Social Media, Cloud Computing and Mobility in the Life Sciences

By Andrew J. Hollander

Information, like a five-year-old child cooped up at the end of a long rainy day, just resists being contained. And electronically sent information can race around the world in seconds, be seen by millions, and remain stored for future viewing, perhaps for all to see, forever.

For the information-intensive life sciences, the impact is mixed. On one hand, loosening the information spigot can cut drug discovery time by harnessing computer clusters, assist clinical trials, shave time to market, and reach countless consumers instantly, personally, and interactively. On the other hand, the greater flow increases the risk of running afoul of U.S. federal and state law and regulations, not to mention creating security and privacy debacles.

Viewed through a legal lens, then, information management and control is more critical than ever. This article looks at several areas of great promise -- and peril -- for the life sciences in the information age: social media, cloud computing, and mobility.

Social Media

What's social media? Wikipedia (itself a social media construct!) defines it as "the use of web-based and mobile technologies to turn communication into interactive dialogue." Interactive at its core, social media results in a mountain of "user-generated content". Major social media platforms have entered the daily routine of millions, and include Facebook, Twitter, and YouTube.

The relationship of the life sciences, a highly regulated field, with social media, where sometimes anything goes, is complicated. The U.S. Food and Drug Administration (FDA) has nine Twitter accounts, providing helpful up-to-the-minute information, such as on drug recalls. However, the FDA has yet to issue guidelines for industry on social media and the Internet.

In November 2009, the FDA held public hearings on use of social media for pharmaceutical and medical device marketing. But, despite calling issuance of a social media policy a high priority, the FDA has not yet published one.

This presents a legal quandary. Consider a Facebook group for a prescription pharmaceutical. Anyone who has seen a "chat room" knows it can turn into a free-for-all. Does a user gripe warrant "adverse event" reporting? Are there "fair balance" concerns? Are there off-label usage problems? Are there other regulatory concerns? Is there a HIPAA (Health Insurance Portability and Accountability Act) problem? Could user-generated content provide fodder for class action lawsuits?

Nor are these concerns merely abstract. In July 2010, a major pharmaceutical company received a warning letter from the FDA's DDMAC (Division of Drug Marketing, Advertising, and Communications) about its website for a new cancer drug. The website had a "Facebook Share" widget (a tiny Facebook logo) that let users share, with two clicks, any page of the company's cancer-drug website via Facebook.

The FDA warned that the shared content misbranded the drug in violation of the Federal Food, Drug, and Cosmetic Act and FDA implementing regulations. (21 U.S.C. § 352(a) and (n), 321(n); 21 C.F.R. § 202.1(e)(3)(i), (ii) and (e)(6)(i).) And among other problems, these materials were not submitted to the FDA 30 days prior to dissemination. The FDA also concluded that the website failed to communicate adequate risk information associated with the drug.

Beyond regulatory concerns, there are human resource issues. It's one thing for an employee to share priceless vacation photos on Facebook. It's another if the employee, intentionally or not, discloses confidential company information. Trade secrets, for example, are destroyed once their subject becomes public.

Using social media for public relations activities carries added risks. What if a company's Facebook page is hacked or defaced, as was the case with a major pharmaceutical company in July 2011? Or what if a blogger "endorses" a life sciences company's product but does not properly disclose free "gifts" or compensation from the company? The company could be liable under 2009 rules from the Federal Trade Commission. 16 C.F.R. § 255.

For these reasons, pharmaceutical, health device and biotechnology companies are using caution about social media. Practical steps companies can take to manage risk include:

- Establish a written social media policy that spells out guidelines and procedures for using social media in marketing, for employee use of social media, and how to deal with third parties such as bloggers and advertising agencies.
- Monitor social media websites for activity relating to the company and take prompt measures, if needed.
- Stay tuned for the FDA's social media policy.

Cloud Computing

If you use Google for email ("gmail") you do cloud computing. In other words, you use your Internet browser to connect with remote computing resources managed by a third party out there in "the cloud." The servers, storage and IT personnel could be next door, in Oregon, or abroad, or all of these places and more.

Cloud computing has many benefits. Computing power is virtually unlimited. The cloud provider just adds servers if you need more power. It can be cheaper -- you don't own the servers, hire the IT personnel, or pay for data storage -- you just use your browser as the "joystick" to control them all. It allows massive collaborative efforts. It lets end users be more mobile. Quick, scalable, and flexible, it can reduce the barrier to entry for a new project and speed time to market. Some of the biggest cloud providers are household names: Google, Amazon, IBM, Microsoft, Oracle.

Cloud computing has its challenges, however. Security and privacy are always questions. You don't own the servers or employ the administrators. You may have limited knowledge of exactly what safeguards are in place regarding your sensitive data. Also, you lose control over the software and hardware and must depend on the provider.

With the above risk/reward profile, cloud computing has made gradual inroads into the life sciences. Pfizer uses a "virtual private cloud" for R&D that requires enormous computing power. Pfizer established rules for a private micro-Internet of its own design walled off from the public Internet, and Amazon provides the cloud platform. Pfizer says that this cuts computing time from weeks to hours for discovering molecule properties. Another cloud user is Varian. The medical equipment maker needed to run Monte Carlo calculations to help develop new products. Varian used Amazon's EC2 (Amazon Elastic Compute Cloud) -- which harnessed numerous servers -- and cut calculations from a projected six weeks to one day.

Cloud computing can facilitate research and clinical trials. Researchers from The National Cancer Institute's Cancer Therapy Evaluation Program and Bristol-Myers Squibb use cloud computing -- joined with digital signatures and digital identity credentials -- to reduce the need for paper forms and signatures. Sanofi-aventis researchers joined these efforts. It's driven by the digital authentication protocol set by a non-profit group, Safe-BioPharma Association, developed by a group of life sciences companies with participation from the FDA and the European Medicines Agency to verify and manage digital identities for the life sciences.

The cloud can strengthen customer relationships and revenues. Oracle and IBM tout it for closed-loop marketing, in which huge amounts of data can flow from customer interactions, undergo analytics, and with constant feedback, help refine marketing, sales, and the ultimate value proposition for the client.

Despite its benefits, cloud computing can present thorny legal issues for life science clients. One is HIPAA. HIPAA (see the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201 et seq. and 29 U.S.C. § 1181 et seq.) is always a consideration for life sciences data. The U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to implement HIPAA. The Privacy Rule mandates that "covered entities" safeguard "protected health information" (PHI). (45 C.F.R. § 160.103, § 164.501.) And there is the Security Rule, which requires that only permitted entities be given access to electronic PHI (ePHI), and there be adequate safeguards -- administrative, physical and technical ones -- to protect the ePHI. (E.g., 45 C.F.R. § 160 et seq.).

In 2009, HIPAA was supplemented by HITECH (the Health Information Technology for Economic and Clinical Health Act, see 42 U.S.C. § 17931 et seq.). HITECH expands security provisions to "business associates" of the covered entity, which could include service providers, subcontractors or downstream entities that come into contact with ePHI -- including, conceivably, cloud computing providers.

While it is not certain if a given cloud computing provider would be considered a "business associate," it may be prudent to consider the possibility. It may be desirable to propose a "business associate agreement" with the provider such that it expressly agrees to adhere to HIPAA and HITECH. Microsoft proclaims that it's one of the first in the industry to offer a "business associate agreement" to customers, through its Office 365 Cloud Service.

Of course, beyond typical negotiating points relevant to software contracts, the underlying cloud computing Service Agreement may have cloud-unique issues. For example, HIPAA has logging and auditing requirements, which might apply even to cloud administrators and may be raised in negotiations.

Also, there are several types of cloud services, and one of them may "subcontract" to another – one more point to consider in the negotiation process. For example, Netflix is layered on Amazon EC2. Netflix provides the software piece of the cloud but Amazon provides storage, servers, and connectivity. You may know the first level provider (Netflix), but not the second (Amazon). So before signing on the dotted line, you may wish to ask whether your cloud service provider (whom you know) is "subcontracting" to a hosting service (which you may not), and find out whom.

Noncompliance with HIPAA/HITECH could "earn" one a mention on the HHS "wall of shame," which publicly discloses security violations affecting more than 500 people. Because cloud computing is relatively young, violations unique to cloud computing are not prominent. But chances are that the shadow of a cloud violation may fall on the wall before long.

Mobility

Mobility is one benefit to cloud computing. You just need a browser, which could be in a "thin" laptop with minimal hardware or software. Naturally, mobility creates added complications, such as security. Google offers two-factor verification for paid applications, where to obtain cloud access you must enter your mobile phone number and a one-time code.

Steps that life sciences companies can take to manage risks of cloud computing and mobility include:

- Undertake good due diligence into a cloud computing provider. If you're not getting sensible answers consult another provider who will address your unique concerns.
- Negotiate a cloud computing service agreement that, besides the usual software agreement negotiating points, takes into account regulatory and compliance requirements, and consider "business associate agreements."
- Set forth a policy that employee access to cloud computing resources be properly managed, and comply with not only company guidelines but regulatory requirements.

Andrew J. Hollander, Of Council, can be reached at andrew.hollander@klgates.com.