluded by HIPAA. Life insurers are transitioning to contracts that instruct policyholders to wear products that continuously monitor their health; companies can increase a customer's premiums on the basis of information gained from this surveillance, but they have no obligation to provide health warnings. Concerns about data use can affect clinical care, particularly when patients seeking to protect their privacy either avoid care or withhold relevant health information from their provider.[2]

Just as indignities common in research in living people led to the articulation of ethical principles in the Belmont Report 40 years ago, we believe contemporary concerns about data use call for stakeholders to promulgate ethical guidance for health data.

Regulations regarding protection of personal data — including the recently enacted General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act — emphasize notification, consent, and deletion rights. But notice and consent, although essential components of data ethics, are insufficient for ensuring ethical use of data. Even under the GDPR's robust protections, research suggests that most Europeans generally click "OK" to accept a company's privacy

terms instead of choosing which data to share.[3] People confronted with end-user license agreements similarly usually click "agree" without reading the legalese. Quick access to a desired product — rather than fastidious deliberation — typically drives these decisions. A legal regime that emphasizes notice and consent provides limited protections and shifts the burden of ethical assessment onto individual users who may not have the time or expertise to make an informed decision.

We believe that data ethics should also incorporate considerations of fairness to individual people and society. Fairness to people who use a product or share their health information requires that data uses align with people's reasonable expectations and be reasonably foreseeable given the context of initial collection. For example, it may be fair to use data collected as part of a workplace wellness program to structure wellness options in ways that improve health, but selling such data to marketers or political operatives — or using them to influence workplace decisions regarding promotions or bonuses — is unlikely to pass ethical muster. Similarly, it may be fair to integrate data collected using wearables into health outcomes research but unethical to use those data for surveillance unrelated to health.

Properly implementing notice and consent is an appropriate first step. Incorporating notification in an ethical way requires using plain language to inform people about data practices. Consent that allows users to opt in or out of data collection — while still granting access to the product or service — also facilitates fair transactions. Other best practices, including "privacy-by-design" principles and "layered notice," promote fairness and increase the likelihood that people will understand the benefits and risks of sharing their data. Such practices involve using privacy-enhancing default settings and summarizing key data-sharing provisions while linking to more detailed information about privacy protections.

Societal fairness dictates that health data be used to advance the public good and not in ways that cause or exacerbate inequities.

Societal fairness dictates that health data be used to advance the public good and not in ways that cause or exacerbate inequities. For example, social-media data mining can be used to support public health surveillance. In addition, it may be ethical to collect and use data on social determinants of health to facilitate public health initiatives but not to set insurance premiums or redline neighborhoods out of coverage. In short, data stewards can be mindful fiduciaries.

A majority of people believe that there should be limits on the use of their health data. People generally are concerned less about who uses their data than about how the data are used.[4] Public health and medical research are widely viewed as legitimate uses, whereas marketing, advertising, and research unrelated to health are not.

Meaningful ethics review can take many forms. Some hospitals and data brokers have established data ethics officers who consider ethical issues beyond HIPAA compliance and seek to foster responsible use of data. We know of only a handful of such institutions, however, and no studies have examined the number or effectiveness of data ethics officers. Moreover, the success of this approach depends on an officer's ability to identify and communicate ethical concerns and an organization's willingness to respond appropriately.

Federal agencies are expected to use disclosure review boards to appraise data-release protocols. The National Institute of Standards and Technology — an arm of the Department of Commerce — recommends that such boards consider legal and ethical issues. But disclosure review boards don't examine data collection or use and thus don't consider the full spectrum of ethical concerns.

Universities and institutions could expand the role of institutional review boards (IRBs) or data and safety monitoring boards to include assessing data-related projects for which ethics review isn't legally required. This approach would require both a sub-

stantial expansion in mandate for IRBs beyond human-subjects research and additional expertise, given the breadth and depth of data-related projects.

Another option would be to implement reviews that focus exclusively on data ethics, which could be performed by data ethics review boards. Such boards — which could be adopted in public and private settings — would review projects in which health data are collected, analyzed, shared, or sold. They would consider the benefits and risks of proposed data use; the protocols and societal impact of the project; and policies governing data access, privacy, and security. Members could include project developers, data analysts, ethicists, and data-subject representatives.

Ethics review forums are clearly not a panacea. Data ethics review boards and data ethics officers are subject to "capture," just as IRBs are sometimes regarded as formalistic entities that protect institutions more than research participants.[5] For ethics review to be meaningful, the interests of the institution should not usurp the interests of people whose data are collected and society as a whole. One option for overcoming these pitfalls would be to implement legal accountability for ethics review, whereby courts could evaluate the legitimacy of ethics review findings and whether organizations appropriately adhered to reasonable recommendations.

Existing health privacy laws leave the market for data analytics unconstrained by ethical considerations. Ideally, laws and regulations would require all stakeholders to assess the potential ethical concerns associated with their activities. More promptly, regulators could issue guidance encouraging structured ethics review during deliberations regarding data collection, sharing, and analysis. In the absence of legal requirements or official guidance, organizations can lead by instituting meaningful ethics review. Although there are costs associated with incorporating ethics review into data deliberations, doing so can help foster trust in the data enterprise, prevent societal backlash, and encourage data sharing, thereby allowing important medical and technological advances to proceed.

Disclosure forms provided by the authors are available at NEJM.org.

From the Moritz College of Law and the College of Public Health, Ohio State University, Columbus (E. Parasidis); the Office of the Chief Information Officer, Department of Health and Human Services, Washington, DC (E. Pike); and Ciitizen, Palo Alto, CA (D.M.).

1. Cohen IG, Mello MM. HIPAA and protecting health information in the 21st century. JAMA 2018;320:231-2.
2. Malin BA, Emam KE, O'Keefe CM. Biomedical data privacy: problems, perspectives, and recent advances. J Am Med Inform Assoc 2013;20:2-6.
3. Mayer-Schönberger V, Ramge T. A big choice for big tech: share data or suffer the consequences. Foreign Affairs. September/October 2018 (https://www.foreignaffairs.com/articles/world/2018-08-13/big-choice-big-tech).
4. Grande D, Mitra N, Shah A, Wan F, Asch DA. Public preferences about secondary uses of electronic health information. JAMA Intern Med 2013;173:1798-806.
5. Grady C. Institutional review boards: purpose and challenges. Chest 2015;148:1148-55.

DOI: 10.1056/NEJMp1816373

Diabetes and Disclosure

Kaitlyn K. Rogers, B.S.

Three surgeons and a medical student stand around the operating table. An attending and a surgical resident are working on the patient's left side. The third surgeon, another attending, maintains tension on the suture as I close the long incision on the patient's right. It's the last week of my third-year surgical rotations but the first time I've met any of these men. So after the expected questions about anatomy, indications for surgery, and alternative treatments, the conversation turns to the personal: Where am I from? What did I study? Do I want to be a surgeon?

"I like surgery," I tell them, "but I'm actually leaning toward family or internal medicine."

"Really?" one of the attendings asks, surprised.

"Really," I reply as I start my next stitch. "About 80% of the time I think I want to go into primary care, and the other 20%