DEFICIENT RISK ANALYSES, STOLEN RECORDS AND DISCLOSURE OF NFL PLAYER'S PHI LEADS TO $2.15 MILLION PENALTY

On October 23, 2019, the Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") announced a civil monetary penalty ("CMP") of $2,154,000 against a nonprofit academic health system ("Health System") for violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Notice of Proposed Determination and the Notice of Final Determination are available here.

THE VIOLATIONS

OCR provided a detailed summary of a number of violations identified by OCR throughout the course of the investigation. The violations occurred between 2011 and 2016 and included violations of the HIPAA Security Rule and the Breach Notification Rule.

- In 2013, the Health System reported losing patient records in paper format for over 1,000 patients in two separate incidents occurring only a month apart. The supervisor who received the initial report of the lost records did not notify the Health System until three months later during the internal investigation of the second incident. The Health System was 160 days late in reporting the breach to OCR and only initially reported the date of the second incident but included the number of patients from both incidents. OCR was not notified of the first incident date until almost three years after the initial report was filed. The Health System did not have a policy related to breaches until 2013, and that policy did not include specific procedures for effectively providing timely breach notification to OCR.
- In 2015 and 2016, the protected health information ("PHI") of multiple individuals, including an NFL player and a "prominent individual in the community," was improperly accessed and certain information was disclosed to the media. OCR opened a compliance review after becoming aware of multiple media reports disclosing the NFL player's PHI, including a photograph of an electronic display board in an operating room and a paper schedule. These breaches led to financial and reputational harm of the NFL player. When the NFL player's injury was publicized, including on Twitter by an ESPN reporter, another NFL team rescinded a $60 million contract offer. There was also improper access to the player's medical records by staff, who were sanctioned. Subsequently, the Health System timely reported a breach relating to another photograph of an operating room electronic display board including the PHI of the prominent community member and another individual. OCR, through its review, determined that Health System employees' ability to access records without a valid business purpose demonstrated a lack of compliance with HIPAA requirements for role-based access.
- In 2016, the Health System reported that an employee inappropriately accessed over 24,000 patient records since 2011. The Health System became aware of the employee selling patient ePHI when an anonymous call was placed to the Health System's office for compliance and ethics. The employee admitted to selling 2,000 patient records for identity theft purposes. The Health System had the ability to create audit logs and access reports for its systems but did not review such logs regularly, despite having procedures in place to do so.
- Additionally, between 2012-2018, the Health System reported 150 "under 500" breaches, which meant that in addition to the violations highlighted above, another 391 individuals were affected by breaches.

THE RISK ANALYSES

When OCR investigates entities for potential violations, it requests certain information from the entity it is investigating. In response to OCR's data request, the Health System provided its risk analyses from 2014, 2015, 2016 and 2017 that were conducted by a third party vendor, as well as internal assessments conducted in 2009, 2012 and 2013.

- OCR determined the 2014 risk analysis was deficient in scope because it did not include all electronic PHI ("ePHI") that was created, received, maintained or transmitted by the Health System. It also failed to identify the totality of threats and vulnerabilities existing in its systems. The risks, threats and vulnerabilities that were identified were not remediated by the Health System to an appropriate and reasonable level, as required by HIPAA. The Health System did not document any response to the vendor's risk assessment recommendations.

THIS IS AN ADVERTISEMENT
© 2002-2024. Hall, Render, Killian, Heath & Lyman, P.C. All Rights Reserved.

- The 2015 and 2016 risk analyses were also determined to be deficient in scope because they did not identify all ePHI created, received, maintained or transmitted by the Health System. Just like the 2014 risk analysis, the totality of risks, threats and vulnerabilities in the Health System were not identified. Sections of the risk analyses were also left blank. The Health System did not remediate the identified risks, threats and vulnerabilities to a reasonable and appropriate level. Year after year, the threats that were identified as high risk remained "high risk" in subsequent risk analyses. No evidence that any actions to implement security measures to reduce these risks and vulnerabilities was provided by the Health System to OCR.
- OCR noted that the risk analyses conducted before 2017 "erroneously" identified several provisions of the HIPAA Security Rule as inapplicable to the Health System.
- The 2017 risk analysis was also found to be deficient. The methodology used to conduct the analysis primarily included policy review and staff interviews, and not all facilities were included in the analysis.

THE PENALTY

The CMP of $2.15 million breaks down as follows:

- $326,000 for violations of the Security Management Process, an administrative safeguard that includes the implementation of policies and procedures to prevent, detect, contain and correct security violations, including the risk analysis process. This reflects 919 total days of violations at the "reasonable cause" penalty tier.
- $328,000 for violations of Information Access Management, an administrative safeguard that includes the obligation to implement policies and procedures for authorizing access to ePHI consistent with the HIPAA Privacy Rule. This reflects 921 total days of violations also at the reasonable cause penalty tier.
- $1,500,000 for violations of the Breach Notification Rule, specifically, failure to give timely and adequate notice to the Secretary of HHS. This reflects 31 total days of violations at the "willful neglect" penalty tier.

PRACTICAL TAKEAWAYS

The Health System's violations include missteps under both the Security Rule and the Breach Notification Rule. OCR's response emphasizes the importance of making continual improvements to security processes and addressing lessons learned from past breaches. Covered entities should consider the following:

- A HIPAA compliant risk analysis is not simply a matter of filling out a form. Instead, it must be thorough, reflecting the potential risks, threats and vulnerabilities to the organization.
- It is critical that any risks identified in the risk assessment be addressed in a risk management plan. Resources should be allocated to address those vulnerabilities that are most likely to be exploited, resulting in greatest risk of harm. It is not possible to resolve all risks, but the risk management plan should note a reasoned, intentional decision to defer any vulnerabilities that cannot be directly addressed.
- Patterns of noncompliance may lead to larger fines. Covered entities with an effective security and privacy compliance program, including diligent risk analyses, should identify risks, threats and vulnerabilities and seek to reasonably mitigate them. If a breach or successful security incident occurs, prompt investigation and remediation must also occur, with timely reporting when required. Workforce members should receive regular reminders regarding the need to promptly report actual or suspected security or privacy issues.
- While sanctions for workforce member violations of HIPAA are an important compliance tool, they are not always sufficient to evidence that a covered entity is appropriately addressing HIPAA compliance issues if additional steps should have been taken to prevent such employee violations. For example, access to PHI must be limited to those with a reasonable need to have that access to perform their job functions.
- HIPAA policies and procedures should be regularly reviewed. When a health system has multiple facilities, care should be taken to ensure policies and procedures reflect the operations of all such facilities. All facilities should be audited on a regular basis for HIPAA compliance.

If you have any questions or would like additional information about this topic, please contact:

THIS IS AN ADVERTISEMENT
© 2002-2024. Hall, Render, Killian, Heath & Lyman, P.C. All Rights Reserved.

- Charise Frazier at (317) 977-1406 or cfrazier@hallrender.com;
- Melissa Markey at (248) 740-7505 or mmarkey@hallrender.com;
- Patricia Connelly at (317) 429-3654 or pconnelly@hallrender.com;
- Stephane Fabus at (414) 721-0904 or sfabus@hallrender.com; or
- Your regular Hall Render attorney.

For more information on Hall Render's HIPAA, Privacy & Security services, click here.

THIS IS AN ADVERTISEMENT
© 2002-2024. Hall, Render, Killian, Heath & Lyman, P.C. All Rights Reserved.