The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

Volume 20, No. 3 March 2012

Healthcare: A Special Area For Privacy And Data Protection

*The Editor interviews **Jo-Ellyn Sakowitz Klein**, who leads Akin Gump Strauss Hauer & Feld LLP's interdisciplinary privacy and data protection initiative.*

Editor: Please tell our readers about your practice.

Klein: I advise clients primarily in the health, technology, professional sports and insurance industries on best practices and compliance with state and federal privacy and data protection laws. Clients typically approach me with privacy and data protection concerns arising in the course of their operations, in transactions and in connection with strategic planning, as well as when a data incident occurs.

Editor: In a September, 2011 article in this newspaper entitled "Legislative Proposals Compete As Privacy, Data Security, And Breach Notification Continue To Draw The Attention Of Federal Policymakers" to which you contributed, a number of measures introduced in both houses relating to data privacy were discussed. Did any of the measures become law?

Klein: None of the federal proposals have become law as of yet. There has been some discussion of adding data security and/or breach notification provisions to the cybersecurity bill that has seen some movement in the Senate, but its future remains unclear, as there are many critics both in and out of Congress. In terms of predictions for the near future, consumer privacy and data protection issues will continue to receive a lot of attention on the Hill, especially if companies experience more data breaches or other major snafus. Given the current climate and minimal appetite for compromise, however, it seems unlikely that Congress will enact a comprehensive consumer privacy bill this year. For any affected entity, it will be important to monitor the debate, understand how proposals would impact operations and make an active decision on whether to engage in the discussion.

Jo-Ellyn Sakowitz Klein

Editor: The Health Information Technology for Economic and Clinical Health Act (HITECH) expanded the reach of HIPAA (the Health Insurance Portability and Accountability Act of 1996) when it was enacted in 2009. In what ways did it increase enforceability of actions against covered companies?

Klein: HITECH overhauled the HIPAA regime, adding a number of new enforcement tools to the government's arsenal and dramatically enhancing penalties for violations. In my view, one of the biggest game changers so far has been the implementation of the interim final HITECH Breach Notification Rule and the related launch of the HHS Breach Notification Website – often referred to as the HIPAA "wall of shame." Before HITECH, there was no federal requirement to provide individuals with notice of breaches of their unsecured HIPAA-protected health information. Now, under HITECH, many data breaches involving health information must be reported to individuals and, for incidents involving more than 500 individuals, prompt notice to federal regulators and the media may also be required. Information about reported breaches involving more than 500 individuals is posted on the HHS Breach Notification Website for all the world to see. Nothing prevents state or federal authorities from moving forward with an enforcement action against a covered entity upon learning of an incident because it was reported under HITECH and posted to the HHS Breach Notification Website. This "wall of shame" provides low-hanging fruit for those who are charged with enforcement.

Editor: Has "covered entity" now become a larger defined term in terms of encompassing more companies?

Klein: HITECH certainly extended the reach of HIPAA beyond the "covered entities" – health plans, healthcare clearinghouses and most healthcare providers – targeted directly under the original HIPAA regime. HITECH extended the reach of HIPAA not by expanding the definition of "covered entity," though, but by bringing "business associates" – persons outside a covered entity's workforce (such as consultants) and entities (such as practice management companies) that create or receive HIPAA-protected health information to perform functions or services for a covered entity – closer into the fold. Before HITECH, business associates only faced contractual liability for HIPAA-related shortcomings. Covered entities were required to pass their HIPAA privacy and security obligations on to their business associates through "business associate agreements," under which the business associates essentially promised not to do anything inappropriate with the data with which they were entrusted and to safeguard it well. If they fell short in their efforts, the covered entity could pursue remedies under the contract. Under HITECH, in addition to this contractual liability, state and federal authorities will be able to pur-

AKIN GUMP
STRAUSS HAUER & FELD LLP

Please email the interviewee at jsklein@akingump.com with questions about this interview.

sue business associates directly for HIPAA privacy and security failings. Further, post-HITECH, even if the parties do not enter into a business associate agreement, the business associate will still have liability.

Editor: Have there been actions brought recently for breaches of the laws?

Klein: Federal authorities stepped up HIPAA enforcement with the passage of HITECH. After years of minimal enforcement activity, since 2009 we have seen a number of six- and seven-figure settlements (including corrective action plans) and the first-ever HIPAA civil monetary penalty. These settlements and penalties followed investigations of incidents ranging from hospital employees snooping in celebrity medical records, to leaving hard copies of sensitive health records behind on a train while commuting, to failing to afford patients access to, and copies of, their medical records as required by law. HITECH also authorized state attorneys general to bring actions on behalf of their citizens to enforce HIPAA, and several suits have already been brought.

Most recently, the Minnesota attorney general, Lori Swanson, made headlines by bringing the first such HIPAA action against a business associate. The complaint in *Minnesota v. Accretive Health, Inc*. (No. 12-145 (D. Minn. Jan. 19, 2012), ECF No. 1) alleges a range of legal violations, including failing to comply with the HIPAA Security Rule and violating privacy and security terms of a business associate agreement. The data incident giving rise to the complaint, like a surprising number of others, involved sensitive, unencrypted data stored on a portable device that was stolen from a car. In light of these enforcement actions, many entities subject to HIPAA are reevaluating their compliance efforts, including taking a fresh look at their written policies and procedures to confirm that all bases are covered, and ensuring that appropriate steps are being taken to operationalize those policies and procedures effectively.

Editor: What guidance have you given your clients that are covered entities or business associates in terms of compliance so that they do not come into the cross-hairs of an audit or investigation by the HHS Office for Civil Rights (OCR)?

Klein: Among other things, I have been advising clients to reinvigorate their HIPAA training programs and to review their policies and procedures relating to the removal of HIPAA-protected health information from the entity's premises. Many of the headline-grabbing health information data breaches – including the one underlying the action brought by the Minnesota attorney general as well as a major data breach recently endured by TRICARE contractor SAIC – occurred when paper or electronic records (often stored on backup tapes or laptops) were removed from the covered entity's premises. For clients that are business associates, much of my advice has focused on making sure that they have taken appropriate steps to live by promises made in their business associate agreements. More generally, I advise clients that are subject to HIPAA to ensure that they have adopted and implemented appropriate data-handling practices throughout the data life cycle, starting from the moment data is created or received; continuing through its use, transmission, storage, maintenance and disclosure; and not ending until the data has been securely destroyed at the end of its useful life.

Editor: Is the definition of "business associate" very broad, covering anyone supplying these covered entities?

Klein: A wide range of entities – from transcription service providers to third-party administrators to software companies – can fall within the definition of "business associate" if they create or receive HIPAA-protected health information in the course of providing a service on behalf of a covered entity. Not all entities working with HIPAA-covered entities are going to be business associates. Companies with questions about whether they satisfy the regulatory definition of "business associate" should engage in a fact-specific analysis. Notably, the July 2010 proposed HITECH rulemaking proposed expanding the definition of "business associate" further to include subcontractors that create, receive, maintain or transmit HIPAA-protected health information on behalf of a business associate. This would extend the reach of the regulators far downstream from the health provider or other covered entity that interacted with the individual. Many in the industry are eager to see what the final rulemaking will hold on this important point.

Editor: The new Affordable Care Act provides for multiple new access points for provider information. Does this also offer the possibility of data breaches?

Klein: Health reform has some really broad goals – increasing access, improving quality and lowering costs – and to accomplish those goals there are a variety of provisions that affect sharing of information across different provider types and sharing of government information with the provider community. These new forms of communication and new access to information implicate privacy and present some risks. The level of risk will depend on the specific circumstances and the provision of law at issue.

Editor: Are healthcare providers and other custodians of private health information using cloud computing?

Klein: The cloud poses challenges for the HIPAA-regulated health sector. Many questions have arisen about storing HIPAA-protected health information in the cloud: Where is my data? Who can access it? What security controls exist to protect it? Are these security controls adequate? To what extent can I audit those controls? Some are finding comfort with specialized cloud vendors and cybersecurity insurance; some have been shying away.

Editor: What is your prognosis about regulation protecting data privacy not only for the healthcare sector but also for other industries involving personal data?

Klein: 2012 is likely to be a big year in privacy and data protection. In the health sector, federal regulators have set a March 2012 target date for issuing final rules to modify the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules to implement HITECH. They have also set a June 2012 target date for finalizing a controversial rule on accounting for disclosures of HIPAA-protected health information. Moving outside the health sector, we can expect to see continued debate on consumer privacy and data protection issues. Just last week, the Obama administration released a framework for protecting consumer privacy online, including a "Consumer Privacy Bill of Rights." We have also seen a marked increase in industry self-regulation, raising questions about the need for extensive government regulation to protect consumers online. This is a very exciting time for those of us who follow privacy and data protection issues, as the debate is moving to the next level.