Suffer a small HIPAA breach? OCR may be looking for you!

9.30.2016

The U.S. Department of Health and Human Services, Office of Civil Rights ("OCR") has raised the stakes for Covered Entities and Business Associates making it clear that it will no longer treat small breaches as a low priority. On August 18, 2016, OCR announced its new Initiative to increase the investigative and enforcement efforts in its Regional Offices concerning small breaches (those effecting less than 500 individuals). Specifically noting five recent settlements involving small breaches, including the Catholic Healthcare Services of the Archdiocese of Philadelphia ($650,000), Triple-S Management Corp. ($3.5 million) and St. Elizabeth's Medical Center ($218,400), OCR made it clear that its intent is to enforce compliance with the HIPAA regulations and understand the root cause of the breaches. This initiative is consistent with OCR's September 7 announcement warning Covered Entities and Business Associates of the ever-increasing cyber threats and encouraging them to share information concerning cyberattacks and other breaches in accordance with the Cybersecurity Information Sharing Act of 2015 (CISA) and President Obama's Executive Order 13691.

> "CISA encourages Covered Entities and Business Associates to help each other prepare for possible threats or vulnerabilities to ePHI systems by sharing information such as a description of the technical, physical, or administrative specifications related to threats to systems or vulnerabilities to systems, in addition a broad description of the harm caused by exploitation of these specifications."

While breach investigations of any size are now given greater priority, OCR made it known that it will also be looking at those Covered Entities and Business Associates that did **not** have any small breaches reported when compared to their industry counterparts:

Related Services

Cybersecurity and Privacy Specialty Team

Health Care

Health Care Industry Team

HIPAA

Telemedicine & E-Health

> "Regions may also consider the lack of breach reports affecting fewer than 500 individuals when comparing a specific covered entity or business associate to like-situated covered entities and business associates."

Beginning this month, OCR, through the continuing hard work of its Regional Offices, has begun an initiative to more widely investigate the root causes of breaches affecting fewer than 500 individuals. While not every small breach will ultimately be investigated at this time, Regional Offices will increase its efforts to identify and obtain corrective action to address entity and systemic noncompliance related to these breaches. Among the factors Regional Offices will consider include:

- The size of the breach;
- Theft of or improper disposal of unencrypted PHI;
- Breaches that involve unwanted intrusions to IT systems (for example, by hacking); The amount, nature and sensitivity of the PHI involved; or
- Whether there are multiple breach reports of similar issues from the specific Covered Entity or Business Associate.

With ever increasing cybersecurity issues, small breaches and heightened enforcement, implementing and maintaining a compliance program and response strategy is critical. Knowing not only what your data is, but where it is located and how it is secured are critical first steps. OCR has highlighted the importance of annual Risk Assessments and has offered quick tips for Covered Entities and Business Associates that bear repeating:

- Know what data you have and where it is located;
- Encrypt or de-identify sensitive information;
- Know why you have the type of data, how it is used and created;
- Strengthen security when sensitive data is in-transit and ensure breaches and security incidents are properly addressed as part of business associate and service level agreements;
- Monitor access to data and limit it to users that need access for their job function; and
- Ensure employees that touch the data are appropriately trained.

With associated costs for security incidents, noncompliance and cyberattacks reaching into the millions, not knowing what is happening in your own organization can have devastating effects.

If you would like additional information about this Alert, or have question about your organization's HIPAA security compliance, please contact one of the individuals listed below or your Butzel Long attorney.

Debra A. Geroux
248.258.2603
geroux@butzel.com

Jennifer Dukarski
734.213.3427
dukarski@butzel.com