**Allison (Ally) Kjellander**

Associate
208.383.3930
Boise
aakjellander@hollandhart.com

# OCR Cracks Down on Electronic Protected Health Information Breaches under HIPAA

**Insight — 02/06/2023**

The U.S. Department of Health and Human Services Office for Civil Rights ("OCR") entered into a Resolution Agreement ("Agreement") with Banner Health on behalf of Banner Health Affiliated Covered Entities ("Banner")[1] to remedy a data breach caused by a bad actor ("Hacker"). The breach affected approximately 2.81 million patients' electronic protected health information ("ePHI")[2]. Banner discovered and reported the breach in 2016, which triggered OCR to investigate Banner's compliance with the Health Insurance Portability and Accountability Act ("HIPAA"). OCR's investigation revealed evidence of Banner's long-term noncompliance with HIPAA's Security Rule under 45 C.F.R. Part 160 and Subparts A and C of 45 C.F.R. Part 164 ("Security Rule"). For example, OCR believed Banner potentially violated the following provisions under HIPAA:

- The requirement to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI held by Banner. *See* 45 C.F.R. § 164.308(a)(1)(ii)(A).
- The requirement to implement sufficient procedures to regularly review records of information system activity. *See* 45 C.F.R. § 164.308(a)(1)(ii)(D).
- The requirement to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. *See* 45 C.F.R. § 164.3012(d).
- The requirement to implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. *See* 45 C.F.R. § 164.312(e)(1).

To remedy this, Banner paid $1,250,000.00 to OCR and agreed to implement a corrective action plan ("CAP") that OCR will monitor for two years. Under the CAP, Banner agreed to take the following steps to ensure compliance with the Security Rule:

- Conduct an accurate and thorough risk analysis to determine risks and vulnerabilities to electronic patient/system data across the organization.
- Develop and implement a risk management plan to address identified risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.
- Develop, implement, and distribute policies and procedures for a

risk analysis and risk management plan, the regular review of activity within their information systems, an authentication process to provide safeguards to data and records, and security measures to protect ePHI from unauthorized access when it is being transmitted electronically.

- Report to OCR within 30 days when workforce members fail to comply with the HIPAA Security Rule.

Although the Agreement is binding only between OCR and Banner, it serves as a stark reminder to other healthcare providers to be proactive in their ePHI security and privacy approach. Thus, healthcare providers must continually monitor and update privacy and security policies, procedures, and the implementation of those policies and procedures to prevent avoidable breaches to patients' ePHI.

For more information on the terms of the Agreement, follow this link.

[1] Banner is a “Covered Entity” as defined in 45 C.F.R. § 160.103. Also, Banner is one of the largest non-profit health systems in the country, with over 50,000 employees operating across six states.
[2] The ePHI accessed by the Hacker included patient names, physician names, dates of birth, addresses, Social Security numbers, clinical details, dates of service, claims information, lab results, medications, diagnoses and conditions, and health insurance information.