Long Term Care Compliance Client News – July 2017

➢ Hospitals billed insurance – and then billed the patient some more

Memphis hospitals face class action lawsuits filed by patients who claim the hospitals engaged in "substitute" or "balance" billing. For example, one patient asserts that he presented his insurance information during an emergency room visit. The hospital charged $4008. The insurance company paid the hospital $1022, and collected a $150 copay/deductible from the patient. The hospital continued to collect an additional $4008 from the patient.

If these allegations are true, they raise questions about whether the hospitals are adhering to the contractually negotiated rates they have in place with insurance companies.

Hypothetically speaking, if this occurred with Medicare or Medicaid patients, the compliance risk of "supplementation" would be involved. Supplementation is prohibited, and involves a provider requiring a patient to pay the provider more than the Medicare or Medicaid rate. If you have questions about supplementation, see your compliance policy and audit tool.

Source: http://www.commercialappeal.com/story/news/2017/07/15/memphis-hospitals-engage-illegal-billing-practices-suits-allege/464065001/

➢ Bupa Global Breach Due to Employee Theft

The international health insurance division of Bupa Global recently disclosed a data breach that affected approximately 547,000 customers of their international health insurance plans. According to Bupa, names, birthdates, nationalities and some contact information was compromised but no financial data or medical information was breached. The incident was due to an employee who copied and removed customer information.

While cyberattacks have been a recent trend, many data breaches are due to insiders or employees (rather than outside hackers). Here's what you can do:

- Conduct (or update) a HIPAA Security Risk Analysis to assess the internal threats to ePHI.
- Consider disabling computer USB ports, DVD or CD drives, so employees cannot download large amounts of data.

- Limit the amount of ePHI that a single employee can access (in Bupa, one employee was able to access – and share – the data of 547,000 customers)
- Consider limiting the amount of data stored in each type of record. For example, do SSNs really need to be included on a record? Could the last 4 digits be used instead of the whole number? Or maybe the SSN can be omitted from many documents entirely.

Source: https://www.bupa.com/corporate/about-us/customer-update

➢ Detroit Medical Center faces breach due to employee theft

The Detroit Medical Center (DMC) learned from a staffing agency that an agency employee stole DMC's PHI and gave it to unauthorized parties. As a result, DMC notified 1,529 patients that their information was compromised between March 2015 and March 2016. DMC did not provide any details on the scope of the breach nor how the information was obtained.

Could this happen in your organization? Are your temporary staff trained (by you) on HIPAA? Do you audit user access to patient records to see if any users are accessing records beyond their job duties? Do these audits include temporary/agency staff? Address all of these questions in your HIPAA Security Risk Analysis to reduce the risk of internal PHI theft.

Source: http://www.modernhealthcare.com/article/20170713/NEWS/170719958

➢ Anthem settles breach lawsuits for $115 million

In February 2015, Anthem made news when it announced the largest health care cyber-attack to date. A database containing names, social security numbers, addresses, dates of birth, and employment and income information for 80 million individuals was hacked. Soon after, the Wall Street Journal reported that the compromised data was not encrypted.

As a result of this data breach, a class action lawsuit was filed. Anthem settled for $115 million, and will offer two years of credit monitoring to the plaintiffs. Anthem also agreed to fund cybersecurity improvements, and to budget $15 million to pay plaintiffs' out-of-pocket breach costs.

We still wait to see if the OCR will enter a settlement with or take enforcement action against Anthem.

Source: http://www.modernhealthcare.com/article/20170623/NEWS/170629931; www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560

➢Upcoding leads to $6.5 million false claims act settlement

Carolina Healthcare System entered a $6.5 million false claims act settlement with the United States Depart of Justice, to resolve allegations that it up-coded claims for urine drug tests. CHS was accused of conducting moderately complex urine drug tests (code G0434), and billing the

government for highly complex urine drug tests (code G0431). The difference is $20 per test – but the up-coding went on for 4 years. This case was brought be a whistleblower, a former lab director for CHS, who will personally receive $1,365,000 from the settlement proceeds.

Source: https://www.justice.gov/usao-wdnc/pr/carolina-healthcare-system-agreems-pay-65-million-settle-false-claims-act-allegations

➢ Physician payments amount to $42 million false claims act settlement

A Los Angeles Hospital will pay $42 million to resolve allegations that its financial relationships with referring physicians violated the Anti-Kickback Statute and the Stark Law. There are two types of relationships at issue in this lawsuit:

1) The hospital allegedly paid above-market rates to rent office space in the physicians'' offices; and
2) Physicians received undue benefit from marketing arrangements with the hospital

This lawsuit was filed by a whistleblower: an employee who worked for as a manager at the hospital He will receive $9.2 million as his reward.

Source: https://www.justice.gov/opa/pr/los-angeles-hospital-agrees-pay-42-million-settle-alleged-false-claims-act-violations-arising

➢ Former Well Care general counsel pleads guilty to making a false statement

Thaddeus M.S. Bereday, who previously worked as WellCare's General Counsel, pleaded guilty to one count of making a false statement to the Florida Medicaid program.

WellCare operates HMOs that contract with Florida Medicare. A 2002 Florida law requires Florida Medicaid HMOs – like WellCare – to spend 80% of Medicaid premiums for behavioral health on providing behavioral health services. Bereday and four other individuals were accused of submitting inflated expenditure information in annual reports to Medicaid in order to avoid violating the 80% law.

Bereday has not yet been sentenced, but faces up to five years in federal prison.

Source: https://www.justice.gov/usao-mdfl/pr/former-wellcare-inc-general-counsel-pleads-guilty-making-false-statement-florida

➢ OCR updates

The HHS Office for Civil Rights (OCR), which enforces HIPAA, issued the following updates:

- HHS unveils improved web tool to highlight recent breaches of health information. https://www.hhs.gov/about/news/2017/07/25/hhs-unveils-improved-web-tool-highlight-recent-breaches-health-information.html

- File Sharing and Cloud Computing: What to Consider? https://www.hhs.gov/sites/default/files/june-2017-ocr-cyber-newsletter.pdf
- New CME Training to Educate Providers about the HIPAA Right of Access: https://www.hhs.gov/hipaa/for-professionals/training/index.html

➢ Missouri Nursing Home Company pays $8.3 million for false claims

Reliant Care Management, a nursing home chain based out of St. Louis, entered an $8.3 million false claims act settlement on July 5. The government alleged that, between 2008 and 2014, Reliant "provided unnecessary physical, speech and occupational therapy to nursing home residents who had a relatively high level of independence and who were residing in a skilled nursing facility primarily because of a psychiatric condition." The DOJ also asserted that Reliant's management "pressured therapists to provide therapy to residents even when the therapists believed that the therapy was not medically necessary."

Source: https://www.justice.gov/usao-edmo/pr/us-reaches-83-million-civil-settlement-reliant-care-group-and-reliant-affiliated

➢ New Compliance Tools

The following updated compliance tools are new this month:

- MPA updated the Billing and Claims Submission audit tool. Pages 57-60, the Payment Reconciliation Audit tools, have been updated.
- *NEW OIG WORK PLAN AUDIT ITEM.* The OIG updated its Work Plan in July. One of the updates is relevant to SNFs: Medicare Part B Payments for Ambulance Services Subject to Part A Skilled Nursing Facility Consolidated Billing Requirements. On the portal (Compliance Tools>Auditing and Monitoring>July 2017 OIG Work Plan Update Audit Tool) is a new audit tool to help you conduct an audit to see whether this OIG concern is an issue in your home.

➢ Monthly Compliance Moment

A Monthly Compliance Moment on the Compliance Officer is on the next page. Or, choose a different Moment from the updated Monthly Compliance Moment packet provided this month.

Monthly Compliance Moment

Meet the Compliance Officer:

[Compliance Officer's Name]

[Insert photograph of the Compliance Officer]

About me:

Why I care about compliance:

My inspiration: "[Insert quotation]

What I want you to know about compliance:

My door is always open. [Insert phone #]

Hotline: