Bloomberg BNA

Privacy and Security Law Report®

EU-U.S. Privacy Shield

Health-Care Data Transfers

The EU-U.S. Privacy Shield data transfer program will have a substantial impact on how many U.S. companies will be able to receive data from Europe and on how data can be transferred and used, the author writes, noting that although some health-care companies may find the program useful, others may be unable to participate or find compliance too difficult.

Impact of the EU-U.S.Privacy Shield on Health-Care Data Transfers

By Kirk J. Nahra

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, specializing in litigation and counselling related to privacy, data security and cybersecurity in the U.S. and across the globe. He chairs the firm's Privacy Practice and co-chairs its Health Care Practice. He represents companies in virtually every industry in navigating the complexities of privacy and security laws and regulations, across industries and jurisdictions. He can be reached at 202.719.7335 or knahra@wileyrein.com. Follow him on Twitter @kirkjnahrawork.

Health care used to be local. You went to the neighborhood doctor for your physical or to a pediatrician for your kids. If something went wrong, there was a local hospital. You got insurance, if at all, through your employer, who likely went through the local Blue Cross Blue Shield plan. These entities were all independent, and data sharing between these entities was largely limited to sending in claims information so doctors could get paid.

As with most industries, times certainly have changed. Your doctor is part of a large physician group. Your hospital is owned by a national conglomerate. The health insurer may have merged several times. Managed care has made data even more important, and increased movement towards ''accountable care'' and risk sharing have exploded the need to share data. At the same time, we now have electronic health records, personal health records, health information exchanges, mobile applications, wearables and more, all collecting and sharing our health information, for a broad variety of public and private purposes.

Beyond these developments, health care also is becoming global. The health insurer may have a call center in India. The latest drug is being developed by a company from Europe, using physicians and patients across the globe. Researchers everywhere are developing new health care protocols and exploring the efficacy of new treatments. Your employer is managing health-care costs across its full employee population, which often covers multiple continents.

 ISSN 1538-3423

In the U.S., we are familiar in the health-care industry with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and Security Rule, which govern the sharing of health information among ''covered entities'' (doctors, hospitals and other health-care providers and health plans) and their ''business associates'' (service providers). We also are aware that there are gaps in this structure, driven by the limited scope of the HIPAA rules and the emerging new sources for health-care data. *See* Kirk Nahra, ''Moving Toward a New Health Care Privacy Paradigm,'' *Privacy in Focus* (November 2014).

We haven't always paid as much attention to the international role in privacy law for the health-care industry. But we need to, as the business of health care is expanding globally and the number of countries with strong privacy rules is growing consistently. There is ambiguity, inconsistency and constant evolution, creating the need for smart, effective privacy officers at health care companies (and companies in virtually all industries).

The latest wrinkle involves the need to find a way to transfer data from one country or region, regulated by one set of laws, to another country, such as the U.S., in a way that complies with all of the applicable laws. For more than a decade, an effective program had been built to transfer individually identifiable data from the European Union to the U.S. Called the ''Safe Harbor'' program, this self-certification program provided a means for more than 4,000 companies to transfer data to the U.S., across a wide range of industries, including health care.

Health care also is becoming global. The health insurer may have a call center in India. The latest drug is being developed by a company from Europe, using physicians and patients across the globe.

Recently, in October 2015, the European Court of Justice (ECJ) struck down the Safe Harbor program, driven primarily by concerns about the U.S. government's access to personal data that was transferred under the program (14 PVLR 1825, 10/12/15). Corporate panic ensued, followed by massive uncertainty.

Now, after several months of teeth gnashing, the U.S. government and the EU recently announced the launch of ''EU-U.S. Privacy Shield,'' the new and improved Safe Harbor program, designed to meet the concerns raised by the ECJ and others (15 PVLR 269, 2/8/16). While lots of uncertainty remains (mainly how will the court address this new program in the face of the expected new lawsuit challenging it and how various countries will respond), companies in all industries are evaluating whether to participate in the new Privacy Shield program as a means of ensuring the appropriate ability to transfer data from the EU to the U.S.

What does this all mean for the health-care industry? What are the key areas for consideration? And will this program help or hurt privacy rights for individuals and the ability of the health-care system to improve treatment and make the system more efficient? While we have lots to continue to digest and analyze about the Privacy Shield program, and there is both an ''annual review'' process for the program (with the primary privacy oversight group in Europe already staking out its ground to make this a meaningful review) and the likely need for additional change based on the new EU privacy law that is coming into effect in 2018, the health-care industry needs to be thinking today about how this program will affect both individual businesses and the overall operation of the health-care system.

The Program Will Be Challenging for Everyone

The primary goal of the Privacy Shield program is to improve on the privacy protections that were created for the Safe Harbor program. This means that it will be harder to meet the challenges of the Privacy Shield program, individuals will have more rights, overall monitoring and compliance will be more significant, and the risks of enforcement will be greater. This does not at all mean that companies should not pursue Privacy Shield certification, but it does mean that this is a meaningful effort that will require a significant review of a company's overall privacy activities and protections.

There Will Be Additional Challenges if You Were Not Part of the Safe Harbor Program

For the companies that participated in the Safe Harbor program, the Privacy Shield certification will follow many of the same steps, with additional requirements and the broader need for stringent assessment and oversight. It is a significant modification to Safe Harbor, but not a wildly different framework. For those companies that did not participate in the Safe Harbor, however, the Privacy Shield will be a significant mountain to climb. It will require companies to review overall data collection activities across the business, to identify what personal data is collected from the EU, how it is used, and to whom it is disclosed. It will require the development of specific kinds of policies and procedures, a detailed privacy notice, new contracts with vendors and an overall monitoring program to evaluate the privacy activities on an ongoing basis. Many companies will undertake this effort, and will find it beneficial for the overall business activities. But this initial consideration of whether the Privacy Shield is worth the effort for your company is a significant question that will require thoughtful analysis and a meaningful assessment of available alternatives.

The EU-U.S. Privacy Shield will require a significant review of a company's overall privacy activities and protections.

Privacy Shield Won't Work for Health Insurers

One of the limits of the Privacy Shield program is that only companies subject to regulation by specified U.S.

  PVLR ISSN 1538-3423

government agencies are eligible for the program. These agencies—for now—are limited to the Federal Trade Commission (FTC) and the Department of Transportation. That means that there are substantial gaps in who can even participate in this program. One major gap for the health-care industry involves insurers—who are subject to state regulation and generally are not subject to enforcement from the FTC (insurers may be able to participate as employers for their own employee data if needed). So, to the extent that U.S. health insurers need to receive individual information from the EU—and many will, related to vendors, travelers, international operations or the like—the Privacy Shield does not present a means of accomplishing that transfer. There may be other approaches, but this one will not work for health insurers.

Non-Profits Also Will Have Issues

Also, the FTC's jurisdiction generally does not extend to non-profit organizations. So, for the many hospitals and other entities that operate—in a corporate sense—as non-profits, the Privacy Shield also is not an option. While many of these non-profits may be smaller organizations that do not engage in meaningful data transfer with the EU, this obviously will impact larger health-care providers who operate on a non-profit basis.

Obtaining Consent Will Be More Difficult

One of the alternatives to the Privacy Shield is to obtain the consent of the individual to the transfer. In addition, one of the Privacy Shield requirements includes the need for consent for certain data transfer in certain situations. In general, the intersection between the new EU data protection rules (stemming from the General Data Protection Regulation (GDPR) going into effect in 2018) and the Privacy Shield is to make consent a more challenging option in every respect. Also, the intersection of these two developments will both expand the situations where consent may be needed, and increase the complexity of obtaining meaningful consent consistent with the applicable rules.

Sensitive Information

At the same time, consent requirements and data protection rules generally are more significant across the board for ''sensitive'' information, which includes health-care information. There is some subtlety to this point, as what is considered ''health information'' may be more specific and narrow under these rules than the term would be under HIPAA, where any information about an identified patient or insured (including name, address and the like) is considered ''protected health information'' even if it says nothing specific about someone's health. But, it will certainly be much more challenging in general to transfer health information than other ''less sensitive'' information about individuals. Under the Privacy Shield provisions, certifying organizations ''must obtain affirmative express consent (opt in) from individuals'' if this ''sensitive'' information is to be disclosed to a third party or used for purposes beyond which it was originally collected. While this will not require consent for disclosures to business associates, there will be interesting and challenging questions about the variety of other third parties who may receive information (and the purposes for these disclosures), particularly in the context of HIPAA's long list of ''public policy'' disclosures (e.g., health care oversight, public health, litigation, etc.).

Research

One of the key areas for data transfer involves health-care research, where information about patients in a broad range of geographic settings may be useful for research projects in the U.S. and elsewhere. Although the Privacy Shield includes some specific provisions related to research (and consent often may be a viable option in research settings), the need to develop appropriate transfer mechanisms for research activities will be a significant challenge. In addition, while the Privacy Shield provisions recognize the usefulness of personal data for beneficial research, the primary ability to use personal data obtained for one study in another context is dependent on whether ''appropriate notice and choice'' have been provided in the first instance.

Privacy Shield Certification May Complicate Business Associate Relationships

One of the key expanded protections from the Privacy Shield involves the ''onward transfer'' provision, which regulates how data that is transferred to the U.S. is subsequently transferred by the recipient to other entities, in the U.S. or elsewhere. These onward transfer requirements require specific kinds of contractual requirements and ongoing monitoring of vendors and others who receive information. The Privacy Shield is simply different than the contractual requirements for business associates under HIPAA. This may require companies to re-evaluate existing agreements, to modify them consistent with the onward transfer provisions, and to adopt more aggressive monitoring of vendors beyond the existing HIPAA provisions.

Although the EU-U.S. Privacy Shield does incorporate the idea of individually identifiable information (as does the new General Data Protection Regulation), it provides a less certain path to making information "de-identified."

De-Identification issues

One alternative to any data transfer program is to ensure that the data being transferred is not subject to existing data protection rules. Under HIPAA, this kind of action would involve ''de-identification'' of protected health information subject to the specific HIPAA requirements. Although the Privacy Shield does incorporate the idea of individually identifiable information (as does the new GDPR), it provides a less certain path to making information ''de-identified.'' Therefore, compa-

nies wishing to bypass Privacy Shield requirements due to de-identification will need to re-evaluate how to ensure appropriate de-identification consistent with the EU and Privacy Shield standards, which are different than the existing HIPAA framework.

Alternative/Different Enforcement

The ability to certify under the Privacy Shield is dependent on the ability of the Federal Trade Commission to take enforcement action against an entity for violation of the Privacy Shield commitments. Therefore, for any health-care entity subject to the HIPAA rules as a covered entity or business associate, the FTC will become an independent enforcement agency in connection with the commitments made under the Privacy Shield (which may be similar to and overlap with HIPAA, but which are different). Although HIPAA-regulated entities should be aware of the FTC's view that it already can take action against HIPAA entities based on the FTC's own privacy and security principles (as they did in the longstanding and controversial LabMD Inc. case (14 PVLR 2185, 12/7/15)), the Privacy Shield will make the FTC's enforcement ability explicit, and will define the standards that underlie any enforcement activity. The Department of Commerce also will have jurisdiction to engage in proactive audits and to evaluate complaints against participating companies.

Conclusion

Overall, the Privacy Shield program will have a substantial impact on how many U.S. companies will be able to receive data from Europe, and on how this data can be subsequently transferred to other recipients and for other purposes. Some companies in the health-care industry (e.g., drug manufacturers, pharmacies, larger health-care providers, for example) may find the Privacy Shield to be a useful and viable option; others will be unable to participate or will find the compliance challenges too broad and complicated. In this event, there may be other options, and companies will need to consider these alternatives based on their own situation. In any event, the Privacy Shield will provide a new path to ensure data transfer from Europe for many companies, but also will create new compliance challenges and new avenues for complicated analysis of how best to ensure the appropriate use and disclosure of health-care information.

  PVLR ISSN 1538-3423