



# KEEPING YOUR GENES PRIVATE

In spite of recent legislation, tougher laws are needed to prevent insurers and employers from discriminating on the basis of genetic tests

By Mark A. Rothstein

## KEY CONCEPTS

- Genetic testing will expand quickly and soon, adding highly targeted data to people's medical records. As those records go electronic, outsiders will find it increasingly easy to peruse an individual's health information.
- Able to uncover private details, health and life insurers could deny coverage to someone with a complex medical condition, and employers could fire or refuse to hire the person to avoid burdening the company health plan.
- Existing laws offer weak protection at best; legislation is needed to give individuals more control over their own data, to limit unauthorized disclosures by others and to penalize wrongdoers.

—The Editors

In years gone by, if colon cancer ran in your family all you could do was wait and worry about whether you might get it, too. Today a genetic test can determine whether you have inherited a greater-than-average risk of the disease and so could benefit from preventive care. The more doctors know about your genes, the better able they are to prevent, treat or cure illnesses.

Excitement about such prospects surrounded the start of the Human Genome Project in 1990. But the enthusiasm was soon tempered by widespread concern about the need to protect the privacy of a person's genetic information. Simple tests that could readily reveal an individual's genetic endowment could also readily cause embarrassment or stigma. Furthermore, insurers could deny people health coverage or raise the premiums they have to pay. And employers seeing the results could deny people jobs or fire them. At the same time, scientists and public health officials recognized that the potential to improve health care based on genetic studies across large populations could never be achieved if legions of people refused to participate out of fear that the results could be misused.

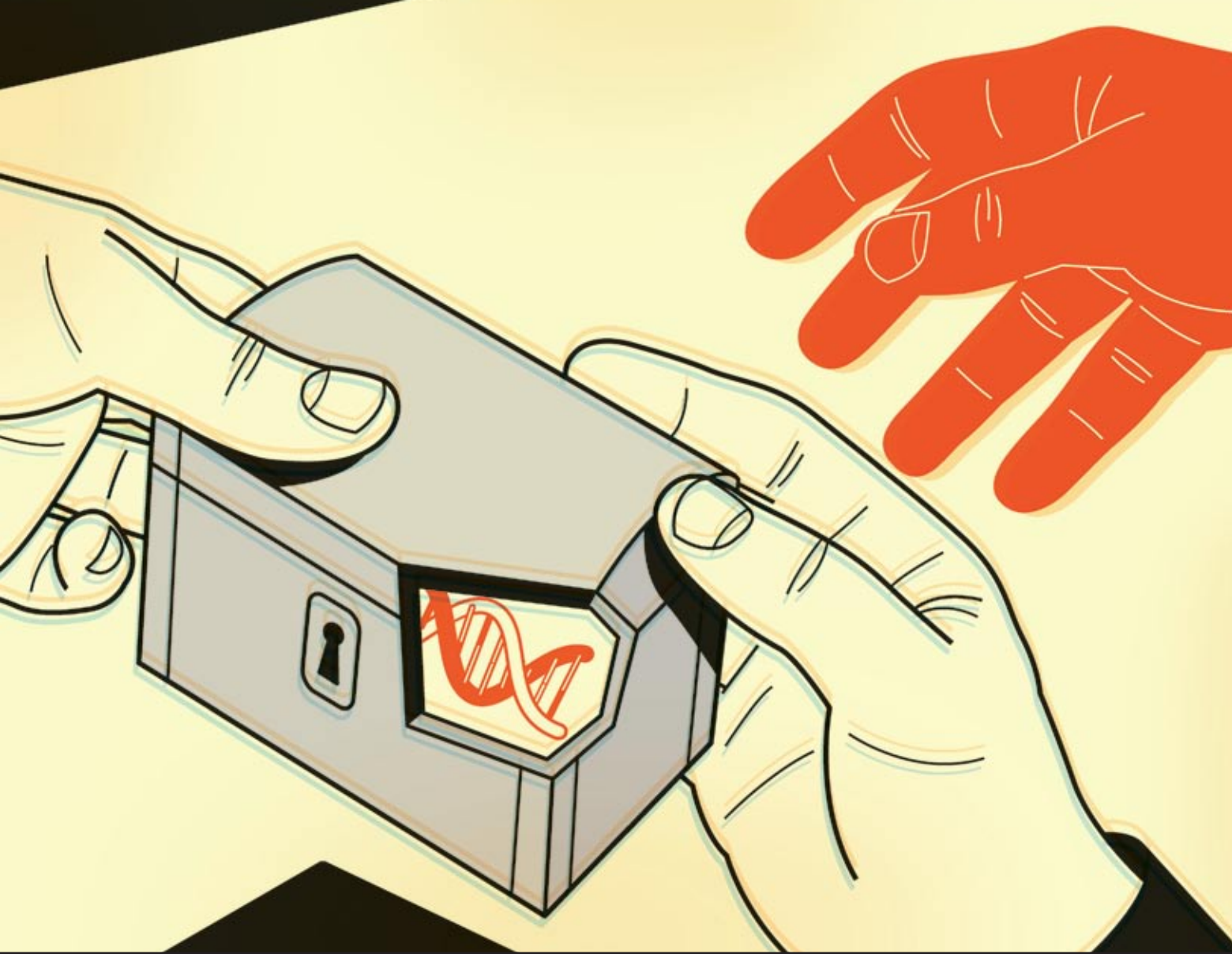
Worries about discrimination have not come true—yet. Even though the Human Genome Project was completed in 2003, genetic testing has not become widespread, so there is little in the average person's health record to divulge.

And genome-wide analyses remain costly—as much as several thousand dollars each. What is more, scientists still lack standard techniques for making whole-genome scans useful for health risk assessment.

Nevertheless, in many societies—particularly the wealthy ones—genetic testing for multiple disorders will soon become routine. New technologies and scientific discoveries are making the tests more useful and affordable. The health care sector's sweeping transition from paper to electronic records will also make genetic information more readily accessible. Safeguarding genetic privacy is more complicated than many people realize, and recently enacted laws such as the 2008 Genetic Information Nondiscrimination Act offer little protection. Better regulations must be developed soon, before testing spreads and abuses grow.

## More Information Everywhere

Figuring out how best to secure genetic privacy would be simpler if “genetic information” and “genetic conditions” were easy concepts to define. But they are not. Medical investigators are finding that almost all illnesses have a genetic component. Distinguishing between genetic and nongenetic health information is becoming increasingly meaningless. Yet policymakers have been inclined to give special protection to genetic information. For legal purposes, the



most common definitions include the results of an individual's genetic tests, those of his or her family members, and the health histories of all these people (because disorders that run in families typically have a genetic link).

The data that fit into these categories are expanding noticeably. In the past decade genetic research and its clinical applications have shifted from disorders linked to a single gene, such as cystic fibrosis and muscular dystrophy, to more common and complex ills characterized by the interactions of multiple genes and environmental factors, including asthma, cancer, cardiovascular disease and diabetes. More than 1,500 genetic tests are now in use, and hundreds more are being developed. As these tools become part of standard medical practice, including primary care, most, if not all, health records will contain substantial genetic information.

Genome-wide analyses could vastly expand those contents. These tests can look for single changes in hundreds of thousands of nucleotide

bases—the famous A, T, C and G “letters” of DNA code—associated with particular illnesses and conditions. Although most scientists think that it is premature to apply this technology routinely, some companies such as 23andMe in Mountain View, Calif., and deCODE Genetics in Reykjavik, Iceland, have started aggressively marketing genome-wide scans, even if they do not have a license to operate as a medical laboratory. Within a decade, whole-genome sequencing that reads all three billion bases in human DNA might well be available for less than \$1,000.

At least two other factors will add to the amount of information in health records. The great desire for personalized medicine—drug therapies tailored to each person's body to improve effectiveness and reduce side effects—depends on genome-wide analytical tools. This “pharmacogenomic” testing is already becoming standard practice in selecting drugs and doses for treatment of certain cancers, and the trend

HARRY CAMPBELL

will continue. Likewise, “toxicogenomics”—the use of genome-wide tools to study how individuals respond to toxins—is becoming more important in assessing a person’s health risks in the workplace and in the general environment.

### Networks Amplify Risk

The challenge of protecting health information is compounded by an increasing reliance on digital data. Medical records of all kinds are shifting from largely paper-based systems to electronic health records (EHRs), which should improve the quality of care and reduce its cost. The transition is under way in many developed countries. In the U.S., a Nationwide Health Information Network (NHIN) is being developed as a “network of networks.” Its key goal is establishing electronic formats that will make records of all kinds compatible and thus easy to transport across networks and across the country. Ultimately, a person’s EHR will include all his or her medical information from “cradle to grave.” The Office of the National Coordinator for Health Information Technology in the Department of Health and Human Services is leading the NHIN’s development, but state governments and the private sector are engaged in research, development and trial implementation.

The NHIN raises contentious issues. In a paper-based system, privacy is mainly protected by chaos. Precisely because the system is fragmented, people find it impossible to compile, or even to locate, an individual’s records from a multitude of providers in different locations over extended periods. But comprehensive, longitudinal records will inevitably contain sensitive information. Individuals will no longer have the option of “selective recall” in giving facts to health care providers or of obtaining care from one provider without the knowledge of another. Unlike today, an old diagnosis of depression made at a college mental health clinic or the results of a genetic test taken because of family history will become a permanent part of one’s EHR. Many people with conditions that might stigmatize them, such as a history of substance abuse, might delay or forgo treatment. Such a result could be disastrous for individuals and for public health.

### INTRIGUED BUT WARY

According to a May 2008 Knowledge Networks survey:

Forty-seven percent of Americans are interested in using online personal health record services such as Google Health or Microsoft HealthVault. The services allow consumers to control their own medical records online.

Ninety percent of the respondents, however, indicated they would be wary about the services’ ability to keep records private.

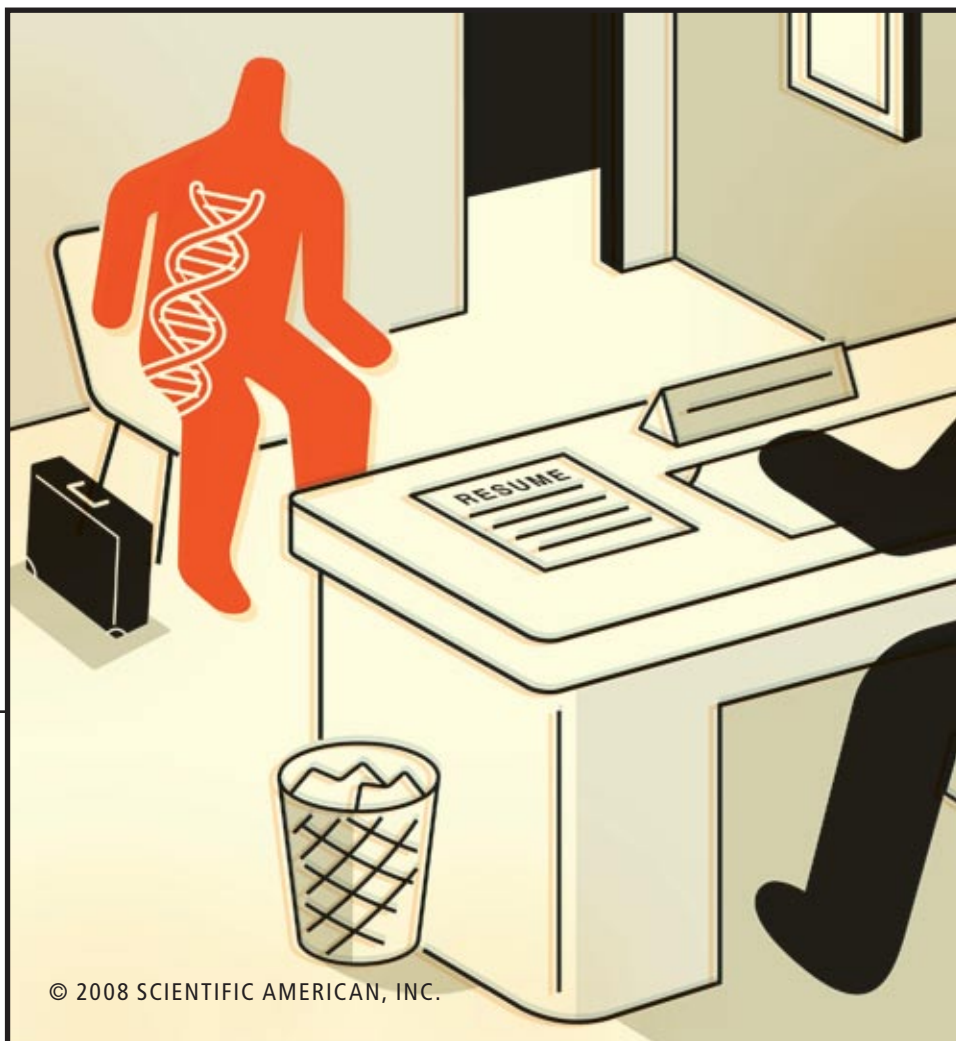
In response, the Markle Foundation has recommended ways to make such systems as private as possible. Provisions would allow consumers to audit who is accessing their medical data and to dispute information provided by health care providers.

A full report is not needed to render effective care, however. A physician treating a sprained ankle does not need to know if a patient has a predisposition to breast cancer. A dentist filling a cavity does not need to find out about a family history of Huntington’s disease.

To protect patients from unnecessary disclosures of sensitive information, countries such as Canada, the Netherlands and the U.K. are considering ways to restrict which information is revealed to which health care providers. These measures include giving patients complete control of their health records, permitting individuals to remove certain old information, limiting disclosures only to details needed for a given diagnosis or type of provider, applying special rules to sequester especially sensitive information, creating a subset of basic health data that would be available to all providers and establishing independent health record banks to disclose files according to a patient’s direction. In Denmark’s EHR network—one of the most advanced—people can “block” any information in their records. Although this option is rarely exercised, it is greatly valued.

The U.S. has no such measures in place. This

HARRY CAMPBELL



**People fear they might not get a job if they could be a burden to the company medical plan.**



past February the National Committee on Vital and Health Statistics (which advises the secretary of health and human services) recommended that individuals be able to prevent the routine disclosure of sensitive health information in predefined categories, such as domestic violence, substance abuse, mental health, sexually transmitted diseases and genetic information. But methods for doing that have yet to be created. And how to strike the right balance between broad and narrow disclosure remains unclear. If patients have too much control, physicians will not have confidence in the accuracy or completeness of the records. In response, they will likely feel compelled to retake histories and order new tests, undermining the efficiencies of networks and adding cost to care. On the other hand, if patients have too little control, many may engage in defensive steps such as opting out of networks, paying cash for off-record services or declining certain care altogether.

Other issues must also be resolved. For example, should privacy rules be set for systems that scan electronic records and advise clinicians on possible drug interactions, so the systems do not divulge actual drugs taken? Should health care providers see an electronic notation in a patient's file indicating that certain health information has been made unavailable at the patient's request? And in such cases, will doctors have a way to lift those restrictions if the person needs emergency care?

### Weak Laws

With more genetic information and far-reaching electronic networks on the horizon, legislation protecting health privacy is essential. Unfortunately, comprehensive laws do not exist in the U.S. The closest thing to a national safeguard is the 1996 Health Insurance Portability and Accountability Act (HIPAA) and the 2003 Privacy Rule attached to it. The Privacy Rule spells out the permissible uses and disclosures of individual health information by providers, plans and record clearinghouses.

There is a big loophole, however: the Privacy Rule applies only to entities that handle health claims data electronically. Hundreds of thousands of providers still do not, including doctors who take cash payments exclusively, fitness clubs that ask for medical information when putting members on workout plans and health care providers who work under contract to third parties, such as personnel in on-site employer clinics. A related problem is the lack of enforce-



## Should Family Members Be Warned?

**S**arah, a 40-year-old mother of three, has found out from various tests that she has an elevated risk of Alzheimer's disease, as well as of breast cancer. Does she have a legal or moral obligation to tell her children or close relatives that they, too, might be at high risk of getting these illnesses in the future?

The legal issue is straightforward: no court has held an individual liable for failing to warn a relative about genetic test results. The moral issue depends on many factors, including the severity of a genetic condition, the number of years before it is likely to produce symptoms, and whether the condition is treatable. The nature of relationships (parent and child) and their emotional closeness matter, too, as do relatives' ages, their interest in knowing about the chance of future ills, and the individual's own concern about not divulging his or her personal problems.

The nature of the danger often plays a strong role. In rare cases, genetic conditions can be lethal if combined with environmental stressors. For example, individuals with the genetic mutation for malignant hyperthermia can die during surgery if certain anesthesia is used. People with hypertrophic cardiomyopathy can suffer sudden death from strenuous exercise. The potential for these types of harm warrant notifying at-risk relatives.

Yet sharing one's genetic information with family members can be perilous. Testing may reveal, for instance, that the man everyone thought was a child's father actually is not, sending a family into turmoil. Genetic counselors can help people decide whether to undergo genetic testing and how to respond to possible results, but currently only 2,500 counselors practice in the U.S. The most common mistake is getting tested and waiting for results before considering what to do. Anyone contemplating testing should determine in advance whether to share the results with close relatives. There is no simple answer. The best advice is to consult with professionals and think ahead about the possible consequences.

—M.A.R.

ment. About 36,000 complaints related to the Privacy Rule were filed with the Department of Health and Human Services's Office for Civil Rights between April 2003 and May of this year. Although corrections were made, only one civil monetary penalty has been assessed to date. Wrongdoers face few deterrents.

In addition, HIPAA only applies to entities involved in health care. The public, however, is most worried about stigma or discrimination from others. People fear complications when applying for a job, obtaining a life insurance policy or filing for workers' compensation benefits. Yet it is common for administrators involved in these and other everyday situations to require people to sign an authorization directing their provid-

ers to release their health information. According to one estimate, at least 25 million such authorizations occur every year in the U.S.

The parties requiring the disclosures are usually acting lawfully. And one's health can have legitimate bearing on decisions. An electric power company, for example, would not want to hire someone who is prone to seizures to fix wires at the tops of utility poles. The problem is the amount of information disclosed. The electric company has no need to know whether a job applicant has a genetic mutation that may increase susceptibility to heart disease decades from now. Judging a worker's compensation claim for a broken leg does not require reproductive health information. An automobile insurance adjuster handling a claim for a chipped tooth sustained in an accident does not need any genetic test result. But most of the laws authorizing disclosure of health information are written so broadly that no limits are placed on the scope of the requests.

Ironically, EHR networks could solve this problem. Software programs could scan electronic records and select only the data related to a specific inquiry. Yet this capability requires the use of "contextual access criteria"—software algorithms specifying that, for an inquiry of type X, only data A, B and C are needed. For example, contextual access criteria would disclose only information bearing on mortality risk to a life insurer. This technology is feasible but not yet available. And because commercial demand alone probably will not provide adequate incentives to develop the technology, laws may be needed to require it.

## Legislation of Little Help

Given the general weakness of federal regulations, various state legislatures have enacted their own protection laws. In so doing, the states have adopted the notion of "genetic exceptionalism"—that genetic information is treated differently from other forms of sensitive health information. Whether this approach is desirable is an open question, but it parallels how some mental health, substance abuse and HIV information is handled.

Although the laws vary, 12 states require people to give written, informed consent for a genetic test, and 27 states require express consent to disclose test results. Nevertheless, these laws, like the federal regulations, continue to allow insurers and employers to legally require individuals to sign an authorization for the release of their

## GENE DETAILS COMING SOON

**The 1000 Genome Project, an international research consortium started this year, intends to create a map of the human genome that is five times more detailed than the one created by the International HapMap Project.**

**HapMap discoveries spawned the recent explosion of genome-wide studies that have identified more than 130 genetic variants linked to a range of diseases, including type 2 diabetes, coronary artery disease, prostate and breast cancers, rheumatoid arthritis and mental illnesses.**

**In the next three years the 1000 Genome Project hopes to sequence the genomes of at least 1,000 people drawn from populations around the world. For more see [www.1000genomes.org](http://www.1000genomes.org)**

### [THE AUTHOR]



**Mark A. Rothstein** is chair of law and medicine and director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine. From 2001 to 2008 Rothstein chaired the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics, which advises the U.S. secretary of health and human services.

medical information. As a result, 47 states have laws that prohibit insurers from denying or restricting coverage or charging different rates, based on an individual's genetic information. HIPAA already covers these cases for people in employer-sponsored group health plans, however, so the state laws in effect only extend protection to people who buy individual insurance.

Other laws in 35 states prohibit employers from requiring a genetic test as a condition of employment and from using predictive genetic information to deny an individual a job. Yet after a conditional offer of employment, the laws allow an employer to require prospective employees to authorize the release of their health records as a condition of being hired. The states differ on whether genetic information may be disclosed at this time, but that provision is largely immaterial: it is impracticable for anyone to excise genetic information from paper records and equally infeasible to exclude it from electronic records until the contextual access algorithms are devised.

Given such shortcomings, Congress has been under increasing pressure to improve privacy. In May members finally passed the Genetic Information Nondiscrimination Act (GINA), which had been pending since the mid-1990s. The act prohibits health insurance companies from discriminating in providing coverage, and in setting rates, on the basis of genetic predispositions. Unfortunately, the legislation is not much better than or even different from many state laws, and it doesn't cover life, disability or long-term care insurance.

## Universal Solutions

The flaws in GINA, HIPAA and state regulations are not loopholes or oversights. They are the natural result of a health care system in which individual coverage is medically underwritten [see "Reflections on Privacy 2.0," by Esther Dyson, on page 50]. People in the U.S. can obtain insurance in one of three ways: a group health plan such as that offered by most employers, individual insurance, or federal programs such as Medicare and Medicaid. For group and individual plans, underwriters calculate the individual or collective health risks of those covered and impose premiums based on the relative risk they represent. Of course, one prime purpose is to protect the financial interests of the insurer. Insurers want to know about each person's past ailments and the possibility of future illnesses (genetic and otherwise) so they can bet-



## Canada and the Netherlands may give patients complete control of their health records.

The U.S., though, is unlikely to adopt universal health care anytime soon, even though it is front and center in the 2008 presidential campaign. Thus, better privacy laws must be enacted, even though some observers say new genetic technologies add little threat to privacy. Although very few legal cases have been brought over discrimination in employment or health insurance, almost all medical geneticists and genetic counselors know of numerous patients who have declined to undergo genetic testing because they feared possible discrimination or stigma. (According to Francis S. Collins, former director of the National Human Genome Research Institute, one third of eligible people decline to participate in genetic research because they fear discrimination.) Furthermore, the number of genetic tests and the number of people taking them, along with the tests' usefulness, will increase significantly in the next decade. And EHR networks will make it easy to disclose the information widely with the click of a mouse.

As the U.S. and other countries contemplate better ways to deal with genetic information, policymakers are seeing that protecting privacy is neither cheap nor easy. Improved security measures can keep information from being disclosed without authorization, but restricting the scope of authorized disclosures is equally important. It is essential, and challenging, to decide which individuals and entities have a right to which information and for what purposes.

Effective legislation should, at minimum, include four elements. First, it should address the underlying difficulties in gaining access to health insurance and carefully balance the rights of employers and employees. Second, legislation should limit nonmedical uses of predictive health information, including for life insurance, disability insurance and long-term care insurance. Third, any legislation should limit the scope of disclosures, penalize wrongdoers and provide remedies for people harmed by wrongful disclosures. And fourth, EHRs and EHR networks should be designed so that they can limit disclosures to relevant health information. Tackling these matters will provide an effective first step toward shaping the future of medical privacy. ■

ter determine price and ward off those who might make huge claims.

None of the privacy laws mentioned apply to Medicare or Medicaid, because technically these programs are entitlements, not insurance. Different laws attempt to protect information within these programs, but the government has no real incentive to look at anyone's genetic information because there are no rates to adjust.

Indeed, concerns about keeping information private are best addressed by a national system of universal health care, as in Canada. In universal plans, risk is spread across the entire population, and the plan is funded by the entire population. Whether any given person has a high risk for any disease has no bearing on the equation, so there is no incentive for others to seek protected information. The situation eliminates people's two greatest worries: that they will have trouble obtaining or will be dropped from health insurance, and that they will be denied a job because their medical conditions could impose a burden on the company's health plan.

Complications in obtaining life insurance must still be addressed, however. And health information still has to be made secure so records are not stolen or improperly disclosed. But the big incentives to discriminate largely disappear.

### ➔ MORE TO EXPLORE

**Genetic Privacy: A Challenge to Medico-Legal Norms.** Graeme Laurie. Cambridge University Press, 2002.

**Genetic Privacy.** Pamela Sankar in *Annual Review of Medicine*, Vol. 54, pages 393–407; 2003.

**Genetic Exceptionalism and Legislative Pragmatism.** Mark A. Rothstein in *Hastings Center Report*, Vol. 35, No. 4, pages 27–33; July/August 2005.

**Ensuring the Privacy and Confidentiality of Electronic Health Records.** Nicolas P. Terry and Leslie P. Francis in *University of Illinois Law Review*, pages 681–735; 2007.