

Part B Insider (Multispecialty) Coding Alert

Physician Notes: 2 Payers Face Settlements, CAPs for Laptop Breaches

Plus: Watch out for aggressive OCR audits this fall.

Stolen unencrypted laptops were to blame for two HIPAA settlements, which totaled nearly \$2 million in settlements, as well as extensive corrective action plans (CAPs). **Concentra Health Services**, a subsidiary of **Humana, Inc.**, agreed to a \$1.7 million settlement with HHS for alleged HIPAA violations related to a breach notification stemming from a stolen unencrypted laptop.

According to Concentra's HHS-ordered CAP, the company must:

- Implement a security management process, including a risk analysis and risk management plan;
- Provide written updates to HHS describing encryption requirements for all devices;
- Provide security awareness training for all workforce members;
- Submit an Implementation Report to HHS; and
- Submit Annual Reports to HHS.

QCA Health Plan, a health insurance provider in Arkansas, paid out a smaller settlement of \$250,000, also due to a breach involving a stolen unencrypted laptop. The laptop contained the protected health information (PHI) of 148 individuals. Under QCA's CAP, the insurer must:

- Implement a security management process, including a risk analysis and corresponding risk management plan;
- Provide security awareness training for all workforce members who have access to electronic PHI (ePHI); and
- Submit Annual Reports to HHS.

These two breach cases share many similarities. Among them are three key steps these companies did not take that could have prevented the breaches in the first place □ or at least minimized the breach-associated costs and sanctions.