Healthcare organizations face pressure to remedy cyber weak-spots

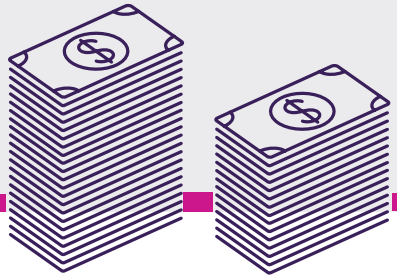
Speculation that the Office for Civil Rights (OCR), the federal Health Insurance Portability and Accountability Act (HIPAA) enforcer, may be less active under the current administration has proven untrue. Over the last year, OCR was quite busy. Analysis of OCR's 2018 activity by Beazley's in house breach response team, Beazley Breach Response (BBR) Services, reveals these highlights:

- OCR issued the largest Resolution Agreement payment to date - $16 million against Anthem in its capacity as a HIPAA business associate as the result of its 2015 data breach affecting over 78 million individuals' protected health information (PHI). OCR Resolution Agreement amounts paid last year ranged from $100,000 to Anthem's $16M, bringing the $2.6 million average payment in 2018 sharply up as compared to the $1.9 million average payment in 2017.
- OCR investigations are taking longer to close. Investigations ranged from three to seven years in length for Resolution Agreements issued in 2018. From the time of the data breach to the final OCR Resolution Agreement, OCR took an average of 4.3 years to bring matters to closure last year (versus an average of 4 years in 2017 and an average of 3.6 years in 2016).
- OCR is actively scrutinizing reports of small breaches for patterns of noncompliant behavior. Frensenius Medical Care paid OCR $3.5 million for five separate breaches by subsidiary companies affecting between 10 and 245 individuals each; each breach involved lost or stolen devices, drives or desktops. In issuing its corrective action plan, OCR focused on the lack of policies and procedures for devices and failures to assess the risks involved in device security.

Other noteworthy developments included a rare look at an administrative law judge's (ALJ) interpretation of OCR's exercise of authority in imposing civil monetary penalties (CMPs) against a covered entity. The University of Texas MD Anderson Cancer Center reported three separate breaches to OCR which affected a total of 35,000 individuals and involved an unencrypted laptop and unencrypted USB thumb drives. During its investigation, OCR noted that MD Anderson acknowledged and documented lack of encryption as a key risk, yet did not implement access controls to address these encryption issues. After failing to reach resolution informally, OCR moved to impose over $4 million in CMPs and MD Anderson appealed. The ALJ granted summary judgment in favor of OCR. In supporting OCR's decision and the amount of the CMPs, the ALJ made several insightful observations in addressing MD Anderson's assertions, including:

- Documented risk mitigation plans must be followed;
- While there is no direct regulatory requirement to encrypt, other measures to secure PHI must be used and must be successful;
- Reinforcement of the meaning of disclosure. PHI does not have to be seen by someone in order to have been disclosed;
- Employees who do not follow policies and procedures during the discharge of employment duties remain the problem of the employer; and
- MD Anderson failed to avail itself of HIPAA's hybrid entity structure that could potentially have reduced its exposure to HIPAA's non-disclosure requirements.

$16 million = largest OCR Resolution Agreement payment to date



$2.6 million

average Resolution Agreement amount in 2018

BZCER022_US_08/19

Other themes emphasized by OCR this year included the importance of performing and documenting regular security risk analyses and risk management plans, ensuring that business associate agreements are in place and making sure that media access policies are up to date and followed.

This ALJ decision and all of the OCR Resolution Agreements issued this year, which can be found on OCR's website https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html, provide information on lessons learned for HIPAA covered entities and their business associates.

$100k - $16million

range of 2018 OCR Resolution Agreement amounts

About Beazley's BBR Services Team

Beazley has managed thousands of data breaches since the launch of Beazley Breach Response in 2009 and is the only insurer with a dedicated in-house team focusing exclusively on helping clients handle data breaches.

The BBR Services team works directly with BBR insureds during all aspects of incident investigation and breach response and coordinates the expert services that BBR insureds need to satisfy legal requirements and maintain customer confidence. In addition to coordinating data breach response, BBR Services maintains and develops Beazley's suite of risk management services, designed to minimize the risk of a data breach occurring.

Protecting your organization from OCR scrutiny

- Regularly train employees on HIPAA and document training.
- Conduct proper risk assessments for all protected health information (PHI) and electronic PHI (ePHI).
- Encrypt data at rest and in transit.
- Utilize the minimum necessary PHI when relaying data.
- Notify affected individuals in a timely matter – without unreasonable delay and in no case later than 60 days following the discovery of the breach. This also applies to notifying OCR if the breach affects more than 500 individuals. If fewer than 500 are affected, then disclose in an annual report.
- Ensure business associate agreements (BAAs) are current, executed, and stored somewhere such that they are easy to locate in the event of an incident or OCR investigation.
- Monitor user credential access to ePHI, and modify as necessary with terminations or changes to position.
- Train employees on email guidance for communications within your organization, with external providers or business associates, and with patients, as well as the use of any encryption solutions you have implemented.
- Institute procedures to double-check patient demographics at visits so information is not sent to outdated locations.
- Train employees about the risks of exposing patient information through the use of social media and the risks of unauthorized access or access beyond the minimum necessary. Audit access to electronic medical records. Audits may include random spot checks across the patient population and monitoring of records of celebrities, VIPs, or other patients who might be of particular interest.

beazley

www.beazley.com/bbr