HINSHAW

Federally Qualified Health Center Agrees to Settlement for Failure to Implement

Healthcare Alert | 5 min read
Aug 26, 2020

As detailed in a press release from the U.S. Department of Health and Human Services (HHS), "Metropolitan Community Health Services, doing business as Agape Health Services (Metro), has agreed to pay $25,000 to the U. S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and to adopt a corrective action plan (CAP) to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule." This ruling demonstrates that *all* covered entities should annually adopt and implement basic HIPAA security compliance measures to prevent breaches and subsequent fines.

The Alleged HIPAA Violations

Metro—a Federally Qualified Health Center (FQHC) in rural North Carolina that provides medical, dental, behavioral health, and pharmacy services to low-income and uninsured individuals—filed a breach report with OCR concerning an "impermissible disclosure of protected health information" for 1,263 patients to an unknown email account. As explained in the press release, the subsequent OCR investigation and HIPAA compliance review "revealed longstanding, systemic noncompliance with the HIPAA Security Rule." Prior to the breach, Metro had failed to implement HIPAA Security Rule policies and procedures, in violation of 45 C. F. R. §164. 316, and an accurate and thorough assessment of the potential risks to the confidentiality, integrity, and availability of electronic protected health information (ePHI) had not been conducted, in violation of 45 C. F. R. § 164. 308(a)(l)(ii)(A). In addition, no HIPAA security awareness and training had been provided to the workforce until five years after the occurrence of the breach, in violation of 45 C. F. R. §164. 308(a)(5).

The Resolution Agreement and Corrective Action Plan

Under the terms of the Resolution Agreement reached with OCR, Metro agreed to pay $25,000, and to adopt and implement a two-year corrective action plan (CAP) that requires it to undertake the following tasks:

> **Risk Analysis**: Conduct and complete an analysis of its enterprise security risks and vulnerabilities of all electronic equipment, data systems, programs, and applications that contain, store, transmit, or receive

ePHI. The risk analysis must incorporate a complete inventory of all electronic equipment, data systems, off-site storage, and applications that contain ePHI. Metro must report its planned scope and methodology for the risk analysis to OCR for approval, and provide OCR with a copy of the risk analysis.

Risk Management Plan: Within 60 days after OCR approval of the risk analysis, Metro is required to develop a risk management plan to address and mitigate any security risks and vulnerabilities identified in its risk analysis. The risk management plan must include a process and timeline for implementation, evaluation, and revision. The risk management plan must be forwarded to HHS for its review and approval.

Policies and Procedures: Metro will need to review and revise its written policies and procedures to comply with the HIPAA Privacy, Security, and Breach Notification Rules. Metro's policies and procedures, at a minimum, must address: (i) Uses and Disclosures of PHI; (ii) Minimum Necessary; (iii) Disclosures to Business Associate; (iv) Training; (v) Safeguards; (vi) Changes to Policies and Procedures; (vii) Administrative Safeguards; (viii) Physical Safeguards; (ix) Technical Safeguards; (x) Notification to Individuals; (xi) Notification to the Media; and (xii) Notification to the Secretary of HHS.

Annual HIPAA Compliance Planning: Annually conduct a risk assessment and develop a risk management plan, documenting the security measures implemented to sufficiently reduce the identified risks and vulnerabilities to a reasonable and appropriate level. Metro must annually review the policies and procedures, and promptly update the policies and procedures to reflect changes in operations, federal law, HHS guidance, or material compliance issues discovered that warrant a change in policies and procedures. Metro is further required to create or revise policies and procedures in response to any findings in its annual risk analysis or to implement actions required by the corresponding risk management plan.

Education and Training: Adopt and distribute the policies and procedures to all current workforce members and to new workforce members within 14 days of retention, and routinely update the policies and procedures. Metro must submit its planned training materials to HHS for review, and provide security training to its workforce within 30 days of HHS approval of the security training materials.

Investigate and Report Potential Violations: Promptly investigate reports of potential violations of the revised policies and procedures and, if a violation has occurred, notify HHS within 30 days.

Annual Reports: Provide HHS with annual reports on its policies and procedures, accounting of business associates, training materials, security implementation, and reportable events, among other items.

OCR's Consideration of the Nature and Size of the Covered Entity

When deciding on an appropriate settlement, OCR took the nature of the organization and several other factors into account. OCR considered that Metro is a FQHC that provides free or discounted health care services to an underserved population, however that did not stop it from taking enforcement action against a small covered

entity that only serves 3,100 patients annually. Metro's multiple HIPAA breaches of multiple HIPAA rules spanning over several years would have normally resulted in a much larger financial settlement, thus OCR did consider the nature and size of Metro when determining the appropriate financial penalty.

Compliance Take-Aways

The Metro resolution agreement illustrates OCR's focus on enforcement of the HIPAA Security Rule, and OCR's belief that compliance is critical for all covered entities, even when the covered entity is a small, nonprofit FQHC that provides care to rural underserved populations. "Health care providers owe it to their patients to comply with the HIPAA Rules. When informed of potential HIPAA violations, providers owe it to their patients to quickly address problem areas to safeguard individuals' health information," said Roger Severino, OCR Director. All covered entities should annually adopt and implement basic HIPAA security compliance measures, including but not limited to the Metro corrective action plan requirements summarized above.

Cyber threats and data breaches can negatively impact FQHC operations, therefore FQHCs must take proactive efforts to manage cyber risks. Metro is the second FQHC resolution agreement as the result of a security breach created by a phishing attack on FQHC employees (See, Metro Community Provider Network, April 2017), and therefore it emphasizes the need for FQHCs to include phishing risks in their risk analysis and risk management plans. In light of recent phishing, ransomware, and cyberattacks on healthcare organizations, FQHCs should consider undertaking cyberattack prevention measures recommended by OCR, which may include vulnerability patching, risk analysis, adoption of a cybersecurity incident response plan, training, and a risk management plan.

Hinshaw attorneys have significant experience in advising health care organizations on HIPAA privacy and security compliance matters. For further information, please contact Michael A. Dowell or your regular Hinshaw attorney.

Related People

Michael A. Dowell

Partner

213 614-7341