OCR Audit Results and Enforcement Actions on HIPAA Compliance Sends A Message to Covered Entities and Business Associates that their New Year's Resolutions Must Include HIPAA Compliance

1.11.2021

2020 saw an increase in enforcement action by the Department of Health & Human Services, Office of Civil Rights ("OCR") regarding noncompliance with the HIPAA Privacy, Security and Breach Notification Rules, with penalties ranging from $3,500 to $6.85 million. As discussed in our October 29, 2020 Client Alert, there is a known "imminent cybercrime threat" in the health care industry, so ensuring your organization can withstand an attack is critical not only to ensure business continuity but also to avoid the costs associated with such an attack and HIPAA non-compliance generally.

With 2021 underway, now is the time for Covered Entities and Business Associates to get their HIPAA compliance efforts in check. As a starting point, Covered Entities and Business Associates should learn from the OCR's 2016-2017 HIPAA Audits Industry Report ("Report") issued December 17, 2020, to identify the issues that OCR found lacking in the 166 Covered Entities and 41 Business Associates audited. A review of the Report reveals one simple truth; many of the compliance challenges that Covered Entities and Business Associates faced in the past are the same challenges experienced today.

Among the most significant violations found in the Report was Covered Entities and Business Associates not implementing the HIPAA Security Rule requirements for risk analyses and risk management. According to the Report, only 14% of the Covered Entities and 17% of the Business Associates audited "substantially fulfilled their regulatory responsibilities to safeguard ePHI they hold through risk analysis activities."

Other findings in the report include:

- *Positives:* Most covered entities met the timeliness requirements for providing breach notification to individuals

Related Services

Cybersecurity and Privacy Specialty Team

Emerging Technology Specialty Team

Health Care

Health Care Industry Team

HIPAA

and

> (of those that maintained a website about their customer services or benefits) satisfied the requirement to prominently post their Notice of Privacy Practices (NPP) on their website.

- *Negatives:* Most covered entities *failed* to meet the requirements for adequately safeguarding protected health information (PHI), and failed to meet the requirements ensuring individuals' right of access, and providing appropriate content in their NPP.

Covered Entities and Business Associates should review the Settlement Agreements posted on the OCR website for additional lessons-learned for proper HIPAA compliance. However, some key takeaways from the Report and the Settlement Agreement include:

- Encrypt all devices that contain and transmit ePHI.
- Train your workforce annually on Security and Privacy requirements for PHI and ePHI.
- Conduct ***and document*** periodic risk assessments.
- Ensure your organization has a risk management program in place.
- Ensure patients are afforded timely access to their PHI.
- Respond promptly to known or suspected vulnerabilities.
- Report breaches in a timely fashion.

With all the available tools offered by OCR, compliance with the HIPAA Rules should not be as daunting a task as it seems. As the Report provides:

> "HHS offers many tools to assist entities in complying with HIPAA. For example, entities can consult the recently updated HHS Security Risk Assessment Tool and OCR's Guidance on Risk Analysis Requirements under the HIPAA Security Rule for help in evaluating whether they have a compliant risk analysis and risk management process. An entity can use one of OCR's model notices of privacy practices, as a template, to ensure it includes all of the HIPAA required statements in its NPP. Additionally, OCR's access guidance clarifies how covered entities can improve patients' access to their health information by implementing improved policies and procedures and digital technologies.
>
> ***
>
> Several sources of guidance are available for developing risk management programs that include risk analysis. OCR, ONC and the National Institute of Standards and Technology (NIST) offer technical assistance for covered entities and business associates."

OCR's Settlement Agreements, Guidances, and Reports are publicly available to provide notice to Covered Entities and Business Associates of their responsibilities and the penalties that they may face when non-compliant. What 2020 clearly established is that no one is immune from liability. Covered Entities and Business Associates of all sizes must look at their own practices and policies to ensure

they are meeting their responsibilities or face significant penalties.

Of course, if you have any questions at all, our Butzel Long Healthcare Team and Cybersecurity and Privacy team is here to help.

Debra Geroux
248.258.2603
geroux@butzel.com

Jennifer Dukarski
734.213.3427
dukarski@butzel.com

Mark R. Lezotte
313.225.7058
lezotte@butzel.com