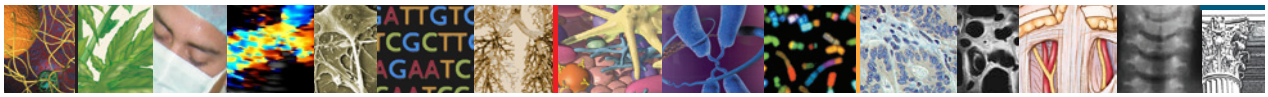

The NEW ENGLAND JOURNAL of MEDICINE

Perspective

Turning the Tables — The New European General Data Protection Regulation

Charlotte J. Haug, M.D., Ph.D.

"Action required: Make sure you receive important information!" was the alarming message my Internet service provider recently sent me. It turned out they wanted me to review my privacy settings — or, really, to agree that they could continue using data about me just as they had before. People throughout Europe have been inundated with such messages over recent weeks. Almost every Web page or app you open presents you with a pop-up window and an "I agree" button that must be hurdled before you can buy your train ticket, access your music, or browse content. Why this sudden concern about privacy settings? The reason is the General Data Protection Regulation (GDPR), a new European privacy law that will be fully enforced this summer.[1] Given that the regulation was proposed in 2012 and adopted in May 2016, it should come as no surprise that it has become fully enforceable throughout the European Union (EU) now, after a 2-year grace period.

The regulation enshrines in law the principles of protection of privacy and personal data that have been internationally agreed on since 1980.[2,3] Because these principles have previously been expressed only in guidelines and directives, they have often been conveniently overlooked for commercial, regulatory, and practical purposes. As of May 25, 2018, that's no longer possible.

Commercial companies are at least acknowledging that the regulation involves a fundamental change in data ownership and control from organizations to consumers. Consumers of all kinds, including patients, must now give their explicit consent for use of their personal data — and can withdraw it at any time. The health care sector and the health research community have been surprisingly quiet, although they collect exactly the type of data the GDPR aims to protect. For example, explicit consent for participating in a single trial will still be enough for the primary analysis of trial data, but secondary analysis or data sharing for analysis by others will probably be impossible without new consent. Patients will have the right not only to see and obtain, but also to correct and erase electronic health records, as well as to know how and why the data are stored and used. There must also be ways for patients to know which data end up in health registries and public health databases, and for what purposes.

The GDPR makes for stronger,

unified data protection throughout the EU. Organizations will be accountable for the personal data they hold and collect from EU residents. Individuals can request a copy of the personal information any company keeps on them and find out what data are being processed and for what purpose. They also have the right to data portability, so they can take data from one entity and give it to another, and the "right to be forgotten." The new law requires entities to gain affirmative consent for any data collected, and violators could face fines as high as 4% of their global annual revenue or €20 million, whichever is higher. The regulation forces us to rethink how we do business, particularly in medicine, where collection, storage, and analysis of personal data are central to clinical practice, clinical research, and public health.

The timing is nearly perfect. Given the Cambridge Analytica scandal and other wake-up calls about misuse of personal digital data, the public is increasingly aware of the kind of data reality we inhabit. Our digital fingerprints are ubiquitous, continuously generated, and processed with lightning speed. There is nearly limitless data-storage capacity, and data can be transferred, combined, and accessed from practically anywhere. Smart algorithms can mine data sets to find patterns and personalize recommendations. The potential value is huge — commercially, politically, and scientifically. But so are the potential harms. These realities highlight questions about who owns and controls data, who gets the benefits, and who takes responsibility. Until now, personal data have typically been expropriated from individuals. In medicine, health records, clinical trial data, and surveillance data have been considered the property of physicians, provider organizations, scientists, private companies, and health authorities. The GDPR is turning the tables by giving European citizens more explicit control of their own data.

Organizations facing this regulation can pursue three main strategies. The first is to try to ignore it, do as little as possible, find ways to convince your customers that their data are safe with you, and continue business as usual. The second is to stop doing business with anyone in Europe. The third is to embrace the law's intention by recognizing that people's personal data are their own and that you will need permission to use them — and will need to be able to explain exactly how you intend to use and store them.

So far, the first option seems to be the preferred strategy. Big tech companies such as Facebook, Google, and Amazon are adjusting their privacy settings to at least partly comply with the GDPR. But they are doing it half-heartedly: in April, Facebook changed its terms of service to move users in Asia, Africa, and Latin America under Facebook Inc. in California rather than Facebook Ireland, where users might have been protected under the GDPR. The companies also try to make it inconvenient for users to deny consent for data use. For example, when I reviewed my privacy settings for Facebook and said I would not let them use face recognition, I was warned that they wouldn't be able to help me if somebody tried to steal my online identity. And my Internet service provider told me that if I didn't consent to their use of my data, "You will only receive information about products you already own, not about exciting new products and services." Why?

The second possibility — stop doing business with Europe — might lead to rapidly shrinking opportunities to do business at all. For example, the Chinese government recently released the final version of a new national standard on personal information protection. It contains detailed regulations for user consent and for collection, storage, and sharing of personal data. Although it's unclear how and when this regulation will be implemented, it contains even stricter requirements than the GDPR.

A key concept in the GDPR is "privacy by design." The concept and its guiding principles were developed in the 1990s by the former information and privacy commissioner of Ontario, Ann Cavoukian, but they are only now becoming part of a legal requirement. Privacy by design calls for inclusion of data protection from the outset in designing systems and makes it clear that consumers own their data and have the power to make corrections. The consumer is also the only one who can grant and revoke consent for data use.

Constructing and maintaining large health care databases that comply with the GDPR will be complicated. So perhaps the third strategy is both the most feasible and the most interesting. Turn the tables: make all patient data the patient's by default, and store only data that are absolutely necessary. Doing so is not impossible but will require changes in the way we think about health

data. Now, such data are something somebody else — a physician, a hospital, a researcher, a government, an insurance company — collects, owns, and uses to provide you treatment, discover something new, or send you a bill. You may or may not be allowed to see these data, but you have little control over how they are used. Giving the patient ownership and control doesn't necessarily mean the data need to be formatted differently or stored somewhere new. But it means, for example, that a hospital cannot automatically share data with an insurance company or other providers — and it will have to give the patient all the personal data they have about her, should she switch to another provider.

Blockchain and Cloud technologies have made it possible to think seriously about a health record under personal control — a MyHealthRecord where patients can see their health-related information and share it with the clinicians and scientists they choose. Blockchain is a decentralized digital ledger technology that records transactions. It's best known for its use in cryptocurrencies such as Bitcoin but has other potential uses — including improving privacy by giving users a way to own, and closely control and monitor, their personal data.[4,5]

"We know what's best for you and what's the best use of your data" doesn't sound so reassuring anymore, whether the message comes from Facebook, Google, health authorities, physicians, or researchers. The GDPR may lead to a shift to viewing patients as collaborators and giving them the tools to manage their own health and participate in clinical trials on their own terms. If so, it may help advance both medical science and health care delivery.

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

Dr. Haug is an international correspondent for the *Journal*.

This article was published on June 6, 2018, at NEJM.org.

1. EU General Data Protection Regulation portal (https://www.eugdpr.org).
2. Organisation for Economic Co-operation and Development. OECD guidelines on the protection of privacy and transborder flows of personal data (http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm).
3. European Union. Directive no. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (http://www.wipo.int/wipolex/en/details.jsp?id=13580).
4. Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using Blockchain for medical data access and permission management. Presented at the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, August 22–24, 2016 (https://ieeexplore.ieee.org/document/7573685/).
5. Czeschik C. Blockchains: a cure for the e-health record problem? Dotmagazine. June 2017 (https://www.dotmagazine.online/issues/innovation-in-digital-commerce/what-can-blockchain-do/blockchains-a-cure-for-the-e-health-record-problem).

DOI: 10.1056/NEJMp1806637