Health Information Compliance Alert

Enforcement News: When Medicare Will Remove Your Patients' SSNs From ID Cards

Plus: Find out how CMS plans to ease your MU reporting duties.

Your patients will soon no longer see their Social Security numbers (SSNs) on their Medicare insurance cards, thanks to a provision in the recently passed Medicare Access and CHIP Reauthorization Act of 2015 (MACRA).

Despite the known risks of identity theft when using SSNs, the Medicare program has continued to utilize beneficiaries' SSNs, or an easily identifiable derivative of the SSN, as the identifier appearing on the Medicare beneficiary's insurance card, noted partner attorney **Laurie Cohen** in an April 23 blog posting for the law firm **Nixon Peabody LLP.** But all that will change.

Under MACRA, Medicare and the **Social Security Administration** (SSA) will embark on a multi-year process to issue or re-issue Medicare identification cards that do not include SSNs, Cohen reported. Industry experts speculate that this change is in response to the recent high-profile data breach cases involving major insurers like **Anthem** and **Premera.** Many experts also believe that this initiative is long overdue.

MACRA mandates that Medicare cards no longer contain SSNs beyond the next four years, by the end of fiscal year 2018.

The process will cost more than an estimated $300 million and will not necessarily eliminate Medicare's continued use of a beneficiary's SSN, Cohen explained. But it will put an end to the use of a beneficiary's SSN on his Medicare ID card, "which today is routinely presented when seeking health services and then is subsequently re-disclosed in medical records and health claims forms, which all create opportunities for theft or misuse of such number."

The complete text of MACRA is available at www.gpo.gov/fdsys/pkg/BILLS-114hr2enr/pdf/BILLS-114hr2enr.pdf. "Prohibition of Inclusion of Social Security Account Numbers on Medicare Cards" is in Section 501 of the law.

You Could Soon Enjoy Streamlined MU Reporting Requirements

Good news: On April 10, the **Centers for Medicare & Medicaid Services** (CMS) announced that it has issued a proposed rule to help reduce complexity and simplify provider reporting for the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs.

CMS wants to align Stage 1 and Stage 2 Meaningful Use (MU) objectives and measures with the long-term proposals for Stage 3, according to the CMS announcement. The proposed rule covers modifications to MU for 2015 through 2017.

"The proposed rule would reduce required reporting, allowing providers to focus on objectives which support advanced use of EHR technology and quality improvement, including health information exchange," CMS states. Specifically, the proposed rule aims to:

- Reduce the overall number of objectives to focus on advanced use of EHRs;
- Remove measures that have become redundant or duplicative, or have reached wide-spread adoption;
- Realign the reporting period beginning in 2015, so hospitals would participate on the calendar year instead of the fiscal year; and
- Allow a 90-day reporting period in 2015 to accommodate the implementation of these proposed changes in 2015.

Statistics: According to CMS, more than 525,000 providers have registered to participate in the EHR Incentive Programs as of March 1, 2015. Also, more than 438,000 eligible professionals, eligible hospitals and critical access hospitals (CAHs) have received an EHR incentive payment. At the end of 2014, 95 percent of eligible hospitals and CAHs, along with more than 62 percent of eligible professionals have successfully demonstrated MU of certified EHR technology.

How Phishing Emails Put Your Patients' PHI At Risk

Do your staffers know how to spot phishing emails that trick them into providing private information or clicking on links that install malware? If not, your organization is greatly vulnerable to a phishing-related HIPAA breach.

Boston-based healthcare system **Partners HealthCare** announced that it's notifying approximately 3,300 patients about a security breach, the Associated Press (AP) reported on April 30. The breach occurred in November 2014 when several of Partners' staff members received phishing emails and provided protected health information (PHI) in response.

Some emails contained patient information including names, addresses, birthdates, telephone numbers, Social Security numbers, and clinical information like diagnoses, treatments and insurance information.

The 3,300 patients were treated at **Massachusetts General Hospital, Brigham and Women's Hospital** and several other Partners-affiliated hospitals, according to AP. Although the breach occurred nearly seven months ago, Partners is just now contacting affected patients and law enforcement. Partners claims there is no evidence of PHI misuse.

Beware Of Employees Taking Home Patient Info-Containing Paperwork

Misplaced paperwork taken home by an employee could land you in trouble for a data breach.

That's just what happened to the Ventura County, CA-run health system, which includes the **Ventura County Medical Center, Santa Paula Hospital** and a countywide network of clinics, the Ventura County Star reported on May 1. After misplacing the paperwork, another person recovered the documents fully intact and turned them into the **Oxnard Police Department.**

The paperwork contained the account information of more than 1,300 hospital and clinic patients, but it did not include Social Security numbers, insurance information, birthdates, addresses nor medical information, according to the Star. Instead, the paperwork included account information involving tracking numbers used internally at the **Ventura County Health Care Agency.**

Agency officials deemed the chances of the information being used for medical fraud extremely low, but they still publicly reported the breach according to the HIPAA statutes.

Bad Break-Up? Don't Leave PHI Lying Around At Home

Yet another employee take-home debacle has caused a separate potential HIPAA breach this time involving a Native American tribal health center.

Lac Courte Oreilles (LCO) **Tribal Governing Board, the LCO Health Center (**LCOHC) and the tribal police in Hayward, WI are investigating potential HIPAA violations, local news outlet NNCNOW reported on April 29. The violations allegedly occurred at LCOHC in late 2014 when the LCOHC Director was informed that several 2010 and 2011 healthcare records were at an employee's home.

The employee allegedly took the patient information to complete work, but failed to return the information in a "timely fashion." When the employee separated from a significant other, the employee's partner brought the health center information to the police, which prompted an internal investigation, NNCNOW stated.

Although the investigation revealed that the files contained protected health information (PHI), and the LCOHC terminated the employee, the tribe's legal department concluded that the case did not involve a HIPAA violation but did involve confidentiality policy violations. Nevertheless, LCOHC is contacting each affected patient individually. The tribe

referred the case to local law enforcement for possible criminal charges.

Keep Your Personal Documents Separate From PHI

Your own personal files and documents versus patients' medical records and protected health information (PHI) should be like the "separation of church and state" — intertwining the two will only lead to an unfortunate breach.

Case in point: On Feb. 13, an employee of the **Denton County Health Department** (DCHD) in Texas went to a printing store to print a personal document from a USB drive and left the drive at the store temporarily, reported local news outlet The Leader on April 10. But in addition to personal documents, the USB drive also contained the unsecured data files of 874 tuberculosis (TB) clinic patients.

Although the patient files did not contain any financial information or Social Security numbers, they did include patient names, birthdates, addresses, TB test results and other PHI, according to The Leader. The DCHD investigated the incident and found no evidence that any confidential information was accessed by the printing store's employees or anyone else outside the DCHD.

The employee voluntarily reported the potential breach. The DCHD is notifying all affected patients by mail in compliance with federal HIPAA and Texas state laws. The health department also announced that it has reviewed and updated its internal policies and procedures, as well as provided additional mandatory training for all its employees and changed the way it stores electronic files.