Advisory

JANUARY 2013

If you have any questions about this Advisory, please contact:

MICHELLE WILCOX DEBARGE
860.297.3702
mdebarge@wiggin.com

Summary of Wiggin and Dana's Fifth Annual Health Care Compliance and Enforcement Roundtable on HIPAA Enforcement

Wiggin and Dana LLP recently held its Fifth Annual Health Care Compliance and Enforcement Roundtable, where state and federal enforcement officials discussed HIPAA/HITECH enforcement priorities and breach notification requirements with members of the health care community.

Michelle DeBarge, Wiggin and Dana Partner and Chair of Wiggin and Dana's HIPAA Practice, moderated the program. Linda Sanches, Senior Advisor for Health Information Privacy in the Office for Civil Rights ("OCR") within the United States Department of Health and Human Services, participated in the Roundtable along with Connecticut Assistant Attorney General ("AAG") Matthew Fitzsimmons, Leader of the Connecticut Office of the Attorney General's ("AG's Office") Privacy Task Force, and AAG Thomas Ryan, Member of the AG's Office Privacy Task Force.

THE FEDERAL PERSPECTIVE

Linda Sanches indicated that the 2009 passage of HITECH, The Health Information Technology for Economic and Clinical Health Act, "changed everything" at OCR because it vested OCR with new authority to pursue different areas of HIPAA enforcement and provided OCR with a new, more robust penalty structure to address violations. In particular, the HITECH Breach Notification Rule, requiring covered entities to notify affected individuals, OCR, and the media of breaches of unsecured protected health information in certain circumstances, creates a higher level of transparency between providers and consumers. Ms. Sanches emphasized the importance of transparency and compliance as more providers shift from paper to electronic medical records and the protection of electronic protected health information becomes a critical concern. Ms. Sanches said that OCR's priority is to ensure a culture of HIPAA compliance within the health care industry. She indicated that OCR's pilot audit project, more fully described below, and the more serious penalties for noncompliance are essential tools OCR is using to ensure this priority is achieved.

CONNECTICUT'S PERSPECTIVE

AAG Thomas Ryan indicated that the AG's office's greatest concern is helping entities protect information and working with them to mitigate harm when there is a breach. The AG's Office primarily investigates calls and complaints from individual consumers. AAG Matthew Fitzsimmons stated that the Privacy Task Force's primary goal is to educate the public on personal data privacy and security generally, including the particular concerns relating to HIPAA compliance.

STATE AND FEDERAL AUTHORITIES WORK TOGETHER

While there has not yet been any joint federal-Connecticut HIPAA investigation,

CONTINUED ON NEXT PAGE

Summary of Wiggin and Dana's Fifth Annual Health Care Compliance and Enforcement Roundtable on HIPAA Enforcement CONTINUED

OCR and the AG's Office communicate about HIPAA investigations occurring in Connecticut. OCR and the AG's Office share information and OCR provides the AG's Office with technical support and assistance in analyzing potential HIPAA violations. Although the two offices work together, the law also allows them to pursue parallel investigations that ultimately could result in "double" penalties, since the federal and state penalties are not mutually exclusive. However, before filing a HIPAA action in federal court, the AG's Office is required to provide OCR with the opportunity to intervene. If OCR decides to intervene, the AG's office is precluded from pursuing actions under HIPAA, but may still proceed based on violations of Connecticut law.

COMPLAINT INVESTIGATION PROCESS

The Federal Process

OCR receives thousands of complaints a year alleging HIPAA violations. Upon receiving a written complaint, OCR determines if it has jurisdiction. If OCR finds that it has jurisdiction, then the appropriate regional office begins the investigation by interviewing the complainant. If the regional office believes there is a potential HIPAA violation, it will then request information from the covered entity or business associate, usually by letter. Such a request typically asks for a response to the allegations, applicable policies and procedures, workforce training records, job descriptions, business associate agreements, and evidence of a compliance program. Above all, OCR looks for evidence that a provider has a true culture of compliance. Evidence of a robust compliance program will likely include records of complaints, investigations of those complaints, and actions taken in response to those investigations. Ms. Sanches mentioned that while documentation of workforce training is important, OCR also looks for evidence of meaningful follow-up between management and workforce members after training, including, for example, documentation of random checks and monitoring of compliance.

With regard to business associates, Ms. Sanches explained that OCR looks not only for signed copies of business associate agreements, but also for evidence of communication between the covered entity and its business associates about potential violations and evidence that the covered entity pursues concerns that it may have about a business associate's conduct. Ms. Sanches stated that while there is no affirmative requirement to monitor business associates under HIPAA, if an entity becomes aware of an issue with one of its business associates, the entity is bound under the Privacy Rule to pursue the issue and take action, up to and including terminating the contract or informing OCR. In a situation where an entity had concerns about a business associate and did not work to resolve those concerns, both the covered entity and the business associate would be liable for any resulting violations.

Ms. Sanches emphasized that cooperation with OCR during an investigation should be a top priority. Refusing to cooperate with an investigation results in a lost opportunity to resolve the matter informally and, in the past, has led to the imposition of civil monetary penalties.

The Connecticut Process

Unlike OCR, the Connecticut AG's Office resolves complaints about many different types of privacy and security breaches, not just those involving health information. The Connecticut General Assembly recently approved a modification to the State statute governing breaches of electronic personal information, requiring any entity conducting business in the State to provide notice of breaches to the Attorney General in addition to notice to the affected individual. According to the AAG panelists, the AG's Office receives approximately seven complaints a week via electronic submissions, correspondence, or telephone. After a discussion with the complainant, the AG's Office contacts the entity or person alleged to have committed a breach to investigate. One of the AG Office's primary objectives upon discovering a breach is minimizing the potential damage to individuals. Therefore, the AG's Office tends to view favorably an entity or person that responds promptly and takes effective actions to mitigate any negative consequences. In contrast, if the AG's Office finds that the entity or person did not react quickly or take steps to mitigate the breach, there likely will be further AG investigation and greater penalties assessed.

OCR PILOT AUDIT PROJECT

Ms. Sanches explained that the OCR pilot audit project began with the development of audit protocols to investigate adherence to the full scope of HIPAA requirements – the Privacy Rule, the Security Rule, and the Breach Notification Rule. The OCR protocol was first tested on twenty entities, and after receiving feedback and improving the

CONTINUED ON NEXT PAGE

Summary of Wiggin and Dana's Fifth Annual Health Care Compliance and Enforcement Roundtable on HIPAA Enforcement CONTINUED

protocol, OCR added ninety-five additional entities, comprised of a mix of public and private plans, clearinghouses, and small and large provider entities. According to Ms. Sanches, the next round of audits will likely include business associates and, in the future, OCR may choose to audit only certain HIPAA provisions as opposed to all HIPAA requirements under the global audit process currently used.

The Audit Process

An OCR audit is initiated by a letter of notice, followed by a request for data and an onsite visit. The request for data and documents is similar to a request made in the complaint investigation process. The length of the onsite visit and the number of auditors in attendance will vary depending upon the size of the entity: while a large hospital may have five to seven auditors visit for a week, a doctor's office may have one to two auditors onsite for only a few days. The onsite visit includes meeting with the entity leadership to discuss observations and findings, after which the entity is given an opportunity to respond. OCR reviews the draft audit and the entity's response and finalizes the audit report. If an audit report indicates a serious compliance issue, OCR may initiate a compliance review to address the problem. OCR will not be posting a list of audited entities or the findings of an individual audit that identifies the audited entity. According to Ms. Sanches, OCR has not yet issued any final audit reports.

Surviving an OCR Audit

Based on the draft reports OCR has reviewed to date, Ms. Sanches listed a number of common problems auditors have uncovered, for example:

- Risk assessments were never completed, were not current or were completed but never used to inform the entity's policies and procedures to safeguard protected health information;
- Policies and procedures were written, but never acted upon or implemented; and
- The parts of the entity responsible for privacy on the one hand, and security on the other, were not communicating with each other to develop and implement necessary protections or to resolve any complaints or issues.

According to Ms. Sanches, an OCR audit looks at the overall *effectiveness* of a compliance program. It is not just a matter of having and implementing a compliance program; the compliance program must be effective in meeting the standards and achieving the goals of HIPAA and HITECH.

BREACH NOTIFICATION

In response to a question about determining what constitutes a "substantial risk" triggering the need to report a breach under HIPAA and HITECH, Ms. Sanches acknowledged that making such a determination is a difficult task and suggested that until additional guidance is available, an entity can best protect itself by documenting its breach notification "substantial risk" assessment and its responses to mitigate the areas of risk found in such assessment. OCR indicated that entities could expect further guidance on this issue to be released soon.

The AAGs indicated that the State breach notification statute requires a business owner who has had a breach of security, as defined by statute, to provide notice both to the individual whose electronic personal information was improperly accessed and to the AG's Office. Unlike federal law, Connecticut's law does not include a "substantial risk" test and therefore if there is improper access to personal information, notification must be made regardless of whether the business owner believes the improper access creates substantial risk to the affected individual.

ASSESSING PENALTIES AND OTHER CONSEQUENCES

The Federal Perspective

Ms. Sanches indicated that there is neither a formal handbook nor a standard formula for calculating civil monetary penalties for violations of HIPAA. Depending upon the facts and circumstances of each case, penalties can be assessed per day, by the number of people affected, or by the number of people affected per day. Ms. Sanches said that OCR would use whichever formulation made the most sense for a particular case. There are penalty caps that place a ceiling of $1.5 million for all violations of an identical requirement or prohibition during a calendar year, and these ceilings can be reached quickly depending upon how OCR chooses to calculate the penalty. Beyond monetary penalties, OCR requires corrective actions to assist entities in fixing systematic problems to protect patient information going forward.

CONTINUED ON NEXT PAGE

Summary of Wiggin and Dana's Fifth Annual Health Care Compliance and Enforcement Roundtable on HIPAA Enforcement CONTINUED

The Connecticut Perspective

The Connecticut AG's Office's primary concern is whether an entity took steps to promptly mitigate the privacy or security issue when it was discovered. As an example of a mitigating step, Mr. Fitzgerald and Mr. Ryan suggested that entities could obtain an affidavit from an individual who may have received protected health information or personal information erroneously, attesting to the fact that there has been no misuse or further transmittal of the information. They stressed that entities are not required to obtain such affidavits, but that the affidavits are an example of a step entities can take to mitigate harm to individuals after a breach has occurred. If an AG pursues civil action in federal court for HIPAA violations, penalties are capped at $25,000 for all violations of an identical requirement or prohibition during a calendar year. This may be in addition to any penalties assessed for violation of state laws.

Both federal and state legislatures have made it clear that they expect covered entities and business associates to implement meaningful and effective privacy and security practices. Now, federal and state agencies are using their audit and investigation powers and implementing penalties to enforce these expectations. It is no longer a question of *if* a covered entity or business associate will be audited or investigated; it is a matter of *when*. Covered entities and business associates should seize this opportunity to analyze their compliance programs with an eye toward preparing for the eventual audit or complaint investigation. Key to this analysis is remembering that OCR and the AG's Office are looking for a culture of compliance, including an effective and well-documented compliance program. Covered entities and business associates should also be on the lookout for OCR's final HITECH rule, which Ms. Sanches assured the audience would be released soon. The rule will provide further guidance to covered entities and business associates on their HITECH responsibilities.

HEALTH CARE COMPLIANCE PRACTICE GROUP

Wiggin and Dana's Health Care Compliance Practice Group brings together the firm's substantive knowledge in health care law and reimbursement with our extensive experience in internal and government investigations. Wiggin and Dana has one of the largest health care practices in the region with breadth and range of experience at both the federal and state levels. In addition, our White Collar, Internal Investigations and Government Investigations Practice Group includes seasoned former federal prosecutors with the essential skills and insights to protect and advance clients' interests during government investigations.

HIPAA PRACTICE GROUP

Wiggin and Dana's knowledgeable HIPAA (Health Insurance Portability and Accountability Act) team helps clients nationwide develop and implement practical, tailored strategies to stay compliant with the far-reaching and complex requirements of HIPAA and HITECH (Health Information Technology for Economic and Clinical Health Act). Our HIPAA team also helps clients address other privacy and security requirements that may apply to them.