

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

MICHELLE DEBARGE  
860.297.3702  
mdebarge@wiggin.com

JODY ERDFARB  
203.363.7608  
jerdfarb@wiggin.com

## HIPAA Enforcement Update

While the Omnibus HIPAA regulations were promulgated over a year ago and are becoming more familiar, the HIPAA enforcement landscape continues to evolve. The federal government is determined to have HIPAA taken more seriously and is continuing to make strides in HIPAA enforcement. Covered entities and business associates need to be aware of these developments so that they are prepared should they be investigated or audited.

Over the last several weeks, the United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) took additional steps to support HIPAA compliance and enforcement. Last month, OCR, in collaboration with the Office of the National Coordinator for Health Information Technology (ONC), released a new security risk assessment (SRA) tool to help health care providers conduct HIPAA Security Rule assessments. In addition, OCR recently announced a new HIPAA settlement with Skagit County in Washington, as well as the launch of a second round of HIPAA audits, which will include HIPAA business associates.

OCR's HIPAA enforcement efforts have steadily increased, but the Federal Trade Commission (FTC) also recently decided to take a more aggressive approach in pursuing HIPAA violations that involve data security. With this additional governmental entity joining HIPAA's enforcement framework, HIPAA covered entities and business associates now face potential

investigations and penalties from multiple federal and state authorities, making it even more crucial to be HIPAA audit-ready and to inculcate an organization-wide HIPAA compliant culture.

### SRA TOOL

In recognition that the risk management process can be exceptionally time consuming and complex, OCR/ONC created a new tool to help health care providers in small to medium sized offices conduct a HIPAA compliant Security Rule risk assessment. During its pilot audit program, OCR uncovered many instances of Security Rule non-compliance, specifically the failure to conduct a thorough and accurate risk assessment. Those results likely motivated the development of this new SRA tool.

The very first Security Rule standard mandates that covered entities and business associates have security management processes in place to prevent, detect, contain, and correct security violations. In order to comply with that standard, HIPAA requires covered entities and business associates to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of their electronic protected health information (PHI). This risk assessment is the foundation for full Security Rule compliance, since it identifies the risks and vulnerabilities that need to be mitigated. However, the assessment also must be ongoing to ensure that risks are reevaluated with the

CONTINUED ON NEXT PAGE

## HIPAA Enforcement Update

development of new technologies and the evolution of business and clinical practices.

The SRA tool consists of 156 questions covering each Security Rule standard and implementation specification, many of which can be answered with a yes or no response. The tool also contemplates that specific information about the use of PHI and a remediation plan to mitigate any identified risks will be detailed as well. Additionally, the tool includes OCR guidance in sections entitled, "Things to Consider to Help Answer the Question." Many will undoubtedly find the tool very helpful; however, populating the form is only one step in the process of complying with the Security Rule. Additional steps must be taken to assess the information and implement appropriate safeguards necessary to protect electronic PHI from identified risks and vulnerabilities.

### ANOTHER ROUND OF HIPAA AUDITS; BUSINESS ASSOCIATE INCLUDED

On February 24, 2014, OCR published a notice in the Federal Register seeking comments on its plan to survey 1200 covered entities and business associates in order to generate a pool of organizations to audit later this year in its second round of nationwide HIPAA compliance audits. The survey will gather information, such as the number of recent patient visits or insured lives, use of electronic information, revenue, and business locations. OCR estimates that it will take between 30-60 hours to complete each pre-audit survey.

OCR audited 115 covered entities for HIPAA compliance in late 2011 and throughout 2012 as a pilot program. While little information is available about the new round of audits,

OCR indicated that it will include business associates this time and will also cover the new regulatory requirements that were promulgated as part of the HIPAA Omnibus Rule in 2013.

Despite OCR's pilot audit program, in November 2013, HHS' Office of Inspector General (OIG) released a scathing report alleging that OCR has not met its obligations to audit covered entities and business associates. OCR responded that it was developing a more permanent audit program. The proposed pre-audit survey seems to be OCR's first step in that direction.

To prepare for these audits, covered entities and business associates should ensure that their HIPAA compliance documentation is readily available, up-to-date, accurate, and in full compliance with all applicable requirements. Required documentation includes policies and procedures, business associate agreements, risk assessments, breach logs, and employee training.

Also, since OCR will be conducting site visits, covered entities and business associates should ensure that all written policies and procedures are fully implemented as drafted. A HIPAA compliance program that is robust on paper, but that is not fully operational "on the ground," will not suffice. All employees should understand the rules applicable to their job responsibilities, be able to identify the privacy and security officers, and know how to report suspected problems. Additionally, covered entities and business associates should closely monitor the OCR website for audit-related announcements, assign a team to handle audit readiness, and consider conducting an internal HIPAA audit to ensure that they are fully compliant.

CONTINUED ON NEXT PAGE

## HIPAA Enforcement Update

### NEW HIPAA SETTLEMENT

On March 7, 2014, OCR announced that it entered a settlement with Skagit County, Washington ("Skagit") for \$215,000. OCR alleged that Skagit failed to comply with HIPAA's breach notification requirements and generally failed to implement Security Rule requirements, having insufficient policies and procedures and no security awareness and training for workforce members. As part of the settlement, Skagit also agreed to enter a three-year corrective action plan.

OCR began its investigation of Skagit after receiving a breach notification report from the county explaining that money receipts for seven individuals, containing electronic PHI, were improperly accessed by unauthorized individuals. OCR discovered that this breach occurred partly because Skagit inadvertently exposed the PHI of 1,581 individuals on a publicly accessible server. Many of the accessible files involved sensitive information concerning the testing and treatment of infectious diseases. OCR alleged that Skagit should have notified each of these individuals pursuant to HIPAA's Breach Notification Rule. Additionally, upon further investigation, OCR alleged that Skagit had virtually no Security Rule compliance at all.

This is OCR's first settlement with a county government and Susan McAndrew, HHS's Deputy Director of Health Information Privacy, stated that the settlement is intended to send a "strong message" about the importance of HIPAA compliance "regardless of size." OCR's investigation of smaller providers for noncompliance, as well as large organizations, is becoming increasingly common. In fact,

OCR's last settlement in December 2013, was for \$150,000 with Adult & Pediatric Dermatology, P.C., a 12-physician private dermatology practice.

### FTC HIPAA ENFORCEMENT

The FTC has a long history of investigating and commencing enforcement actions against companies for failure to adequately protect consumer data. The FTC argues that such failures constitute unfair and deceptive trade commercial practices under Section 5 of the FTC Act and that its enforcement activities have "helped to increase protections for consumers and has encouraged companies to make safeguarding consumer data a priority."

In two cases in the past, in 2009 and 2010, the FTC and OCR jointly entered into settlement agreements with large nationwide health care pharmacy chains for data breaches involving both PHI and other personally identifiable sensitive data. Otherwise, the FTC has left data security cases involving health care providers and health information to OCR to pursue. However, the FTC has recently revealed a burgeoning interest in data security cases involving HIPAA violations.

Notwithstanding that OCR is the federal agency responsible for HIPAA enforcement, the FTC is serious about pursuing data security cases involving organizations covered by HIPAA and is undeterred by objections to its enforcement in this arena. In December of 2013, the FTC entered into a settlement agreement with Accretive Health, a technology and business processes service provider that stores and processes the PHI of hospital patients. The settlement concerned a

CONTINUED ON NEXT PAGE

## HIPAA Enforcement Update

data breach involving a laptop containing over 600 files with PHI on 23,000 patients, which was stolen from an employee's car. More recently, on January 31, 2014, GMR Transcription Services, Inc. which provides medical transcription services, agreed to settle FTC charges that its inadequate data security measures unfairly exposed the PHI of thousands of consumers on the open internet.

In another case, the FTC accused LabMD, a clinical laboratory that performs tests on specimen samples from consumers, of failing to reasonably protect the security of consumers' personal data, including medical information. The FTC claimed that, in two separate incidents, LabMD collectively exposed the PHI of approximately 10,000 consumers. LabMD challenged the FTC's right to enforce HIPAA violations by filing a motion to dismiss the FTC's administrative complaint. However, on January 16, 2014, the FTC denied LabMD's motion, stating that that the FTC, "cannot enforce HIPAA and does not seek to do so," but that "HIPAA and other statutes do not shield LabMD from the obligation to refrain from committing unfair data security practices that violate the FTC Act."

Please feel free to contact any member of our health care compliance team if you have questions about this advisory or need assistance. Wiggin and Dana's health care compliance team regularly counsels clients on compliance with HIPAA and other federal privacy and security statutes and regulations. We advise clients in development of privacy and data security policies and procedures, and help with implementation and internal auditing. We assist clients in preventing and responding to data mismanagement or data breaches, including implementing breach notification, mitigation, and corrective action strategies. We also handle state Attorney General and federal OCR and FTC investigations of alleged data breaches.

*This publication is a summary of legal principles. Nothing in this article constitutes legal advice, which can only be obtained as a result of a personal consultation with an attorney. The information published here is believed accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.*