Codify
BY AAPC

Health Information Compliance Alert

Enforcement News: Why April Was More 'Lion' Than 'Lamb' For HIPAA Breaches

Plus: Find out what new program will replace Meaningful Use.

The month of April experienced a whirlwind of data breach reports by healthcare entities, according to the **HHS Office for Civil Rights**' (OCR) so-called "Wall of Shame," where it displays all reported breaches affecting 500 or more individuals.

Of the 26 total breaches reported in April, 20 were by healthcare providers, five were by business associates (BAs), and only one was by a health plan. The cause of most breaches was unauthorized access/disclosure (13 breaches), while the rest of the breaches arose from theft (eight) and hacking/IT incidents (five).

Interestingly, most of the breaches involved paper films (eight breaches), but the rest of the reported incidents were a mixed bag involving network servers, laptops, email, and desktop computers.

The **Ohio Department of Mental Health and Addiction Services** reported by far the largest breach in April, affecting 59,000 individuals. The breach occurred due to unauthorized access/disclosure, but OCR lists the "location of breached information" as "other." The second largest came from another Ohio healthcare provider, **Mayfield Clinic Inc.**, and affected 23,341 individuals. Mayfield's breach occurred due to a hacking/IT incident and arose from email.

Link: To view OCR's "Wall of Shame," go to https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Good News: Meaningful Use Successor Should Give You More Flexibility

The **Centers for Medicare & Medicaid Services** (CMS) announcement in January that it will do away with the Meaningful Use program was certainly surprising. Now, you can get a good look at CMS' grand plan for replacing the program.

In an April 27 CMS blog posting by Acting Administrator **Andy Slavitt** and **HHS Office of the National Coordinator for Health IT** (ONC) head **Karen DeSalvo**, CMS officially announced its creation of a new program to replace the Electronic Health Records (EHRs) Incentive Program, also known as Meaningful Use.

As part of implementing the Medicare Access and CHIP Reauthorization Act (MACRA), CMS recently reviewed the Meaningful Use program, consulting more than 6,000 stakeholders including clinicians and patients. Based on that feedback, CMS has released a proposed rule that creates a new program named "Advancing Care Information," which CMS will incorporate into the Merit-based Payment System (MIPS).

In revamping the Meaningful Use program, CMS focused on three key aims: improved interoperability, increased flexibility, and more user-friendly technology. Among other changes, the rule proposes to:

- Allow physicians to choose the measures that reflect how EHRs best suit their daily practice;
- Simplify the process for achievement and offer multiple paths for success;
- Align with the ONC's 2015 Edition Health IT Certification Criteria;
- Focus on interoperability, information exchange, and security measures;

- Simplify reporting by no longer requiring all-or-nothing EHR measurement or quality reporting;
- Reduce the number of measures from 18 to only 11 measures;
- Eliminate reporting on the Clinical Decision Support and the Computerized Provider Order Entry measures;
- Exempt certain physicians from reporting when EHR technology is less applicable to their practice; and
- Allow physicians to report as a group.

This proposed new program would impact only Medicare physicians and won't apply to Medicare hospitals or Medicaid programs.

Link: You can find more information on the proposed rule at www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/Value-Based-Programs/MACRA-MIPS-and-APMs/Quality-Payment-Program.html.

Don't Let Your Insurer Dump You When Facing A Data Breach Lawsuit

With the rise in class-action lawsuits relating to healthcare data breaches, many liability insurers are trying to wriggle out of paying on claims for defending these lawsuits. But the good news is many states aren't keen on letting insurers off the hook.

One such case occurred in the **U.S. Court of Appeals for the Fourth Circuit** in Virginia. In Travelers Indemnity Co. of America v. Portal Healthcare Solutions LLC, the circuit court upheld the district court's ruling that the insurer has a duty under state law to defend an insured entity against a putative data breach class action, according to an April 15 analysis by Boston-based partner attorney **Kurt Mullen** for **Nixon Peabody LLP**.

Portal Healthcare Solutions LLC had a commercial general liability (CGL) policy with **Travelers Indemnity of America**. In April 2013, a group of patients filed a putative class-action lawsuit against Portal in New York state court for allegedly failing to safeguard their medical records. The patients had discovered that their records were posted on the Internet.

Unfortunately, decisions in other jurisdictions have concluded that data breach lawsuits aren't covered under standard CGL policies, Mullen noted. "It seems unlikely that the Fourth Circuit's affirmance of the district court in Portal will have a significant impact on the continued development of the cyber liability insurance market." But policyholders will surely continue to argue that CGL policies may indeed provide coverage for data breaches.

To read more about the Portal case, you can access Mullen's analysis at www.nixonpeabody.com/insurer-has-duty-to-defend-data-breach-class-action.