KRONICK
MOSKOVITZ TIEDEMANN & GIRARD

Legal Alert

May 23, 2017
Bulletin No. 127406.1

RELATED AREAS OF PRACTICE

Health Care

WWW.KMTG.COM

Recent Developments in HIPAA Enforcement

During the month of April, 2017, the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) announced three agreements to settle potential violations of the Health Insurance Portability and Accountability of 1996 (HIPAA). The OCR's settlements represent efforts to actively enforce the privacy, security and breach notification provisions of HIPAA. (The standards that govern privacy are set forth at 45 C.F.R. Part 160 and Subparts A and E of Part 164 (the "Privacy Rule"); the standards that govern security are located at 45 C.F.R. Part 160 and Subparts A and C of Part 164 (the "Security Rule"); and the standards that govern notification of the breach of unsecured protected health information (PHI) are located at 45 C.F.R. Part 160 and Subparts A and D of Part 164 (the "Breach Notification Rule").)

Two of the three settlements arose from the health service provider's failure to conduct an adequate risk assessment prior to the breach of unsecured PHI and to have appropriate security remediation policies and procedures in place when the breach occurred. The absence of risk assessment and remediation policies and procedures came to light in the OCR's investigations undertaken after the providers reported thefts of electronic PHI (ePHI) through hacking (phishing) and stolen laptop incidents, respectively. The third settlement involved the provider's disclosure of PHI to a medical records storage vendor in the absence of a valid business associate agreement, which the OCR discovered in the course of investigating the vendor. As detailed below, each of the settlements required the provider to make a substantial payment to the OCR and enter into a multi-year corrective action plan (CAP).

1. FQHC's Failure to Conduct a Risk Assessment and Implement Risk Management Procedures Results in $400,000 Settlement with the OCR

On April 12, 2017, the OCR announced the $400,000 payment in connection with potential HIPAA violations by Metropolitan Community Provider Network (Metropolitan), a federally qualified health center (FQHC). Metropolitan provides primary medical, dental, pharmacy, social work and behavioral health care services in the greater Denver metropolitan area to approximately 43,000 patients each year, most of whom have incomes at or below the poverty level. In addition to the payment of $400,000, the settlement agreement with the OCR required the FQHC to enter into a three-year corrective action plan (CAP).

In December, 2011, a hacker accessed the FQHC's employee e-mail accounts through a phishing incident and obtained ePHI belonging to 3,200 individuals. Metropolitan reported the breach incident to the OCR in January, 2012, which prompted the OCR's investigation. The agency determined that the FQHC had taken necessary corrective action following the breach, but delayed conducting a risk assessment until mid-February, 2012. Further, the FQHC had not conducted a risk analysis prior to the incident to assess the risks and vulnerabilities of ePHI stored in its facilities, and therefore had not implemented any remedial risk management procedures. Further, the risk analyses conducted by the FQHC following the breach incident did not satisfy the HIPAA Security Rule's criteria.

The OCR concluded that the FQHC had violated the Security Rule's standard requiring a "security management process." That standard specifically mandates risk analysis of the confidentiality, integrity and availability of ePHI held by the covered entity (or business associate), and the implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

In addition to the payment of $400,000, the settlement requires Metropolitan to enter into a three-year CAP, which consists of five "corrective action obligations." First, the provider must, subject to the OCR's review and

RELATED AREAS OF PRACTICE

Health Care

approval, conduct a risk analysis and submit written reports of the security risks and vulnerabilities in all facilities, electronic equipment, data systems and applications which are controlled, currently administered or owned by Metropolitan and which store, transmit or receive ePHI. Second, the FQHC must develop and implement an organization-wide risk management plan to address and mitigate the security risks and vulnerabilities identified in the risk analysis. Third, based on the findings from the risk analysis and implementation of the risk management plan, the Metropolitan must review and, as necessary, revise its Security Rule policies and procedures. Fourth, the FQHC must review and, as necessary, revise its Security Rule training materials and administer a Security Rule training program on at least an annual basis for each workforce member who has access to ePHI and, for each new member of the workforce with access to ePHI, within thirty days of his or her start date. Fifth, during the three-year compliance term, upon receiving information that a workforce member may have failed to comply with the FQHC's Security Rule policies and procedures, the FQHC must promptly investigate the matter and, if a violation is detected, report it to the OCR.

The full text of the OCR's announcement of its settlement with Metropolitan is available on the OCR website. The Resolution Agreement and Corrective Action Plan are available.

2. Wireless Cardiac Monitoring Technology Provider's Insufficient Risk Analysis and Security Management Procedures at Time of Laptop Theft Leads to $2.5 Million Settlement

On April 24, 2017, the OCR announced that CardioNet, a wireless health services provider, had agreed to pay $2.5 million to settle potential noncompliance with the HIPAA Privacy and Security Rules. CardioNet is a Pennsylvania-based provider of wireless mobile monitoring and rapid response services to patients at risk for cardiac arrhythmias. The settlement is the first one between the OCR and a wireless health technology service provider. In addition to the $2.5 million payment, the Resolution Agreement between CardioNet and the OCR required CardioNet to enter into a two-year CAP.

In 2012, CardioNet notified the OCR of the theft of a workforce member's laptop computer containing the ePHI for 1,391 individuals. The OCR subsequently investigated the wireless health technology provider's compliance with the Privacy, Security and Breach Notification Rules.

That investigation revealed that CardioNet did not have sufficient risk analysis and management procedures in place when the laptop theft occurred. Among other findings, the OCR concluded that CardioNet failed to comply with the Security Rule's "security management process" standard, which obligated the provider to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI, and to plan for and implement security measures sufficient to reduce those risks and vulnerabilities.

In addition, the OCR found that CardioNet failed to comply with the "device and media controls" standard in the Security Rule in that, until March, 2015, the wireless health services provider did not produce any final policies and procedures governing the encryption, receipt, removal from or movement within its facilities of hardware and electronic media containing ePHI.

Under the two-year CAP, CardioNet must comply with five primary corrective action obligations similar to those described above with respect to Metropolitan. CardioNet's CAP requires it to focus particular attention on Security Rule policies and procedures applicable to wireless device and media controls. In addition, CardioNet must provide the OCR with certification that all laptops, flashdrives, SD cards and other portable media devices are encrypted, including a description of the encryption methods used.

The full text of the OCR's announcement is on the OCR website. The Resolution Agreement and Corrective Action Plan are available.

3. Pediatric Subspecialty Practice

WWW.KMTG.COM

Agrees to Pay $31,000 after the OCR's Investigation of Medical Records Vendor Reveals Missing Business Associate Agreement

The OCR's settlement with The Center for Children's Digestive Health (CCDH), announced on April 20, 2017, involved the relatively smaller payment of $31,000 by CCDH to settle potential violations of the Privacy Rule. Nevertheless, this enforcement action by the OCR warrants attention from all covered entities because it originated from the OCR's investigation of the provider's medical records storage vendor, which lead to discovery of the covered entity's failure to implement a valid business associate agreement with that vendor.

The OCR conducted a compliance review of CCDH in August, 2015, following an investigation of Filefax, Inc. ("Filefax"). CCDH had engaged Filefax as a business associate in 2003 for the purpose of storing inactive paper medical records. Although the OCR's investigation indicated that CCDH had begun disclosing PHI to Filefax in 2003, neither CCDH nor Filefax could produce a signed Business Associate Agreement until October 12, 2015.

Consequently, the OCR determined, first, that CCDH had failed to comply with the provision of the HIPAA Privacy Rule which allows a business associate to create, receive, maintain or transmit PHI for the covered entity only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information. The parties must enter into an agreement that meets the HIPAA criteria for a valid business associate agreement. Second, CCDH impermissibly disclosed the PHI of at least 10,728 individuals to Filefax when CCDH transferred the PHI to Filefax in the absence of a valid business associate agreement.

In addition to the payment of $31,000, CCDH is subject to a CAP for a two-year period. Among the corrective action obligations set forth in the CAP, CCDH must report to the OCR the names of all business associates, and must provide copies of the service and/or business associate agreements between CCDH and such parties. In addition, if CCDH is involved in an asset sale pursuant to which CCDH would, as of the closing date, no longer operate as a covered entity, the CAP requires CCDH to give the OCR assurances that it will appropriately safeguard any PHI that remains in its possession or control after the closing date of the sale.

The full text of the OCR's announcement of the settlement with CCDH is available on the OCR website. The Resolution Agreement and Corrective Action Plan are available.

Questions

Kronick can assist providers and suppliers in the compliance of their health care operations and transactions with HIPAA and in establishing policies and procedures for HIPAA compliance as part of a comprehensive corporate compliance program. To learn more, contact us.

Lawrence Garcia

lgarcia@kmtg.com | 916.321.4500

Christine Cohn

ccohn@kmtg.com | 818.469.7147

RELATED AREAS OF PRACTICE

Health Care

WWW.KMTG.COM