Health Information Compliance Alert

Case Study: Risk-Assessment Fails Lead to Millions in Penalties

OCR continues to make examples of those that skimp on risk management.

HIPAA issues arise at even at the most seasoned practices. However, a recent settlement suggests that if the feds discover compliance negligence after repeated inquiries to fix it, they will deliver a swift but substantial penalty.

Background: The Federal Bureau of Investigation (FBI) warned **21st Century Oncology, Inc. (21CO)** twice about a cyber invasion of its systems in 2015, resulting in large-scale HIPAA violations for failing to adequately secure its patients' electronic protected health information (ePHI) against an "unauthorized third party," said an HHS Office for Civil Rights (OCR) release on Dec. 28, 2017.

The Fort Myers, Florida cancer treatment and oncology specialist with 179 locations in both the US and Latin America left 2,213,597 individuals exposed after internal investigations determined illegal access of its network SQL database through "remote desktop protocol from an exchange server within 21CO's network," the OCR indicated. The report suggested that evidence obtained from an FBI informant is what originally alerted the feds that the files with "names, social security numbers, physicians' names, diagnoses, treatment, and insurance information" had been breached.

Feds Weigh In

OCR levied a $2.3 million monetary settlement against 21CO for its HIPAA violations and required the organization to put together a corrective action plan to rectify its risk issues. "People need to trust that their private health information will remain exactly that; private," stated OCR Director **Roger Severino**. "It's not just my hope that covered entities will learn from this example and proactively find and address their security risks, it's what the law requires."

Why: The OCR's biggest complaint pointed to repeated compliance basics' blunders by 21CO. The healthcare provider missed opportunities to better assess and manage its risk. And with large-scale settlements like this one becoming the norm, practices cannot be too careful when devising their HIPAA protocols. It remains evident that a strong compliance foundation, which promotes and outlines in writing the HIPAA Privacy and Security rules, provides some insulation against steeper penalties.

"Covered entities and business associates must insulate their businesses with a comprehensive compliance plan and risk analysis addressing and mitigating any applicable privacy and security risks," advises attorney **John E. Morrone**, a partner at Frier Levitt Attorneys at Law in Pine Brook, New Jersey. "Through recent settlements, OCR has demonstrated its propensity to impose significant fines on entities that fail to implement appropriate safeguards, independent of the number of affected individuals or the content of the protected health information included in a particular breach."

Do this: If your practice is due for a HIPAA-compliance plan update, consider adding these priorities that 21CO failed to implement - but that the OCR looks for after a breach occurs. The essential standards include:

- Evaluate thoroughly the "potential risks and vulnerabilities to the confidentiality, integrity, and availability" of your patients' ePHI, the OCR advises.
- Integrate the federally required security measures necessary after the risk assessment to reduce the chance of the loss of ePHI.
- Manage and review your protocols often to ensure that the safeguards are working.
- Utilize such tools as audit logs, multi-factor authentication, systems controls, certified vendors and software, and tracking devices and reports that show inconsistencies in your system.
- Use and insist upon business associate agreements (BAA) with all business partners, suppliers, and vendors.

Tip: After you assess your risk and as part of your practice HIPAA-plan implementation and management, it is a great idea to create a list of all business associates (BAs) that provide services to your organization and update this annually as changes arise and your practice evolves. It's easy to forget to alert BAs, and some may feel uncomfortable insisting that business partners, suppliers, and vendors follow HIPAA. Nonetheless, the OCR insists that your final steps include identifying BAs and setting up BAAs - they must understand what your 2018 initiative entails, why HIPAA is important to the integrity of your practice, and sign off on your principles in a BAA.

Resource: For more information about the 21CO settlement and corrective action plan, visit www.hhs.gov/about/news/2017/12/28/failure-to-protect-the-health-records-of-millions-of-persons-costs-entity-millions-of-dollars.html.