KRIEG DEVAULT

Insights

Inquiring Minds Want to Know - Limit Access to PHI to Prevent Snooping

July 6, 2023

By: Robert A. Anderson and Hillary N. Buchler

The U.S. Department of Health and Human Services, Office for Civil Rights ("OCR") recently concluded its **investigation** into Yakima Valley Memorial Hospital ("Yakima"). The matter illustrates the need to limit access to private health information ("PHI") to those members of the workforce with a need to know. OCR investigated Yakima after several security guards accessed the PHI of more than 400 Hospital patients. HIPAA Privacy, Security, and Breach Notification Rules require covered entities to secure and protect PHI. Unlawful access to PHI must be self-reported to OCR. Yakima's breach notification report stated that 23 hospital security guards accessed patients' PHI "without a job-related purpose." Yakima agreed to pay a $240,000 settlement to OCR for the violation. Yakima must also update its policies and procedures to prevent this violation from reoccurring and must train its employees to prevent them from violating PHI safeguards. While one can imagine rare circumstances in which a hospital security guard might find it helpful to access the PHI of a patient, Yakima and its patients (and its security guards) might have been better served by electronically blocking access to PHI by security personnel.

OCR will monitor Yakima for the next two years to ensure that Yakima complies with HIPAA Rules. Under Yakima's **Corrective Action Plan**, OCR requires Yakima to conduct a risk analysis identifying the risks and vulnerabilities to patients' PHI. Yakima must then develop and implement a risk management plan addressing and mitigating those risks and vulnerabilities. Yakima must also develop, maintain, and revise written policies and procedures in compliance with HIPAA and enhance its HIPAA and Security Training Program with updated HIPAA policies and procedures. OCR further requires Yakima to review its business relationships and identify all business associates to ensure that HIPPA compliant business associate agreements are in place.

HIPAA covered entities must ensure that only those employees with permission can access PHI. All other employees cannot be allowed to snoop PHI. When impermissible access of PHI occurs and HIPAA Rules are violated, covered entities are subject to liability from OCR, sizeable settlement costs, and a comprehensive Corrective Action Plan. These types of breaches can also undermine a provider's public image and trust within the community. Thus, it is essential for covered entities to understand and implement the HIPAA Rules and to proactively limit access to PHI to those who need to know.

Contact **Robert A. Anderson** or **Hillary N. Buchler** with any questions regarding the implications of HIPAA privacy and security rules applicable to members of the hospital workforce.

Disclaimer. The contents of this article should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult with counsel concerning your situation and specific legal questions you may have.