Clinical Trial Data

Negotiating the Tension Between Transparency and Privacy

Many scientists in fields involving clinical research reacted with concern when then-U.S. Environmental Protection Agency (EPA) Administrator Scott Pruitt signed a proposed rule that would require individual patient-level data for studies pivotal to EPA actions to be publicly available. “The era of secret science at EPA is coming to an end,” Pruitt said. Press Release, EPA Administrator Pruitt Proposes Rule to Strengthen Science Used in EPA Regulations (April 24, 2018). Opponents noted that most of the largest epidemiological studies had been performed under informed consents that had not contemplated that individual patient-level data would be shared with third parties. See J. Eilperin & B. Dennis, Pruitt to Unveil Controversial Transparency Rule Limiting What Research EPA Can Use, The Washington Post (Apr. 24, 2018).

Pharmaceutical and medical device companies conducting clinical trials face similar calls to make data publicly available, similar allegations of “secret science,” and similar issues with regard to individual patient-level data and informed consent. Proponents for access argue that requiring disclosure of information about clinical trials prevents duplication of unsuccessful or unsafe trials. Moreover, they argue that systematic disclosure of results of all clinical trials eliminates the ability of sponsors, researchers, and manufacturers to release partial information selectively about the results of studies via scientific publications, abstracts, and press releases:

“Communities have expressed concern about the lack of publications from clinical trials (regardless of outcomes) and bias in the literature, which may be due to selective reporting by trial sponsors or by journals in response to manuscripts that they deem less interesting.” Comments to 2016 HHS Rule, 81 Fed. Reg. at 64,985. Supporters of open access argue that open data mean better science.

Making individual patient-level data available for other research presents companies with challenges, but researchers and companies can take steps to minimize the risks.

By Ronni Fuchs, Donna L. Fisher, and Samuel J. Abate, Jr.

Ronni Fuchs, Donna L. Fisher and Samuel J. Abate, Jr., are partners in Pepper Hamilton’s Health Sciences Department, a team of 110 attorneys who collaborate across disciplines to solve complex legal challenges confronting clients throughout the health sciences spectrum.
At the same time, there has been growing recognition of the need to protect individuals’ private data. The identification of the alleged Golden State killer from a relative’s DNA sample provided a warning about the potential use of personal information; it showed that sharing one’s own DNA permits matching to relatives’ DNA—even from crime scenes. Here is another cautionary tale: the Harvard Personal Genome Project posts information about volunteers on the internet to help researchers gain new insight about human health and disease. Volunteers’ names do not appear, but the profiles list medical information, including illegal drug use, alcoholism, depression, sexually transmitted diseases, medications, and DNA sequences. Some of the volunteers provided ZIP codes, dates of birth, and gender information. Dr. Latanya Sweeney, director of the Data Privacy Lab at Harvard, was able to identify 42 percent of these individuals by combining those three pieces of data with information from public records. A. Tanner, Harvard Professor Re-Identifies Anonymous Volunteers from public records. A. Tanner, Harvard those three pieces of data with information percent of these individuals by combining vacuity Lab at Harvard, was able to identify 42 Latanya Sweeney, director of the Data Pri-vation, including illegal drug use, alcoholism, sexually transmitted diseases, medications, and DNA sequences. Some of the volunteers provided ZIP codes, dates of birth, and gender information. Dr. Latanya Sweeney, director of the Data Privacy Lab at Harvard, was able to identify 42 percent of these individuals by combining those three pieces of data with information from public records. A. Tanner, Harvard Professor Re-Identifies Anonymous Volun-teers in DNA Study, Forbes (Apr. 25, 2013). Sweeney performed earlier research showing that she could identify up to 87 percent of the U.S. population with just ZIP codes, birthdates, and gender information.

There are, of course, other numbers. Around 1.13 million patient records were compromised in 110 health-care data breaches in the first quarter of 2018, according to data released on May 3 in the Prote-nus Breach Barometer Report. F. Donovan, 110M Records Exposed by 110 Healthcare Data Breaches in Q1 2018, Cybersecurity News (May 7, 2018).

Approximately 270,000 people used a Facebook app in 2014 to take a personality test for “academic research purposes,” which—because of Facebook’s terms of service and its application programming interface at the time—permitted the app’s developer to collect information about users’ Facebook friends. The app’s developer obtained data from up to 87 million users, which he shared with political consulting firm Cambridge Analytica. H. Tut-tle, Facebook Scandal Raises Data Privacy Concerns, Risk Management Magazine (May 1, 2018).

These disturbing examples define the issues that data privacy is meant to address: The personal information of millions of individuals was collected or used in ways that they were not made aware of, did not consent to, and over which they had no control. These stories, and the European Union General Data Protection Regulation (GDPR), have increased public awareness of data risks, as well as calls for heightened privacy.

The competing values of data transparency and data privacy can conflict, creating tension for parties conducting clinical trials. This article examines the momentum for, and the reach of, increasing transparency demands and the competing privacy obligations imposed on companies. It also discusses how these issues arise when clinical trial data are sought in litigation. The article concludes with suggestions that companies should consider in meeting these competing demands.

The Momentum for Transparency
Several circumstances have driven the momentum toward transparency. These include the call for information about clinical trials from patients, clinical trial registration expansion, and a movement toward open access to clinical trial results and data, among others.

Clinical Trial Registration
The U.S. clinical trial registry, ClinicalTrials.gov, was launched in 2000 to meet the Food and Drug Administration Modernization Act of 1997 requirement that the National Institutes of Health (NIH) create a public information resource on clinical trials to include information about clinical trials conducted under investigational new drug applications. At that time, with the country still in the throes of the AIDS crisis, the call for information about clinical trials was largely coming from patients, who advocated for an accessible resource to find clinical studies in which they might participate.

As views about the public need (or public right in the case of public-funded studies) for information about clinical trials evolved, the clinical trial registry became more focused on clinical trial results.

The purpose of clinical trial registration is to prevent selective publication and selective reporting of research outcomes, to prevent unnecessary duplication of research effort, to help patients and the public know what trials are planned or ongoing into which they might want to enroll, and to help give ethics review boards considering approval of new studies a view of similar work and data relevant to the research they are considering.

See ICMJE Recommendations, Clinical Trial Registration, 2005.

The Food and Drug Administration Amendments Act of 2007 (FDAAA) made registration of most prospective controlled clinical trials beyond Phase 1 trials mandatory. See 42 U.S.C. §282(j)(1)(A) (defining ”applicable clinical trials”). The FDAAA also mandated disclosure of specific information for the registration, including the study’s primary purpose, the study’s design, the primary disease or condition being studied, and the study start and completion dates.

In 2016, the U.S. Department of Health and Human Services (HHS) and the NIH expanded the scope of trial registration. 42 C.F.R. §11.48(a). These rules require all qualifying investigators or sponsors that are conducting clinical trials either regulated by the FDA or funded partially or wholly by the NIH to file information and data about results on ClinicalTrials.gov—even when the studied product is not
approved, licensed, or cleared by the FDA. In addition, the public registration must include the full protocol and statistical analysis plan for the trial.

In the 2017 changes to the Federal Policy for the Protection of Human Subjects (known as the “Common Rule”), the HHS mandated the posting of informed consent forms for federally funded trials to a public website, although final details regarding the requirement are unresolved. See Fed. Reg. Vol. 82, No. 12 (Jan. 19, 2017) (implementation delayed).

This push for more transparency is consistent with the policies of the European Medicines Agency. The European Medicines Agency has its own database, the European Clinical Trials Database (EudraCT), which includes information on clinical trials taking place in the European Union and clinical studies conducted worldwide in accordance with a pediatric investigation plan. A subset of the data is publicly accessible via the European Clinical Trials Register.

Clinical Trial Results and Data
As the clinical trial community was adjusting to trial registration, there was also a movement toward open access to clinical trial results and data. In 2003, the NIH concluded that data from NIH-supported research should be shared. While the precise mechanism for data sharing was not prescribed—it could be through publishing, investigator responses to data requests, availability in a controlled environment in which researchers could perform analyses using the data, data archives, or a mixture of the above—the rationale was clearly stated:

We believe that data sharing is essential for expedited translation of research results into knowledge, products, and procedures to improve human health. The NIH endorses the sharing of final research data to serve these and other important scientific goals. The NIH expects and supports the timely release and sharing of final research data from NIH-supported studies for use by other researchers.


In addition to broadening the categories of clinical trials for which registration was required, the 2007 FDAAA required summary results for applicable clinical trials that began after September 2007 to be posted to ClinicalTrials.gov within one year after completion of the trial. Required information included tables of specified information (i.e., participant flow, baseline characteristics, outcome measures and statistical analyses, and adverse events information).

The movement toward making additional clinical trial data available continues. The 2016 HHS rule expanding the scope of trial registration also expanded the summary results obligations. Thus, for studies with primary completion dates on or after January 18, 2017, in addition to the results tables previously required, sponsors must submit three adverse event tables summarizing (1) all serious adverse events grouped by organ system, with the number and frequency of each event by arm; (2) all other adverse events that occurred with a frequency of five percent or more in any arm of the trial; and (3) all cause-mortality data by arm. 42 C.F.R. §11.48(a)(4). Adverse event tables must include information about events that occurred, regardless of whether the event was anticipated or unanticipated. 2016 Comment, 81 Fed. Reg. at 64983.

Similarly, posting clinical trial summary results in EudraCT became mandatory for sponsors as of July 2014. The European Medicines Agency’s policy on publication of clinical data, along with previously implemented policies, requires the submission of clinical overviews, clinical summaries, and clinical study reports, along with specific appendices, including protocol and protocol amendments, sample case report forms, and documentation of statistical methods, all of which will be posted.

In addition, European Medicines Agency’s Policy 70, adopted in 2014, mandates for data submitted to the agency in support of a marketing authorization that certain anonymized study-related documents (called “clinical reports”) will be made publicly available on EMA’s website. In the future, Policy 70 envisions that individual patient-level data for these studies will also be made available. Anonymized clinical reports are available for many products; the individual patient-level data publication process under Policy 70 has not yet begun.

Sharing Individual Patient-Level Data
Several clinical trial sponsors have pioneered the sharing of clinical trial data, including individual patient-level data, and advocacy in support of such sharing is growing. In an unprecedented step in data sharing, in 2011, Medtronic provided to Yale University’s Open Data Access Project de-identified individual patient-level data from its sponsored clinical trials for rhBMP-2. In addition to providing a grant to Yale to permit two fully independent, third-party systematic reviews of these data, Medtronic made the individual patient-level data available to additional researchers through Yale’s defined registration process and website. Other companies also began making individual patient-level data available to researchers.

In July 2013, the European Federation of Pharmaceutical Industries and Associations (EFPIA) and the Pharmaceutical Research and Manufacturers of America (PhRMA) jointly endorsed principles for responsible clinical trial data sharing. Under these principles, member pharmaceutical companies agreed to dramatically increase the amount of information available to researchers, patients and members of the public by committing to the following:

Patient-level clinical trial data, study-level clinical trial data, full clinical study reports, and protocols from clinical trials in patients for medicines approved in the United States and European Union...
will be shared with qualified scientific and medical researchers upon request and subject to terms necessary to protect patient privacy and confidential commercial information.


In June 2017, the ICMJE issued a statement on data sharing for clinical trials that expressed the belief that “there is an ethical obligation to responsibly share data generated by interventional clinical trials because trial participants have put themselves at risk.” D. B. Taichman, Data Sharing Statements for Clinical Trials: A Requirement of the International Committee of Medical Journal Editors, N. Eng. J. Med. 376:2277–2279 (June 8, 2017).

As a result, ICMJE requires, as a condition of any consideration for publication of a clinical trial report, that (1) as of July 1, 2018, manuscripts submitted to ICMJE journals must contain a data-sharing statement and (2) clinical trials for which enrollment starts after January 2019 must include a data-sharing plan in the trials’ registration.

Id. The data-sharing statements must indicate (1) whether de-identified individual patient-level data will be shared; (2) which data will be shared; (3) whether additional documents, such as the study protocol and statistical analysis plan, will be available; (4) when the data will be available; and (5) under which access criteria data will be shared. Id.

This article focuses on data privacy and consent issues in sharing clinical trial information. Data sharing raises additional issues, including potential exposure of competitively sensitive information, misuse of data, and significant costs of data de-identification. These issues are beyond the scope of this article, though we note that many vehicles for data sharing contain measures to address them. Both ClinicalTrials.gov and the European Medicines Agency website, for example, provide some protections for commercially sensitive information. Data-use agreements contain limitations and conditions for obtaining and using data; some require submission of a scientific protocol and a statement of intent to publish any results from data analysis. Data-sharing sites generally permit companies to refuse certain requests, including, as the PhRMA/EFPIA principles suggest, a competitor’s request for proprietary information. Data-sharing sites can also help address cost because they provide infrastructure for handling requests and for data hosting.

The Evolving Obligation to Protect Private Information

As computers and personal devices have revolutionized the way that records and data are collected, stored, and shared, countries have passed vigorous laws to protect data privacy and security. In discussing these evolving laws, we focus on developments in the United States and the European Union. Countries outside the United States and European Union have their own privacy laws, which also have been strengthened to meet increasing privacy and security concerns. For example, in Canada, many federal, provincial, and territorial privacy statutes govern the protection of personal information, including the Personal Information Protection and Electronic Documents Act and a comprehensive data-breach notification statute, effective November 2018.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA was enacted on August 21, 1996, with the dual goals of making health care delivery more efficient through use of electronic health records and expanding health insurance coverage. HIPAA also mandated the development of nationwide security standards and safeguards for the use of electronic health care information as well as the creation of privacy standards for protected health information (PHI). See HIPAA Privacy Rule (Privacy Rule), codified at 45 C.F.R. §§160, 164. The primary purpose of the Privacy Rule is to protect individuals’ privacy while allowing necessary but controlled access to their PHI.

The Privacy Rule generally prohibits the unauthorized use or disclosure of PHI by “covered entities,” including health care providers, pharmacies, health insurers, and health-care clearinghouses and their business associates acting on behalf of covered entities that use or transmit PHI for any HIPAA-related transaction. Under the Privacy Rule, a covered entity or business associate may not use or disclose PHI unless the individual provides written authorization, including a description of the nature of the information collected and how it will be used or disclosed. Authorization for the disclosure of PHI for research purposes must also identify a specific research study and must contain certain core elements and required statements, such as the right to revoke authorization and that the patient’s PHI may no longer be protected once it is disclosed by the covered entity.

The Privacy Rule permits research to continue without an individual’s authorization if the PHI has been de-identified by removing all 18 HIPAA identifiers, or through an expert’s statistical analysis when the expert confirms that there is a “very small” risk of re-identification, and there is no actual knowledge that the individual could be identified. Alternatively, an Institutional Review Board (IRB) may grant an authorization waiver when (1) the research cannot practically be conducted without the disclosure of the PHI, and (2) there is minimal privacy risk. Another
exception to requiring an authorization involves a limited data set, where limited types of indirect identifiers (e.g., date of birth, dates of treatment) may be accessed by a researcher as long as the researcher and the covered entity sign a data-use agreement that describes the permitted uses and disclosures. Finally, use and disclosure without authorization is permitted if required by law or for public health reasons, such as adverse-event reporting to the product’s sponsor or the FDA.

In January 2013, the Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §300jj et seq., expanded the reach of the HIPAA Privacy and Security Rules by extending HIPAA liability directly to business associates to whom PHI is disclosed, more broadly defining “business associate” to include subcontractors of business associates, adding mandatory new data breach rules reducing the threshold for reporting HIPAA breaches, and increasing noncompliance penalties. 42 U.S.C. §17921 et seq. Failure to comply with HIPAA can result in civil and criminal penalties.

### GDPR

In 1996, the European Union promulgated the Data Protection Directive, 95/46/EC, which established basic principles for privacy legislation for EU member countries. The directive was based on recommendations of the Organisation for Economic Cooperation and Development. Unlike HIPAA, the Data Protection Directive broadly defined personal data to be protected as all information related to an identifiable person, not just health-care data.

While the directive sought to protect personal data for individuals in the European Economic Area, because it was adopted as an EU directive, each EU member state had significant leeway in implementing its own national data protection law. The result was a patchwork of inconsistent obligations relating to personal data across the European Union. To address these and other issues with the directive, in 2016, the European Union adopted a new data privacy regulation, the General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 (now adopted by all 31 European Economic Area member nations).

The highly publicized GDPR—which replaces the Data Protection Directive—took effect on May 25, 2018. The GDPR applies not only to businesses located within the European Union, but also to businesses outside the European Union if they process personal data of individuals in the European Union. It therefore applies to U.S. pharmaceutical and medical device companies with clinical research subjects in the European Union. The GDPR provides the following rights for individuals: (1) the right to be informed; (2) the right of access; (3) the right to rectification; (4) the right to erasure; (5) the right to restrict processing; (6) the right to data portability; (7) the right to object; and (8) rights in relation to automated decision making and profiling. Companies subject to the GDPR need to have processes in place to ensure that when data are handled the data remain protected, either through encryption; anonymization, which is the removal of identifiable information; or pseudonymization, where data components are anonymized and separated.

To ensure compliance with the GDPR, companies need, among other things, a data protection officer, who is responsible for overseeing data security strategy and GDPR compliance, if they process or store large amounts of EU citizen data, process or store special personal data, regularly monitor data subjects, or are a public authority. The GDPR also mandates reporting of data breaches within 72 hours. The Fortune 500 companies, including major pharmaceutical and device companies, were expected to spend at total of $7.8 billion complying with the GDPR, according to a recent Ernst & Young survey. Failure to comply with the GDPR carries significant penalties, up to a maximum of the greater of 4 percent of global revenue or €20 million. Indeed, the Facebook incident has led to a cottage industry of commentators estimating Facebook’s presumptive liability had the GDPR been in effect when the data harvesting occurred.

### California Privacy Act

In June of this year, California joined the drive to broaden protection of individual’s privacy rights to the global standard, thus setting the new US data privacy high watermark by enacting a Privacy Act (the CA Privacy Act), which will become effective in January 2020. The CA Privacy Act provides several GDPR-style individual rights to consumers, and applies to qualifying businesses worldwide that sell in the California market. Qualifying businesses are for-profit entities (a) with annual gross revenues over $25 million that collect consumers’ personal information, or on whose behalf consumers’ personal information is collected, or (b) that obtain the personal information of at least 50,000 consumers annually. The CA Privacy Act requires businesses to safeguard consumer’s personal information and permits a private right of action and statutory damages if a consumer’s unredacted or unencrypted personal information is subject to unauthorized access and exfiltration, theft or disclosure as a result of a business’s violation of the duty to secure that data. It also imposes a duty on qualifying businesses to ensure supply-chain compliance, to require their service providers to delete the personal information of any consumer whose personal information was deleted at the consumer’s request.

### Effect of Informed Consent on Data Sharing

While data privacy is not the first thing that most people think of when they hear the words “informed consent,” consent must address how a study participant’s privacy will be protected. Any public access to clinical trial data must be compliant with principles governing informed consent, including principles that apply to deidentified data.
As data sharing becomes more common, informed consent should include a discussion of the parties’ desire to retain the participant’s data after the study is completed for possible use in future projects by the investigator or others. The consent form should state that identities might be removed; note that de-identified information may be used for future research; and advise the participant of what will happen if he or she revokes consent at a later date.

Historically, informed consent forms did not discuss future use of data, let alone the possibility that unknown third parties might be permitted access to data. Indeed, seeking to comply with regulations and ensure that subjects were informed about the various entities that might access their data, traditional sponsor-drafted informed consents frequently named the specific entities (e.g., the sponsor, FDA, and IRBs) with which data may be shared. See, e.g., 21 C.F.R. §50.20 (FDA requires informed consents to include statements describing the confidentiality of the information collected during the clinical trial, how records will be kept, and the possibility that FDA and others outside the study may review the records). Some consents implicitly or even explicitly limited the disclosure to these entities.

Depending on their wording, these “traditional” informed consents may present barriers to data sharing from studies to which they applied. Under U.S. law, if information privacy risks to U.S. subjects are minimized, an IRB can waive the need for any additional consent to share data. The Common Rule, which applies to human research performed under the HHS (but does not directly apply to research performed with FDA approval), has long permitted a researcher to seek waiver of informed consent for “minimal risk” research—that is, when the research involves no more than minimal risk to the subjects. 45 C.F.R. §46.116(d). In July 2017, the FDA announced in guidance that because it plans to promulgate new regulations to permit waiver for minimal risk studies, it would not object to IRBs’ waiving informed consent for studies performed under FDA approvals. Therefore, when an informed consent is silent pertaining to whether there may be future use of the data, IRBs may approve waivers for minimal risk studies using de-identified patient-level data.

If the informed consent implicitly or explicitly limits access to the data, however, IRBs (or the company itself) may not be able to permit access. A September 2016 EFPIA and PhRMA survey showed that for their members with systems in place to share de-identified individual patient-level data, a leading reason for refusing to share data in specific instances was that the informed consent for the clinical trial did not allow data sharing.

**Data Access in Litigation**

Plaintiffs asserting product liability claims against drug and medical device manufacturers often seek all clinical trial data relating to the involved drug or device. Allegations purporting to require these data range from claims of hidden clinical data to misreporting of results. In some cases, plaintiffs have gone so far as to seek individual patient-level data. In doing so, they not only argue that full disclosure of individual patient-level data is required to ensure that the study was accurately reported, but also that permitting them access to individual patient-level data will create better science (or “is compelled by public health”) by allowing their experts to perform their own analyses.

All of the difficulties of individual patient-level data production, including de-identification, still apply in the context of litigation. Despite arguments to the contrary, properly de-identifying individual patient-level data is costly and time-consuming. The increased public awareness of the implications of privacy breaches may help courts understand the importance of data de-identification. Defendants should also educate courts about the burdens of de-identifying data and should use proportionality arguments when available. See Fed. R. Civ. P. 26(b)(1). In addition, defendants should propose shifting of the cost of de-identifying data to plaintiffs if individual patient-level data is required.

Finally, as for plaintiffs’ arguments that their experts must be permitted to adjudicate the science “in the public interest,” litigation is a poor avenue for such a venture. Even organizations at the forefront of open access generally support access to the data for scientific research purposes—but not for litigation experts. See, e.g., ICMJE Data Sharing Statement, NEJM 376:2277-2279 (June 8, 2017) (discussing sharing for research purposes); Press Release, EFPIA-PhRMA Rules for Clinical Trial Data Sharing Active (Jan. 1, 2014) (data will be shared “with qualified scientific and medical researchers upon request and subject to terms necessary to protect patient privacy and confidential commercial information”).

**Best Practices for Sharing De-Identified Patient-Level Clinical Trial Data**

As the above demonstrates, there are competing obligations imposed on parties responsible for clinical trials to make data publicly available but also to comply with the multiple privacy statutes or regulations, some of which carry significant penalties for noncompliance. The growing expectation for more organic data at the patient level will only increase the challenge. Companies conducting clinical trials should consider the following.

**For future trials:** Consent for the future use of de-identified data should be included in informed consents and should be unambiguous. Subjects should be told of their

**Transparency**, continued on page 93
right to revoke consent for this use and the consequences of revocation.

For existing trials: If a company is seeking to share individual patient-level data from trials with informed consents that do not address data sharing, and if the participants are all in the United States, the company can satisfy HIPAA by removing all 18 HIPAA identifiers, or through an expert's statistical analysis when the expert confirms that there is a “very small” risk of re-identification. Under recent FDA guidance, a company can also seek an IRB waiver for additional use of the data as presenting minimal risk of harm to the participant (including his or her privacy). For study participants in the European Union, a company must consider whether there are similar options to share individual patient-level data collected in earlier trials.

Consider the vehicle for data sharing. There are several established sites for sharing and using data from clinical trials and other scientific research. Most are controlled sites, where researchers who seek access to individual-level data are required to enter into a data-sharing agreement. Data-sharing agreements generally include requirements to protect participants’ privacy and data confidentiality, and they may prohibit the recipient from transferring the data to other users or require that the data be used for research purposes only, or both. Many prohibit a researcher from trying to use the data to “re-identify” subjects. Established sites include the following:

• ClinicalStudyDataRequest.com: A consortium of 14 major pharmaceutical companies that facilitates access to patient-level data from clinical studies;
• Yale Open Data Access Project: A university-based organization that facilitates access to clinical trial program data for pharmaceutical and medical device companies;
• Supporting Open Access for Researchers (SOAR): A university-based collaboration to facilitate access to patient-level data from clinical studies.

Use data-sharing agreements to address additional concerns. Data-sharing agreements can include additional restrictions beyond privacy. For example, the European Medicines Agency’s clinical data website permits a user access only upon agreement that data will not be used for commercialization purposes. Other sites require submitting a protocol to a gatekeeper, who reviews it for scientific merit.

Ensure data de-identification. Data de-identification is not an easy process. Both direct and indirect identifiers need to be considered. Direct identifiers include information such as a participant’s name, initials, email address, and postal code. Indirect identifiers include information such as demographic, biological, and geographic data that if combined, might lead to identification. Consider reducing the risk by hiring a consultant who can perform a statistical analysis to confirm there is a very small risk of re-identification.

Recognize that there are instances in which data cannot be shared. There may be instances in which data simply cannot be shared, including these:
• When data cannot be sufficiently anonymized to safeguard patient privacy, particularly when there are small clinical trials, such as rare disease trials.
• When the obtained informed consents explicitly preclude data sharing.

Conclusion
Data transparency is highly valued; it permits researchers to have faith in clinical trial results. Making individual patient-level data available for other research, however, presents companies with challenges—including potential data privacy risks to clinical trial subjects and the costs of ameliorating that risk. There are steps being taken to ease some of these challenges for future trials: new informed consent forms are being debated and designed, and best practices for de-identification are being developed. At the same time, caution suggests that more powerful computer technology and larger databases will increase the risk of re-identification of research subjects, and we receive daily reports of data privacy breaches. Sponsors of clinical trials remain at the intersection of these forces.