International In-house Counsel Journal
Vol. 5, No. 17, Autumn 2011, 1

Data Protection in the Pharmaceutical Industry: Concerns and Considerations

LESLIE GLADSTONE RESTAINO
General Counsel, Validus Pharmaceuticals LLC, USA
DAVID RESTAINO
Partner, Fox Rothschild LLP, USA
&
MICHAEL SHAW

Introduction

Data protection is an important aspect of the pharmaceutical industry throughout all stages of a product lifecycle – from innovation to exit. In the early stages of product development, manufacturers seek to secure trial data to provide a competitive edge; security issues arising during licensing and collaborative activities in the later stages of product development; after development and approval, patients seek to protect their privacy surrounding use of a drug. This latter issue has seen a large amount of recent press. In *Sorrell v. IMS Healthcare, Inc.*, the U.S. Supreme Court struck down a Vermont law involving the purchase of doctor prescribing records from data mining companies to reveal prescribing histories.[1] These prescribing histories were used by pharmaceutical companies to develop targeted marketing strategies. Vermont's Prescription Confidentiality Law of 2007 required doctors' consent for such practices.[2] Data mining companies and pharmaceutical manufacturers protested the law, and the Supreme Court in *Sorrell* ruled that the law in question was an unconstitutional violation of the First Amendment.

The Health Insurance Portability and Accountability Act ("HIPAA"), passed by Congress in 1996,[3] is another source of controversy in the data protection sphere. HIPAA requires confidential treatment of protected health information yet provides for disclosure of it in certain instances, such as when related to treatment, payment or healthcare operations.

Another issue is social media. Pharmaceutical manufacturers want to utilize social media tools to promote their products and provide information on health and diseases, but the industry is hesitant to proceed due to a lack of consistent guidance from the Food and Drug Administration ("FDA") regarding enforcement in the social media sphere, as well as the onus of monitoring and reporting adverse events.

Other data protection issues surround transactional due diligence, *i.e.*, the practice of gathering information regarding a transaction with a company. Buyers and licensees need to have requisite information to make an informed decision regarding the deal (*e.g.*, licensing a pharmaceutical product) but, at the same time, the selling or licensing company has an interest in protecting its valuable information in case the deal falls

[1] *Sorrell v. IMS Healthcare, Inc.* ("*Sorrell*"), ___ *U.S.* ___, 131 *S.Ct.* 2653, 180 *L.Ed.*2d 544 (2011).
[2] 18 *V.S.A.* § 4631.
[3] Pub. L. No. 104-191, 110 *Stat.* 1936 (1996).

through – and avoid having provided a third party with unfettered access to protected information. Similarly, companies have varied policies regarding corporate records retention, that is, the duration that corporate records must be preserved. Record preservation is required in order to comply with regulatory obligations, but preservation beyond the required period, while valuable, must be weighed against the large costs of preserving vast quantities of information and the potential liability of maintaining confidential information.

Finally, litigants can demand to see protected information if pertinent to a legal dispute. Companies do not want their protected information leaked out, and try to protect against disclosure by using confidentiality agreements to ensure the protection of the data that must be disclosed in litigation.

The Supreme Court's Current Stance on Pharmaceutical Data Mining

In the United States, it has become common practice for data mining companies to collect doctors' prescribing records. As noted in *Sorrell*, when doctors prescribe drugs to patients, pharmacies receive "prescriber-identifying information" during the processing of those prescriptions. Pharmacies then sell the records to data mining companies. After receiving the doctor prescribing records, data mining companies create reports on these doctors and their prescribing habits. The reports are subsequently sold to pharmaceutical manufacturers, who buy the reports to help target their marketing strategies.[4] For example, if a pharmaceutical manufacturer is developing a new drug, then it wants to market to doctors who already prescribe similar drugs. Therefore, the incentive of knowing which doctors prescribe which drugs can be crucial to a manufacturer's promotional activities.

The controversy came to light in *Sorrell* – because data mining companies purchase the "prescriber-identifying information" from pharmacies *without* doctor or patient consent.[5] In 2007, Vermont passed the Prescription Confidentiality Law. It prohibits the use of prescribing records for commercial gain,[6] ostensibly to decrease the cost of health care.[7] Several pharmaceutical manufacturing companies and one of the largest global data mining companies sued Vermont's attorney general, William Sorrell, to repeal the statute. After losing in district court, the plaintiffs appealed the case, and won in the Second Circuit; the court of appeals held that Vermont's Prescription Confidentiality Law violated the First Amendment by burdening pharmaceutical marketers' speech without adequate justification.[8]

When the *Sorrell* case reached the Supreme Court, the court ruled that the Prescription Confidentiality Law violated the First Amendment. Justice Kennedy, writing for a 6-3 majority, stated that:

The statute . . . disfavors marketing, that is, speech with a particular content. More than that, the statute disfavors specific speakers, namely pharmaceutical manufacturers .... The law on its face burdens disfavored speech by disfavored speakers.[9]

This ruling has large implications for the future of pharmaceutical marketing and the use of data in such practices. For many years, pharmaceutical manufacturers have been arguing against any regulation of their truthful speech. This case demonstrates that, under

[4] These practices were summarized in *Sorrell*, 131 *S.Ct.* at 2659-60.
[5] *Sorrell*, 131 *S.Ct.* at 2660.
[6] 18 *V.S.A.* § 4631.
[7] *Sorrell*, 131 *S.Ct.* at 2661, 2670.
[8] *Id.*, 131 *S.Ct.* at 2662.
[9] *Id.*, 131 *S.Ct.* at 2663.

constitutional scrutiny, these companies *do* have the right to market their products using doctors' prescribing records.

Not only are the results of this case being felt in the realm of prescribing records, but also in the area of off-label marketing. The case of *United States vs. Caronia*, currently awaiting decision in the Second Circuit, involves a pharmaceutical sales representative who attempted to promote a drug for off-label usage and was charged with two misdemeanors under the misbranding provisions of the Food, Drug and Cosmetics Act.[10] A critical issue to be decided is whether the First Amendment protects the right of individuals to speak truthfully about off-label uses of FDA-approved products; the court below found no such protection.[11] The *Caronia* appeal is particularly important given the number of federal and state laws and regulations banning off-label promotion, and it will be interesting to see how the court interprets the *Sorrell* ruling in light of those legal prohibitions.

The Health Insurance Portability and Accountability Act ("HIPAA")

HIPAA, passed by Congress in 1996, seeks to protect personal health information ("PHI"). It imposes obligations on all persons who deal with PHI to protect the privacy and security of that information. HIPAA contains two main sections: the Privacy Rule and the Security Rule.

HIPAA was amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH") as part of the American Recovery and Reinvestment Act of 2009.[12] In addition to creating economic incentives for adoption of electronic health record technologies, HITECH contains a number of provisions which strengthen HIPAA's Privacy and Security Rules.[13]

The Privacy Rule seeks to protect the distribution of health information of patients by "covered entities," such as healthcare providers who transmit data electronically, and also give individuals some rights concerning the distribution of their private information.[14] The Privacy Rule specifically protects against the distribution of "individually identifiable health information," which is information that includes an individual's mental or physical health condition or the granting of healthcare to that individual – including any payment for such healthcare.[15] HIPAA's Privacy Rule also contains several "standards" that outline the rules and implementations of this section of the law.

Standard A of the Privacy Rule deals with the primary function of that rule – protecting patient information. It states that covered entities may not share PHI with any other individual or group, unless expressly permitted to do so.[16] Covered entities may share PHI: (a) with the individual in question, (b) for reasons relating to treatment or payment,

---

[10] *United States vs. Caronia* ("*Caronia*"), 576 *F.Supp.*2d 385, 388 (E.D.N.Y. 2008), appeal docketed No. 09-5006 (2d Cir.). Oral argument was conducted in 2010; subsequently, supplemental briefs were filed.

[11] *Id.*, 576 *F.Supp.*2d at 402.

[12] The American Recovery and Reinvestment Act of 2009 was adopted as Pub. L. No. 111-5, 123 *Stat.* 115 (2009).

[13] HITECH contains breach notification requirements for unauthorized uses and disclosures of unsecured PHI's, individual access to electronic PHI, and "bootstraps" the requirements of HIPAA to business associates (*e.g.*, any partner of a health care provider, health plan or health plan clearinghouse that may provide legal, actuarial, accounting, consulting, data aggregation, management, administration or financial services wherein the services require the disclosure of individually identifiable health information). *See* 45 *C.F.R.* § 164.300 *et seq.* and 45 *C.F.R.* § 164.500 *et seq.*, as adjusted by Section 13400 *et seq.* of HITECH.

[14] "Covered entities" refers to health plans, health care clearinghouses, or a health care provider who transmits any health information in electronic format. 45 *C.F.R.* § 160.103. The Privacy Rule is codified at 45 *C.F.R.* §§ 164.500 to 164.534.

[15] 45 *C.F.R.* § 164.502.

[16] *Ibid.*

or (c) other permissible disclosures, for example, mandatory disclosures when the Department of Health and Humans Services requests information.[17] The other standards of the Privacy Rule outline the further intricacies of the proper usage of PHI. Some notable standards include: covered entities must only release the minimum amount of PHI necessary to meet the need of the current situation, and once PHI has been de-identified (*i.e.*, the information cannot be linked to a particular person) that information can be disclosed for special purposes such as clinical studies and public health research.[18] Additionally, if an individual is incapacitated or in a similar emergency state, covered entities can use professional discretion to determine the proper disclosure of PHI.[19]

The Security Rule deals mainly with protecting electronic Personal Health Information ("ePHI").[20] Essentially, covered entities must keep ePHI confidential and protect it from potential breaches of security. The rules take into account the difficulty of creating sweeping regulations for all types of entities, so they provide a section stating that flexibility is allowed depending on the covered entity's size, its technical capabilities, the costs of data protection, and the potential of risk to protected information.[21] This flexibility means that covered entities can choose how they protect their data, so long as it is secure enough to meet HIPAA's guidelines. However, although there is some flexibility, some regulations *must* be met by all covered entities. For example, covered entities must: assign one individual to be responsible for security measures; ensure that only employees who need access to PHI have it; train all employees and managers in effective security; and much more.[22]

One reason HIPAA was passed into law was the goal of protecting individuals' PHI. However, many critics claimed that the Department of Health and Human Services is not taking a tough enough stance on data protection under HIPAA. Thus, HITECH contains language implying that weak enforcement is a thing of the past. That is to say, mandatory penalties are now imposed for "willful neglect."[23] The degree to which enforcement occurs remains to be seen, but it appears that Congress expects there to be a stronger position taken on enforcement.

Another controversy surrounding HIPAA is its policy allowing individuals to obtain a list of who has accessed their PHI from their covered entity.[24] These lists include, among many items, who accessed the information and for what purpose.[25] However, a loophole in the law allowed covered entities and other healthcare providers to not report the disclosure of PHI as it pertains to healthcare operations.[26] HITECH sought to overcome, and now limits, this loophole.

Under HITECH, a communication is not considered a health care operation if the covered entity receives payment for making the communication.[27] However, there are some exceptions. A communication is no longer considered a healthcare operation that requires an individual's authorization unless the communication: (1) describes only a drug or

---

[17] *Ibid.*
[18] *Ibid.*
[19] 45 *C.F.R.* § 164.510.
[20] The Security Rule is codified at 45 *C.F.R.* §§ 164.302 to 164.318.
[21] 45 *C.F.R.* § 164.306.
[22] *See* 45 *C.F.R.* § 164.308.
[23] *See* 42 *U.S.C.* § 1320d-5 (Section 1176 of the Social Security Act), as amended by Section 13410 of HITECH.
[24] 45 *C.F.R.* § 164.528.
[25] *Ibid.*
[26] *Ibid.*
[27] *See* 42 *U.S.C.* § 1320d-5 (Section 1176 of the Social Security Act), as amended by Section 13406(a)(2) of HITECH.

biologic currently being prescribed for the individual and the payment for the information is deemed reasonable amount; or (2) is made by a covered entity or business associate who has received a valid HIPAA authorization from the individual to whom it is making the communication.[28] It remains to be seen if the exception will swallow the rule, but ostensibly certain pharmaceutical marketing practices, such as the use by pharmaceutical manufacturers of patient information sold by pharmacies, in order to send letters encouraging prescription switches, are acceptable.

Many believe that HIPAA harms patients because it denies them the ability to fully know who has accessed their private information. For this reason, the Department of Health and Human Services recently proposed new HIPAA privacy rules that will mandate the complete disclosure of who has accessed one's PHI, in addition to other details about the disclosure.[29] Presuming adoption of these new rules, they would go into effect starting January 1, 2013 for electronic record systems acquired after January 1, 2009, and on January 1, 2014 for electronic record systems acquired on or before January 1, 2009.[30]

The Pharmaceutical Industry's Struggle with Social Media

The term social media encompasses a large area of online activities. Whether it refers to networking on Facebook, posts on Twitter, or simply an informational website, pharmaceutical manufacturers want to use social media in order to promote their products and provide awareness about health and diseases. However, due to the relatively recent emergence of online social media, current FDA regulations fail to fully encompass online activities, making pharmaceutical manufacturers hesitant to proceed. Furthermore, there is a concern that the FDA has not adopted a uniform and consistent approach to online activities, thus failing to provide a predictable environment conducive to marketing online. Since pharmaceutical manufacturers are unable to predict the legal boundaries of social media usage, many are hesitant to proceed.

However, despite hesitation from some companies, others are moving forward with use of social media. Some manufacturers take the position that so long as they stay within the FDA's guidelines which apply to Direct-To-Consumer ("DTC") advertising, to the extent such FDA policy can be discerned as more fully discussed below, they will be legally compliant in their social media usage. For example, one manufacturer has created an active social presence that utilizes a blog focused on stories of employees, wellness information, and corporate content.[31] Such blogs can contain robust content and be supplemented with YouTube and Facebook pages, and also connect with community members via a communications staffer who "tweets" on behalf of the brand in a more personal voice.[32]

Another manufacturer has worked on development of its own social networking website to connect patients and clinical trial researchers while also making use of a Twitter account, and its website will allow users to post confidential health information made available to researchers studying those users' conditions.[33] However, this represents an issue critical to data protection; that is, if confidential health information is posted online, patients expect that information to remain confidential. Pharmaceutical manufacturers must ensure the confidentiality of that data by protecting their online social networking site from potential breaches of security.

---

[28] 45 *C.F.R.* § 164.501, as adjusted by Section 13406(a)(2) of HITECH.
[29] 76 *Fed. Reg.* 31426 (May 31, 2011).
[30] 76 *Fed. Reg.* at 31429, 31442.
[31] http://jnjbtw.com
[32] *See* http://www.toprankblog.com/2011/01/social-media-marketing-pharma
[33] http://inventorspot.com/articles/top_ten_drug_companies_social_media_31760

Other manufacturers avoid any online presence. An issue that has been presented as being of great concern is whether posting by patients also creates an affirmative regulatory obligation on the part of the manufacturer. For example, if community members are allowed to post comments on their experiences with a given drug, the concern is that the manufacturer may have a duty to report any negative comments to the FDA as adverse events, *i.e.*, file a report under the FDA's regulatory scheme.

In 2009, the FDA indicated that it would issue new guidelines covering the use of social media tools.[34] The new guidelines are expected to cover fulfilling regulatory requirements, fulfilling post-marketing submission requirements, on-line communications for which manufacturers are accountable, use of links on the Internet and correcting misinformation.[35] However, well over a year has passed since an FDA comment period expired and the agency has still not issued the long-awaited guidelines.

Protecting Data During Due Diligence

When two companies make any sort of business deal it is standard practice for companies to research the inner workings of each other to ensure financial stability, among other factors. This process is called due diligence. Essentially, such a party – normally the purchaser or licensee but often both parties – seeks to discover any adverse information that could impact a corporation's or a product's value.

It is universally accepted that due diligence constitutes a vital part of any transaction; companies must know the status of their potential business partners prior to bonding over business. However, in the pharmaceutical industry there exists a fine line between sharing the requisite amount of data for an educated transaction and sharing so much that other companies gain access to trade secrets. Every business has information that helps it compete in the free market; for pharmaceutical manufacturers, that information could include data collected from clinical trials, the results of new drugs just released to market, sales data, and more. Therefore, in order to protect this valuable information, drug companies must find a way to provide enough data to their potential business partners to prove the stability of their reputations, while not providing so much that other businesses have access to protected data should the deal fall through.

In order to walk this fine line of data protection versus due diligence, many pharmaceutical manufacturers sign confidentiality agreements during due diligence. These agreements can be written to protect one side's data, but can also be mutually protective. Essentially, they prohibit either company from revealing any information about the other company that they might uncover during due diligence. Confidentiality agreements not only protect important information which could hurt a company's competitive edge if leaked, but also speed up the time it takes for a deal to go through. Instead of worrying about protecting data and only giving small amounts of information at a time to protect trade secrets, companies can disclose all necessary information to the other company in the transaction right away without legitimate fear of that information being leaked.

Dealing with the Challenges of Retaining Corporate Records

All businesses have – or should have – some sort of corporate record retention policy, which dictates how long certain documents are kept and in what format they are stored. Some obstacles in creating these policies involve: (1) where to keep the vast amounts of information that corporations create, and (2) the potential liability of maintaining confidential information. However, in the past decade the pharmaceutical industry has

[34] 74 *Fed. Reg.* 48083 (September 21, 2009).
[35] 74 *Fed. Reg.* at 48086 to 48087.

pursued a method of data storage that could help allay some challenges of traditional data storage: electronic storage. In 1997, the FDA published the regulations regarding electronic record storage.[36] The rules have been subject to varying interpretations and FDA guidance documents;[37] notwithstanding, most drug companies now utilize electronic data collection and storage.

Moreover, the FDA mandates that a pharmaceutical company must retain certain records such as manufacturing and quality records, for a certain period of time.[38] Likewise, all documentation supporting the filing of a new drug application must be retained for at least two years.[39] The Securities and Exchange Commission also calls for covered organizations to store business documents for stipulated periods,[40] and HIPAA has a number of guidelines for document retention and security.[41]

By digitally archiving corporate records, pharmaceutical companies gain several advantages. First, the information is easily accessible. Accessing a document requires only a few keystrokes on a computer as opposed to traveling to a warehouse filled with thousands of documents. This greatly enhances productivity. The second advantage, relevant to data protection, involves the selectivity of who has access to the information. As opposed to being in a physical state, such as on paper, digital archives put information in a digital state. This means that in order to access this information one has to be authorized to view it. The difference between being authorized to view a physical document versus a digital document is that electronic archives minimize human intervention in the process of releasing the data to internal or external agents. However, electronically storing information does inevitably lead to another issue with data protection; drug companies must ensure that any data is protected from external access.

Finally, it is much easier to dispose of documents when they are in an electronic state than when on paper. As computer systems are subjected to numerous back-up procedures and periodically upgraded, each such step provides another opportunity for electronic data to be destroyed. Retention policies need to account for these continuous processes or risk destroying data that is required in the future – especially as courts have become aware of the need to preserve electronic mail and insist on sanctioning those parties which destroy electronic data contrary to their own retention policies.

Other Litigation Issues

In litigation, each party is entitled to get "discovery" from the opposing side. For example, plaintiffs alleging personal injuries in the products liability context will want discovery about testing of that drug, and what research found, if anything, to cause an adverse reaction. However, the defendant will be concerned about releasing confidential information about processes in making the drug, or releasing privacy information concerning the people given the drug during testing (such as name and medical condition of participants in a drug study).

Because each party is entitled to discovery, the parties cannot hide behind the need for confidentiality as an excuse to prevent the release of certain information. But something is required. So, the concept of a "confidentiality agreement" was born. Basically, it is an agreement executed by both sides and governing the exchange of confidential

---

[36] 62 *Fed. Reg.* 13430 (March 20, 1997). The rules are codified at 21 *C.F.R.* Part 11.
[37] *See* Guidance for Industry Part II, Electronic Records; Electronic Signatures and Application dated August 2003.
[38] 21 *C.F.R.*§ 211.180.
[39] 21 *C.F.R.* § 312.57.
[40] *See*, *e.g.*, 17 *C.F.R.* § 240.17a-4.
[41] *See*, *e.g.*, 42 *C.F.R.* Part 1003; 42 *C.F.R.*§ 482.24(b). *See also* 45 *C.F.R.*§ 164.530.

information. Typically, litigation counsel execute an agreement to keep confidential information in the strictest of confidence. If an expert witness needs to see the information, like a doctor giving an opinion about causation, then the expert witness also needs to sign on to the confidentiality agreement.

However, confidentiality agreements do not themselves have the approval of the court, so issues can arise in the event of a breach. For this reason, the better approach is to create an agreement and then have it reviewed, approved and signed by a judge. This is called a "confidentiality order." Breach of such an order allows the harmed party to seek immediate relief from the court and, hopefully, immediately end the flow of the confidential information at issue.

Finally, the interplay between confidentiality and FDA requirements is an important one. In a recent dispute between a pharmaceutical manufacturer and a generic producer seeking to enter the market, the manufacturer sought relief from a confidentiality order in order to send the generic producer's expert reports to the FDA and, presumably, argue that the FDA should use these reports to delay approval of the competing generic product.[42] The court refused to modify the confidentiality order for a number of reasons, including its belief that the generic producer would be harmed if its confidential formulations and research techniques were revealed beyond the litigation.[43]

* * *

Leslie Gladstone Restaino, Esq. has a broad range of experience with the legal and regulatory issues involved in the pharmaceutical/biotechnology, and medical device industries and their complex product, device and services offerings. Leslie has particular expertise in the areas of business/corporate law, pharmaceutical, medical device, and healthcare law, FDA regulatory matters, complex licensing and strategic alliances, commercial contracts, pharmaceutical operations and commercialization, and patents and intellectual property. She is currently the General Counsel of Validus Pharmaceuticals LLC, a specialty pharmaceutical company focusing in the psychiatry and neurology markets.

Validus Pharmaceuticals LLC is focused on acquiring, reformulating and marketing prescription products relevant to the psychiatry and neurology markets. Validus seeks to acquire mature products that have well defined and accepted clinical utility relevant to today's practice of medicine.

David Restaino, Esq. is a Partner in the Princeton, New Jersey office of Fox Rothschild LLP, where he provides compliance counsel in many subject matter areas, including the compliance aspects of health law. In addition, David's practice encompasses complex litigation in federal and state jurisdictions. As a former Deputy Attorney General, David also brings a working knowledge of government enforcement proceedings. He may be contacted by e-mail at drestaino@foxrothschild.com or by telephone at 609/895-6701.

Michael Shaw is currently a senior at Ridge High School in New Jersey. As a member of his high school's debate team, he spends a lot of time researching various current issues. He is in the process of applying to colleges in order to continue his education next year.

[42] *Medeva Pharma Suisse A.G. v. Roxane Laboratories*, Civil Action No. 07-5165 (FLW) (D.N.J., Letter Opinion and Order dated August 25, 2011).
[43] *Ibid.*

Fox Rothschild is a national, general practice law firm with more than 500 attorneys in 16 offices coast to coast. Approximately 150 attorneys practice in three New Jersey offices located in Princeton, Roseland and Atlantic City, making the firm one of the state's largest. The firm has significant depth in the traditional practice areas most relevant to pharmaceutical clients.