# Advisory

SEPTEMBER 2016

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

JODY ERDFARB
203.363.7608
jerdfarb@wiggin.com



## OCR Continues to Strengthen HIPAA Enforcement Efforts

The United States Department of Health and Human Services Office for Civil Rights ("OCR") sent a strong HIPAA enforcement message this summer, entering four resolution agreements, including the highest financial settlement to date, and announcing an initiative to investigate smaller breaches more widely. Each new resolution agreement resulted from self-reported breaches and demonstrates OCR's focus on portable electronic devices:

1. On June 29, 2016, OCR entered into a resolution agreement with Catholic Health Care Services of the Archdioceses of Philadelphia ("CHCS"), a senior living provider that also delivers management and information technology services as a business associate to six of its nursing homes. In February 2014, the nursing homes reported to OCR that a CHCS-issued unencrypted iPhone, containing the protected health information ("PHI") of 412 individuals, was stolen. CHCS agreed to pay $650,000 and enter a two-year corrective action plan to resolve OCR's allegations that CHCS had "no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident" and "no risk analysis or risk management plan."[1] This is the first enforcement action OCR has taken against a business associate since the HIPAA Omnibus Rule was enacted in 2013.
2. On July 18, 2016, Oregon Health & Science University ("OHSU") agreed to pay $2.7 million dollars and enter into a three-year corrective action plan to resolve OCR's allegations of "widespread and diverse" HIPAA noncompliance. OHSU reported breaches involving:
   - an unencrypted laptop, containing the PHI of 4,022 patients, that was stolen from a vacation apartment in Hawaii rented by an OHSU surgeon;
   - an unencrypted laptop, containing the PHI of about 1,000 patients, that was stolen from an employee's car;
   - a stolen unencrypted thumb drive, containing the PHI of about 14,000 premature infants, that an employee brought home without authorization; and
   - the storage of the PHI of over 3,000 individuals on Google Drive/Mail, a cloud-based server – even though OHSU did not have a business associate agreement in place with Google – by OHSU's residents who were using the internet based service to maintain spreadsheets in order to provide each other with up-to-date information about patients.[2]
3. On July 21, 2016, OCR announced a resolution agreement with the University of Mississippi Medical Center ("UMMC") under which UMMC agreed to pay $2.75 million and adopt a three-year corrective

CONTINUED ON NEXT PAGE

## OCR Continues to Strengthen HIPAA Enforcement Efforts

action plan. UMMC filed a breach report regarding a missing laptop that was used as a shared device by clinicians. According to OCR, its investigation revealed that PHI stored on a network drive was vulnerable to unauthorized access via UMMC's wireless network because users could access an active directory containing PHI after entering a generic username and password.[3]

4. On August 4, 2016, in the largest monetary HIPAA settlement to-date against a single entity, Advocate Health Care Network ("Advocate"), the largest fully integrated health care system in Illinois, agreed to pay $5.55 million and to enter into a two-year corrective action plan to resolve OCR's allegations that it violated multiple HIPAA requirements. OCR began investigating Advocate after receiving three breach notification reports affecting approximately 4 million individuals, involving Advocate's subsidiary, Advocate Medical Group, a nonprofit physician-led medical group that provides primary care, medical imaging, outpatient and specialty services. The breaches involved stolen desktop computers, a stolen laptop, and unauthorized access by a third party to the network of Advocate's business associate. According to OCR, the large settlement was a result of "the extent and duration of the alleged noncompliance (dating back to the inception of the Security Rule in some instances), the involvement of the State Attorney General in a corresponding investigation, and the large number of individuals whose information was affected."[4]

Finally, on August 18, 2016, OCR announced its initiative to "more widely" investigate breaches affecting fewer than 500 individuals. In an email message posted to the OCR Privacy list serve, OCR explained that OCR's Regional Offices currently investigate all reported breaches involving the PHI of 500 or more individuals, but only investigate reports of smaller breaches, "as resources permit." OCR announced that it "has begun an initiative to more widely investigate the root causes of breaches affecting fewer than 500 individuals." Each Regional Office will retain discretion to prioritize which smaller breaches to investigate, but will increase efforts to obtain corrective action to address noncompliance.

The resolutions, settlements and the announced new initiative signal that OCR continues to strengthen its HIPAA enforcement efforts. Covered entities and business associates should take this opportunity to emphasize the risks of noncompliance within their organizations and ensure that they have robust HIPAA compliance programs that can withstand OCR's ever-increasing scrutiny.

### 2016 CYBER AND PRIVACY FORUM

Wiggin and Dana will be hosting its annual Cyber and Privacy Forum on Thursday, September 22, 2016 at the Omni New Haven Hotel at Yale. For more information please **click here**.

*[1] http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/catholic-health-care-services/index.html.*

*[2] http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ohsu/index.html.*

*[3] http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/UMMC/index.html.*

*[4] http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ahcn/index.html.*