Eli's Rehab Report

Security: Protect Private Information From the Public Eye

Your NPI application could hold the key to leaking critical information

Although the initiative is temporarily on hold, CMS will be making NPIs publicly available on the Internet -- and if you didn't fill out your application properly, your confidential information may be up for grabs.

Background: The CMS initiative is in accordance with the National Plan and Provider Enumeration System (NPPES) Data Dissemination Notice that CMS published on May 30.

Basically, CMS is making certain NPPES healthcare provider data, including National Provider Identifiers (NPIs), available to the public via the Internet.��'The data CMS is making available are disclosable under the Freedom of Information Act (FOIA) and are required to be available on the Internet by the e-FOIA Amendments to the FOIA, CMS explained on its Web site.

The good news: You'll be able to look up the NPI of referring/ordering practitioner information for claims filing purposes, and you can query the NPI database by NPI, provider name, practice location and state, said **Gayle Lee, JD,** director of regulatory affairs for APTA, at a course titled "Emerging Issues in Reimbursement and Medicare," during the organization's annual conference in Denver.

The bad news: "CMS found that some providers accidentally put data in the wrong fields of their application," Lee said. For example, CMS notes on its Data Dissemination Web page that some providers put their social security numbers in the employee identification number (EIN) field by mistake. Bottom line: You don't want your social security number or other confidential identifiers unintentionally broadcasted online.

Know What You Can and Can't Change

Luckily, CMS is aware of the issue and has taken steps to protect providers. "The NPPES Data Dissemination Notice and outreach documents from CMS encouraged healthcare providers to review their FOIA-disclosable NPPES data and edit it as necessary and to remove, if they wished, sensitive data from FOIA-disclosable fields that were furnished on an optional basis," CMS said.��'

And to further help protect SSNs and taxpayer identifiers, "CMS is suppressing from display in the NPI Registry and in the downloadable files any SSNs or IRS ITINs that remain in any of the FOIA-disclosable fields in the records of healthcare providers who are individuals," the agency said.

Your turn: But you'll want to cover your own back too, and you can start by double-checking the data you submitted by making sure everything is in the correct fields. Know that you can also update certain data elements, such as your name, provider license number, mailing address, phone number and state, according to the APTA presentation slides.

Tip: "You may want to make sure you aren't listing your home address on the Internet if that's the address you put on the application," Lee said.

You can also change or delete your healthcare provider taxonomy code and other provider identifiers.

Caveat: You can't change your NPI, entity type, provider enumeration data, last update date, or NPI deactivation information, according to APTA's slides.

Your best bet is to review your data. And know that you can delete any NPPES data that CMS did not require for you to obtain an NPI, Lee said.

How to do it: Visit nppes.cms.hhs.gov, and have handy the user ID and password you received when you applied for the NPI, Lee said. Your other option is to call the enumerator at (800) 465-3203.

For more information and updates, see www.cms.hhs.gov/NationalProvIdentStand/06a_DataDissemination.asp#TopOfPage.