WELCOME TO LEGAL ISSUES AFFECTING SUPPLY CHAIN

This new series of articles, brought to you by the attorneys at Stinson Leonard Street LLP in partnership with the Medical Alley Association, provides thoughtful analysis of privacy obligations, licensing compliance, transparency and gift ban statutes, data rights and other legal issues that can have a significant impact on life sciences companies.

MEDICAL ALLEY ASSOCIATION

STINSON LEONARD STREET

Learn more about the authors at the end of each article. Look for more supply chain articles in coming weeks.

ARTICLE 01

HEALTHCARE PRIVACY

IN THIS ARTICLE:

MEDICAL ALLEY ASSOCIATION
STINSON LEONARD STREET

HEALTHCARE PRIVACY: IT'S MORE THAN JUST THE HIPAA THING TO DO

It seems that not a day passes without one of our life sciences companies wrestling with a question about privacy laws. Whether the concern behind the question is proactive (how can we use patient data for product development targeted marketing while respecting privacy rights?) or reactive (how can we minimize the increasing risk of liability for privacy breaches arising from our digital health or connected device offerings), we have noticed that companies that "silo" their various development teams with little or no interaction between them are more likely to experience significant problems with patient privacy requirements. Thus, whatever your reason for intersecting with patient data (e.g., clinical, marketing, customer service), a good strategy for both assuring compliance with privacy laws and ensuring that you may use valuable data as intended is to seek the input of members from various teams as you develop your programs and products. This broad and encompassing approach will help protect against gaps in knowledge and ensure alignment in objectives.

One of the challenges in developing privacy policies in the U.S. is that there is no national privacy law of general applicability. As a result, companies understandably tend to focus their privacy compliance attention on federal health-focused privacy regulation such as HIPAA and the HITECH Act. But discounting the myriad of other privacy laws can be a huge mistake, and neglecting the breadth of a company's privacy obligations can create conflicts and inconsistencies that increase the likelihood of an enforcement action or legal claim.

IN ADDITION TO HIPAA, PRIVACY OBLIGATIONS ALSO CAN ARISE FROM:

- Confidentiality and privacy obligations assumed in contracts
- The Federal Trade Commission (FTC)
- State truth-in-advertising laws
- State privacy laws relating to health records or genetic testing
- Foreign country laws

One Solution: Using the EU Paradigm as a Model for Privacy

U.S. companies that collect personal information in the European Union are grappling with the upcoming May 2018 implementation deadline for the General Data Protection Regulation (GDPR). Even for healthcare companies that do not touch EU data, however, following the GDPR "Privacy by Design" model can prevent some common mistakes that can result in costly consequences.

Privacy by Design means that privacy is a paramount consideration at the design stage of any program or device software that involves personal information: Each new service or business process that makes use of personal data must take the protection of such data into consideration and the company must be able to demonstrate that it took privacy into account during the whole life cycle of product development. This principle acts in tandem with the concept of "Privacy by Default," which means that the strictest privacy settings automatically apply once a customer acquires a new product or service (i.e., the customer need not opt in to privacy) and that personal information must by default only be kept for the amount of time necessary to provide the product or service.

This requirement can help ensure that life sciences companies focus on the full range of privacy compliance issues while also making sure that privacy compliance protocols track through internet-related services, medical devices, mobile apps and other technological innovations. In addition, even though recent focus has been on the GDRP, it should not be forgotten that the FTC released a privacy report in 2012 espousing Privacy by Design as an essential concept in its framework. While the FTC's Privacy by Design framework takes the form of a recommendation as apposed to the binding regulation of the European Union, following the Privacy by Design approach can be a helpful step to reduce the likelihood of enforcement actions in the U.S.

PRIVACY BY DESIGN

Privacy is a paramount consideration at the design stage of any program or device software that involves personal information.

A Cautionary Tale

Privacy by Design would have helped avoid a recent FTC enforcement action against Practice Fusion. Practice Fusion is a cloud-based electronic health record company that planned to provide a publicly available healthcare directory featuring patient reviews of their physicians. The FTC charged that Practice Fusion misled consumers by soliciting reviews for their doctors, without disclosing adequately that these reviews would be publicly posted on the internet, resulting in the public disclosure of patients' sensitive personal and medical information.

The company solicited the reviews of providers in emails to patients identified from the providers' electronic health records (EHRs), in which it asked patients to rate their providers in order to improve future service. The Practice Fusion site included the rating screen featured to the right.

The screen contained no statements as to how this data would be used other than "to help improve your service in the future." Using data to improve service is a common use disclosure in general privacy policies. However, the FTC found that "Practice Fusion's actions led consumers to share incredibly sensitive health information without realizing it would be made public," according to Jessica Rich, Director of the FTC's Bureau of Consumer Protection. "Companies that collect personal health information must be clear about how they will use it – especially before posting such information publicly on the internet."

CONTINUED ON PAGE 6

PRACTICE FUSION SAMPLE SCREEN

How was your visit?

Thank you for making an appointment with your provider, **Doctor Imadoc.** To help improve your service in the future, please let us know how your visit went.

How would you rate your provider overall?

Thank you,
Doctor Imadoc

powered by practice fusion

This email was sent to you by Practice Fusion®, a tool Doctor Imadoc uses to deliver the highest quality of care to patients. Please do not reply to this message. It will not reach the medical office.

Sent on behalf of Doctor Imadoc's office by: Practice Fusion, Inc. 420 Taylor Street San Francisco, CA, 94102, USA

CONTINUED FROM PAGE 5

The FTC complaint explained that patients likely thought that information they provided in the text box would only be shared with their healthcare provider. Because of this, many respondents included personal information such as their name, telephone number and health-related information. Consumers disclosed information about Xanax prescriptions, depressed children, yeast infections and other medical conditions while attaching this to their personally identifiable information. Misleading disclosures as to the use of personal information are a common target of the FTC. This was a case where Practice Fusion's privacy compliance team and website marketing teams were not in sync, or where Practice Fusion saw its only obligations as HIPAA-related.

Where Do You Start?

Healthcare companies should take proactive steps

As a practical matter, Privacy by Design, or a U.S.-based privacy program that espouses the Privacy by Design concept, would require early cross-functional coordination between a healthcare provider's privacy compliance team, legal team, product design team, information technology team and marketing team. While this sounds like a simple and obvious proposition, quite often these five groups do not operate in harmony. The end result is inconsistency in company policies and procedures. A company's HIPAA addendum might be well vetted and espouse HIPAA best practices but lack consistency with the company's website privacy policy, mobile app privacy policy and policies and procedures that govern personal data collected through medical devices. A disconnect between the privacy and security compliance teams and the website and marketing compliance teams can lead to costly fines, legal costs and negative public relations.

Further, life sciences companies should keep in mind that privacy compliance specialists typically undertake their review and analysis with a compliance-first mindset. Marketing teams and development teams with a first-to-market approach may not be so circumspect. Website teams often include analytics tools, remarketing tools, data collection technologies and third-party advertising services that conflict with promises made by the company. Careful coordination between these teams is needed to avoid representations about the scope of privacy afforded that may be true in one context, but false in others, as regulators often target companies that over-promise privacy.

One other key aspect of the GDRP that might be a useful touchstone for U.S. privacy compliance is the notion of Privacy by Default. Privacy by Default provides that data controllers implement organizational and technical measures to ensure that only personal data necessary for a specific purpose are processed by default. The concept of Privacy by Default also includes appropriately limiting storage and access.

WATCH OUT!

Inadequate privacy disclosures often occur when companies add new features to a mobile app, website or product.

Example:

The product engineering team designs a medical device with a GPS tracking feature. That feature isn't active in the initial release because the company is anxious to get the product to market. The feature is then activated in a future release without much thought as to privacy concerns, sparking backlash from consumers and regulators.

Under a Privacy by Design model, the code for the GPS feature would not even be written until the feature was analyzed for privacy issues with code specifications modified to include a disclosure and consent mechanism and a default setting that restricts GPS tracking.

Sounds Easy, Right?
Maybe not

Privacy by Default contrasts with the norm in the U.S. today. In the European Union, opt-in mechanisms rule the day, as they are generally required to meet the standards of Privacy by Design and Privacy by Default. Businesses in the U.S. have long taken the opposite approach, disclosing broad potential uses of consumer data coupled with an opt-out mechanism for those wishing to limit the use of their data. The opt-out approach often is intended to support the broad use of personal information by default, and companies may feel entitled to use the information in any way that is, at least technically, disclosed.

This stance presents difficult issues for a company's website and mobile app compliance team, as in the U.S. these broad potential uses are often buried in long and cumbersome online privacy policies that are not often thoroughly read by consumers. This practice can lead to a lack of sensitivity to the FTC's position that any intended use of personal information in a manner not normally expected by consumers must be conspicuously disclosed. A company may engage third-party service providers to provide mailing, fulfillment, data processing and other such services. The company may transfer information in connection with a bankruptcy, asset sale or other such transaction. These sorts of disclosures may be left to standard terms of a privacy policy or disclosure statement. However, a disclosure that is buried in a privacy policy may not be effective to disclose a particularly concerning use of information, such as marketing, the development of new intellectual property, sharing with an employer or the public at large. Though a detailed privacy policy is necessary and must include typical uses that consumers have come to expect, use of personal information in a more public facing context, such as in the Practice Fusion case, or in connection with third-party providers of other services, needs to be conspicuously disclosed, as regulators also target companies that make disclosures regarding the use of data, that lack the conspicuousness necessary for expansive use of consumer information.

IMPLEMENTING PRIVACY BY DEFAULT - AN EXAMPLE

One example of Privacy by Default would be for a company to include a specific check box in all of its mobile apps for patients to consent to collection and use of personal information in a particular context.

For instance, an app for a medical device company that collected heart rate information would require a check box (that is not pre-checked) allowing the user to conspicuously consent to collection of heart rate information for use in the company's medical device dashboard.

That approach has the added advantage of emphasizing collection and use of information during the design process to avoid situations where inaccuracies creep into a privacy policy through added features.

With a Privacy by Default approach, features could not be added without careful design of a specific consent mechanism.

KEEP EVERY PROMISE YOU MAKE AND MAKE ONLY PROMISES YOU CAN KEEP.

| **Anthony Hitt**

Finding the Balance

Although marketing and product development teams are often seen as the primary offenders in pushing the envelope on privacy concerns, there is also the possibility that companies, in an effort to achieve compliance, are not taking full advantage of the uses to which data can be put.

For example, the HIPAA treatment exception permits personal health information (PHI) to be disclosed for the purposes of providing care or treatment to a third party. Many website or mobile app privacy policies provide broad assurances of privacy and fail to include simple disclosure language around this and other HIPAA exceptions, creating the possibility that they have undermined the capacity of the company to use the data in a way that is permitted.

When it comes down to it, privacy compliance may seem complicated but it really boils down to a simple maxim: Keep every promise you make and make only promises you can keep.

This quote from American businessman Anthony Hitt sums up the vast majority of privacy compliance actions in the U.S. Growing concerns from consumers about the use of their personal information coupled with expansive global restrictions through the GDPR hint that "promises you can keep" is morphing into "promises you must keep." U.S. life sciences companies are well advised to take a Privacy by Design-oriented view to making sure that the bucket of promises they can keep aligns with the expectations of consumers and regulators.

AUTHOR CREDITS

Steve Cosentino, an attorney at Stinson Leonard Street LLP, combines deep intellectual property experience with a technology and corporate finance background to help companies pursue opportunities and growth. Steve's primary focus is on technology-related transactions and compliance, with an emphasis on software licensing, data center services, outsourcing, data privacy, advertising, cloud computing and cyber security.

Tricia Kaufman, an attorney at Stinson Leonard Street LLP, focuses her practice on the life sciences industry. She counsels medical device and pharmaceutical manufacturers and their vendors, drug compounding outsourcing facilities, healthcare providers, GPOs and others on issues relating to FDA regulations and healthcare compliance laws.

Sheva Sanders practices health law at Stinson Leonard Street LLP. She advises healthcare, managed care, medical device, pharmaceutical, life sciences and PBM clients on complex regulatory issues including fraud and abuse, compliance, reimbursement and transactional matters. She is a frequent teacher, speaker and writer on topics related to health law and health policy.

LEARN MORE

If your company is wrestling with privacy issues or if you want to understand Privacy by Design better, contact one of the authors on the left. Click their names to view their biographies.

HAVE A TOPIC IDEA?

Email your ideas for future articles to Stinson Leonard Street at **tricia.kaufman@stinson.com**


MEDICAL ALLEY
ASSOCIATION


STINSON
LEONARD
STREET