OASIS Alert

Industry Notes: OIG Focuses On Missing Home Health OASIS Data

You'd better make sure you're submitting OASIS data to back up your claims, because the OIG is like a dog with a bone on the issue.

In its new Semiannual Report to Congress, the HHS Office of Inspector General tells lawmakers about an estimated $25 million overpayment due to missing OASIS data. The OIG highlighted the problem in a report it released in March. "Overpayments occurred because HHAs often had inadequate controls for the submission of OASIS data," the OIG says in the new semiannual report.

"CMS should complete a process that would allow the claims processing system to interface with State survey agency systems to identify, on a prepayment basis, HHA claims without accepted OASIS data submission," the OIG urges. See the report at http://oig.hhs.gov/reportsand-publications/archives/semiannual/2014/SARS14-Web-Final.pdf.

Study: Med Management Helps Some Patients Avoid Hospital

Your lowest risk patients may benefit from medication management to reduce rehospitalizations, but it probably isn't going to help high-risk patients much. At least, that's what one new study has found.

A recent study in Health Services Research, assessed the efficacy of pharmacist-led telephone medication therapy management (MTM) at reducing hospitalizations in Medicare patients entering home care. The experiment used an initial phone call by a pharmacy technician to verify active medications; a pharmacist-provided medication regimen review by telephone; and follow-up pharmacist phone calls at day seven and as needed for 30 days.

Results: "There was no significant difference in the 60-day probability of hospitalization between the MTM intervention and control groups," acknowledge the study authors in the abstract. But "for patients within the lowest baseline risk quartile ... the intervention group was three times more likely to remain out of the hospital at 60 days ... compared to the usual care group."

Bottom line: "This MTM intervention may not be effective for all home health patients," say the authors led by pharmacist **Alan J. Zillich** at the **Purdue University College of Pharmacy**. "However, for those patients with the lowest-risk profile, the MTM intervention prevented patients from being hospitalized at 60 days.

See the abstract at http://onlinelibrary.wiley.com/doi/10.1111/1475-6773.12176/abstract.

Stolen Unencrypted Laptops Lead To Nearly $2 Million In HIPAA Fines

Two recently announced HIPAA settlements show that the **HHS Office for Civil Rights** is cracking down on unprotected data contained on mobile devices. And if you're not already encrypting your mobile devices, you could be next in the OCR's crosshairs.

Background: Stolen unencrypted laptops were to blame for two HIPAA cases, 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 workers who have access to electronic PHI; and
- Submit Annual Reports to HHS.

Keep Data Safe with Better Password Habits

Providers that don't make staffers change their passwords quarterly are taking unnecessary risks. Users should change their passwords regularly and should be prevented from reusing at least their last two or three passwords, instructs the **HHS Office of the National Coordinator for Health Information Technology** (ONC).

You should ensure that your systems are configured so that passwords must be changed on a regular basis, ONC stresses. "By requiring passwords to change quarterly, you help prevent passwords from being discovered and used illicitly."

Also, remember to ensure that staff members create strong passwords. According to ONC, strong passwords are at least eight characters long, and include a combination of upper and lower case letters, at least one number, and at least one special character like a punctuation mark.

For more regulatory, compliance and reimbursement news, see Eli's Home Care Week. Information on subscribing is online at www.aapc.com/codes/coding-newsletters/my-homecare-week-alert.