Health IT Market Trends

*The Editor interviews **Christine Savage** and **Julia Hesse** of Choate, Hall & Stewart LLP in Boston about Healthcare IT market trends, developing and selling big data, and data security issues. Christine Savage and Julia Hesse are partners in Choate's Healthcare IT practice, and Savage chairs the firm's Healthcare Group.*

Christine Savage

Julia Hesse

Editor: Tell us a little bit about Choate's Healthcare IT practice.

Savage: Choate's Healthcare IT practice is interdisciplinary and draws on our firm's collective experience in managing healthcare regulatory, licensing, financing, and M&A transactions for clients in this space. In the past two years, Choate completed 20 deals worth more than $530 million in Healthcare IT, including deals for emerging companies as well as private equity funds and their financed portfolio companies.

Editor: What advice would you give "traditional" players in the healthcare space (like providers or health plans) that want to develop Healthcare IT product lines?

Hesse: Many traditional healthcare companies are developing their own Healthcare IT products to leverage existing data, often to improve patient outcomes or health plan design, or to foster new medical research. Whatever the goal, engaging regulatory counsel early in the life cycle of any new venture is important to help issue-spot potential regulatory hurdles. For example, what barriers may prevent the company's ability to use or disclose certain data it holds? Will the company be required to implement HIPAA business associate agreements in light of the new business or administrative services to be provided? What types of fees can the company charge for accessing data? How will the company engage with customers (especially those with referral relationships) in a way that conforms with fraud and abuse laws (e.g., Stark and Anti-Kickback)?

Regular check-ins with legal counsel as the project hits important milestones will help avoid last minute surprises, which can cause costly delays or require product restructuring. Being realistic about the unique value of your data or Healthcare IT service is also critical to ensure that significant resources are not spent developing a product for which there is little or no market.

Editor: What are some opportunities and challenges of harnessing an entrepreneurial workforce in Healthcare IT?

Hesse: "Traditional" healthcare players, especially academic medical centers, have experience with their workforce developing intellectual property (IP) through research activities, but they are often less prepared to address potential conflict of interest or commitment issues when workforce members develop Healthcare IT applications. Many institutions – particularly providers that are not academic medical centers – do not have standing IP policies or employment agreements in place with the bulk of their workforce, which poses a challenge to the organization's ability to harness and control resulting IP.

If your institution does not have an IP policy, you should consider developing one. If your institution *does* have an IP policy, you should consider revisiting it to ensure that it is broad enough to cover all the workforce members that may be potentially relevant to Healthcare IT. Many administrative or operational staff (e.g., those in Finance or IT) do not perceive themselves to be subject to rules related to IP and inventions (even when they exist) and therefore may need to be re-trained in order to understand that those policies apply to them.

Other challenges arise when workforce members use "live" data from their employer in order to test applications. Such use of patient or client data may be unauthorized if the venture is not being done under the auspices of the institution and could expose the institution to various regulatory actions.

However, the benefits of having an entrepreneurial workforce can outweigh the challenges. First, the increased impetus to develop more user-friendly healthcare applications and process improvements may broaden the IP generators at your organization. With more individuals committed to the cause of improving Healthcare IT, there is an increased likelihood that organizations will find ways to license and commercialize their technologies and generate new revenue streams. Those revenues can then be used to expand patient care initiatives or foster additional IT development efforts, and in some cases, be used to reward and retain those in-house entrepreneurs that helped develop the application or other IP.

Editor: What is the allure of big data?

Savage: For healthcare providers, it can be a way to monetize existing data. For example, a hospital may wish to identify patient outcome trends and determine whether or not particular treatments, therapies or interventions have affected their ability to provide quality care at a good value. For non-provider entities such as pharmaceutical and medical device companies, big data can be used to identify trends among patients using their products, to track different products' effect on long-term health, and to assess trends that may drive future research and development projects.

Editor: What are the risks to developing and selling big data?

Hesse: There are a number of significant risks. First, you need to ensure that the party that wants to develop and sell the data actually has the power to do so. In certain circumstances, additional patient or participant consent is necessary to use or further disclose data, particularly when the data includes individually identifiable sensitive information. There are also concerns about the need – and yet possible inability – to de-identify fully the information to be aggregated and parsed out to purchasers. Once information has been disseminated, you must have operational systems in place to monitor business partners and enforce restrictions on using the data for specific purposes that do not go beyond the agreed-upon scope of the contract.

There are also numerous regulatory restrictions on the sale of Protected Health Information without consent. Even where this is permitted, there are potentially significant limitations on the amount that can be charged, which may destroy the financial viability of a particular application or initiative.

Editor: What should a company do if it thinks it has had a data breach?

Savage: The laundry list of things to do if a suspected data breach occurs is too long to cover in a few paragraphs. The following triage items must be taken care of immediately. Review your data breach policy and ensure that you are following it. Categorize the nature of the incident: was it accidental, malicious, an internal errant disclosure or a disclosure to third parties? Is the disclosure or breach ongoing, was it an isolated incident that has already occurred, or can you stop it from recurring immediately? Designate an incident manager and immediately assemble an internal triage team (e.g., personnel from HR, IT, compliance, public relations, and legal).

Depending on the circumstances, you may need to retain a forensics vendor to ensure that your systems can be backed up or taken off-line in a way to allow investigation without leaving data vulnerable for any longer than necessary. If there are vendors involved, gather your contracts and put the vendor on notice about your expectations for securing or blocking further access to the information deemed to be at risk, and the preservation of all system logs or reports for your investigation.

It is crucial in the first few days to gather as many facts as possible and to consider whether it is possible that no breach has occurred (by conducting a risk assessment) or whether it is clear that there has been a breach. You will want to consider the scope of the unauthorized use or disclosure; the sensitivity of the data involved; whether the data compromised could lead to identity, credit or medical services theft; to whom the data was disclosed; and the extent to which meaningful mitigation efforts have reduced the risk that the privacy or security of the data was compromised.

Also, it is never too early to begin planning a communications strategy. While you do not want to provide notice before you have gathered sufficient facts, you do not want to leave communications planning to the last minute. Experienced regulatory counsel can help you determine where and when you need to notify law enforcement, state or federal agencies, and affected consumers.

Editor: What do recent enforcement activities tell us about the state of data security compliance?

Savage: Recent enforcement activities, particularly those relating to data breaches involving HIPAA Protected Health Information, tell us a lot about the government's perspective on the state of data security compliance. Within the past two years, the Department of Health and Human Services Office for Civil Rights has entered into Settlements and Corrective Action Plan Agreements with an increasing number of healthcare providers and plans. Those agreements suggest that regulators are concerned about data security compliance in a number of areas. For example, they have reached settlements with organizations that improperly disposed of Protected Health Information by returning copiers to a leasing company without having the hard drive properly wiped clean.

Failure to encrypt laptops or other portable devices remains a significant compliance concern, along with unauthorized use or disclosure of information due to misdirected mail or electronic communications resulting from human error or IT programming/processing problems. Breaches caused by vendors or subcontractors without sufficient data safeguards in place have also been a significant issue – highlighting the need for better data security diligence prior to entering into vendor relationships. Notably, regulators have also begun to scrutinize smaller organizations that have experienced breaches involving fewer than 500 people.

Enforcement trends clearly show that no one is too small to be scrutinized by an investigative agency if a breach occurs. Also, with the implementation of the Omnibus HIPAA rules and the expansion of enforcement authorities' jurisdiction to include business associates, entities that previously did not need to give data security as much attention now need to ensure that they are devoting sufficient resources to ensure compliance.

Please email the interviewees at csavage@choate.com or jhesse@choate.com with questions about this interview.