OCR CONTINUES HEIGHTENED PACE OF HIPAA ENFORCEMENT ACTIONS

If HIPAA covered entities thought the increased rate of enforcement actions at the beginning of 2017 by the Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") was an anomaly, a flurry of settlement announcements by OCR in April indicate the trend may continue. The three recent enforcement actions discussed below demonstrate the varied nature of these actions and the types of covered entities involved.

BREACH OF ELECTRONIC PHI VIA PHISHING SCHEME

On April 12, 2017, OCR announced a $400,000 settlement with a federally qualified health center ("FQHC") as a result of unauthorized access to electronic PHI ("ePHI"). Given the nature of the provider, a significant portion of the individuals served by the FQHC are below the poverty level, which was a factor in OCR's determination of the settlement amount but did not allow FQHC to avoid liability.

FQHC fell victim to a phishing scheme that provided unauthorized users with access to FQHC employee email accounts, which ultimately resulted in access to ePHI. Through its subsequent investigation, OCR concluded that FQHC violated 45 C.F.R. § 164.308 due to its failure to conduct a sufficient risk assessment regarding its ePHI and to implement a reasonable and sufficient risk management plan in accordance with HIPAA. Although FQHC eventually took corrective action in response to the phishing scheme, the security risk analysis was conducted after the fact and was not compliant with the HIPAA Security Rule.

FQHC's corrective action plan requires FQHC to: (i) conduct a comprehensive risk analysis of security risks and vulnerabilities; (ii) develop an organization-wide risk management plan based on the risk analysis; and (iii) review and revise its Security Rule policies and procedures and training materials based on the risk analysis.

LACK OF BUSINESS ASSOCIATE AGREEMENT

Under a settlement agreement announced by OCR on April 20, 2017, a small Illinois health care center with a pediatric subspecialty practice ("Center") must implement a corrective action plan and pay $31,000 as a result of failing to have a business associate agreement in place. This enforcement action against a small, for-profit provider demonstrates OCR's enforcement attention to all types of covered entities.

Notably, OCR's investigation of the Center flowed from an initial investigation of FileFax, which was functioning as a business associate to the Center by providing storage of records containing PHI. The investigation concluded that the Center was in breach of 45 C.F.R. § 164.308 by providing PHI to FileFax without first executing a business associate agreement.

Among various other obligations, the corrective action plan between OCR and the Center requires the Center to do the following: (i) develop, maintain and revise, as necessary, its HIPAA policies and procedures, including the information specified in the corrective action plan; (ii) provide HHS with a list of all business associates and the corresponding service agreements and/or business associate agreements; and (iii) review and revise their training program.

BREACH OF EPHI VIA STOLEN LAPTOP

On April 24, 2017, OCR issued a press release regarding its first enforcement action involving a wireless health service provider ("Service Provider"). While Service Provider provides mobile monitoring and response services for cardiac arrhythmia patients, they are part of a larger trend toward mobile, real-time monitoring. As delivery methods and technology in health care continue to evolve, so also does the nature of enforcement actions.

The $2.5 million settlement between OCR and Service Provider stemmed from an impermissible disclosure of unsecured ePHI, as a Service Provider employee's laptop containing ePHI of nearly 1,400 individuals was stolen. This fact pattern has become a common theme among OCR enforcement actions, as the use of and risks presented by mobile devices continue to grow. In this case, OCR's investigation into the breach concluded that Service Provider's risk analysis and risk management processes were inadequate. Additionally, their Security Rule policies had been drafted, but not finalized and implemented, including those for ePHI and mobile devices. These shortcomings failed to comply with the requirements of 45 C.F.R. § 164.308(a)(1) and C.F.R. § 164.310(d)(1).

In addition to paying the significant settlement amount, OCR's corrective action plan requires Service Provider to: (i) conduct a risk analysis;

(ii) develop and implement a risk management plan; (iii) implement secure device and media controls; and (iv) review and revise their training program.

PRACTICAL TAKEAWAYS

OCR's continued heightened activity with HIPAA enforcement actions should put covered entities on alert. Specifically, covered entities should consider the following.

- As security breaches continue to increase in regularity, covered entities should ensure that their HIPAA Privacy Rule and Security Rule policies and procedures are up to date and compliant. Additionally, covered entities must provide appropriate training to their workforce members so they are aware of organizational and HIPAA requirements, as well as ongoing threats to the privacy and security of PHI.
- Covered entities must enter into compliant business associate agreements prior to providing PHI to third parties. It is important for covered entities to understand when a business associate agreement is and is not required. Covered entities should maintain and regularly update a log of their business associate agreements.
- While the settlement amounts imposed by OCR are often the most noticeable aspect of an enforcement action, covered entities should note the numerous obligations imposed by the corresponding corrective action plans. Those requirements often entail significant financial and/or personnel commitments.

Additional information on these enforcement actions is available at the following links: FQHC; Center; and Service Provider.

If you have any questions, please contact:

- Elizabeth Callahan-Morris at (248) 457-7854 or ecallahan@hallrender.com;
- John Weber at (248) 457-7816 or jweber@hallrender.com; or
- Your regular Hall Render attorney.